TONE at the TOP®

Trazendo à alta administração, conselhos de administração e comitês de auditoria informações concisas sobre tópicos relacionados a governança.

Edição 127 | Fevereiro de 2025

Uma Nova Ferramenta para Monitorar Riscos Estabelecidos

Este mês, o The IIA lançou o primeiro de uma série de novos requisitos que apoiarão os esforços dos auditores internos para melhor abordar áreas de temas quentes. O mais novo componente do International Professional Practices Framework (IPPF), *os* Requisitos Temáticos *garantirão que todas as funções de auditoria interna, independentemente de seu tamanho, estrutura de propriedade ou localização, apliquem a mesma metodologia de auditoria ao avaliar a eficácia da governança, do gerenciamento de riscos e dos controles de uma área temática em especial.*

Os Requisitos Temáticos estabelecem uma linha de base que eleva o trabalho da função de auditoria interna e o valor das informações e insights que ela fornece ao conselho e à organização. Esta edição de Tone at the Top examinará os Requisitos Temáticos e o que eles significam para os membros do conselho e suas organizações.

Preocupações Difusas e de Alto Risco

Os auditores internos prestam avaliação e consultoria independentes e objetivas para aprimorar os processos e a tomada de decisões para maximizar o valor. Para assegurar que os auditores tenham o conhecimento e habilidades necessárias para atender às necessidades das organizações, o The IIA aprimora e atualiza regularmente suas Normas e orientações. A introdução dos Requisitos Temáticos é como parte do projeto de evolução do IPPF, que também inclui as novas *Global Internal Audit Standards™* (Normas Globais de Auditoria Interna) apresentadas no ano passado, bem como outras orientações globais.

Os Requisitos Temáticos destinam-se a "temas globais frequentemente auditados que são tipicamente de risco mais alto e de natureza difusa". Os Requisitos Temáticos abordarão áreas de risco maduras e fornecerão orientação com base nas melhores práticas estabelecidas. Um requisito, sobre cibersegurança, foi lançado no início deste mês, e outros sete estão em desenvolvimento.

Requisitos Temáticos Planejados

Os requisitos temáticos que deverão ser lançados nos próximos anos incluem:

Cibersegurança	Anticorrupção/suborno
Terceiros	Gestão de pessoas
Cultura	Ger. do Risco de Fraude
Resiliência de Negócios	Sustentabilidade/ESG

A cibersegurança recebeu prioridade como o primeiro requisito temático, devido à profunda dependência das organizações da Internet na maioria ou em todas as suas atividades e devido à necessidade de proteger seu perímetro baseado na Web.

Os auditores internos estão bem conscientes da ameaça que as questões de cibersegurança representam. No mais recente relatório global Risk in Focus do IIA, os líderes de auditoria interna não apenas citam a cibersegurança como o maior risco atualmente e no próximo ano, mas também dizem que esperam que ela continue sendo a maior ameaça para suas organizações nos próximos três anos.

Os entrevistados também estão preocupados sobre um tópico relacionado, a disrupção digital, incluindo riscos associados à inteligência artificial (IA), IA generativa (GenAI) e outras tecnologias emergentes. Eles colocam a disrupção digital no fim de sua lista dos cinco principais riscos atualmente e no próximo ano, mas a colocam em segundo lugar quando olham para os próximos três anos. Embora a GenAI possa melhorar a detecção de ameaças e vulnerabilidades, ela também pode facilitar o desenvolvimento de ataques mais sofisticados e eficazes por parte dos malfeitores.

Usando os Requisitos Temáticos

Os Requisitos Temáticos formalizam como os auditores internos abordam as áreas de risco predominantes. Os requisitos:

- Estabelecem uma linha de base para as funções de auditoria interna usarem em seus esforços para mitigar os riscos na organização.
- São necessários para serviços de avaliação relevantes e recomendados para consideração em serviços de consultoria.
- Exigem que a aplicabilidade de um requisito temático seja determinada por um plano de auditoria baseado em riscos. Observando que a avaliação de riscos é uma parte importante do planejamento do chefe executivo de auditoria, eles exigem que essa determinação seja feita com base em uma avaliação das estratégias, dos objetivos e dos riscos da organização.
- Estabelecem uma abordagem globalmente consistente para a auditoria dentro de cada área temática, o que melhorará a confiabilidade dos serviços e resultados da auditoria interna.
- Fornecem critérios relevantes para a prestação de serviços de avaliação de cibersegurança.
- Devem ser aplicados no nível da entidade ou da organização em áreas que tenham impacto em toda a organização.
- Identificam os riscos difusos que deveriam, no mínimo, estar no radar da organização.
- Agregam valor ao assegurar a cobertura e a consistência apropriadas do risco cibernético.
- Não se destinam a cobrir todos os aspectos a serem considerados em um trabalho de auditoria. Em vez disso, definem os requisitos mínimos para uma avaliação consistente e confiável do tema.

Os requisitos são elaborados para permitir que os auditores internos os utilizem criteriosamente. Para entender como os requisitos podem ser colocados em prática, considere uma situação em que a cibersegurança tenha sido identificada como um risco difuso ou extenso para a organização durante o processo de planejamento da auditoria interna, e uma auditoria do assunto será realizada. Esse é claramente um caso em que o Requisito Temático deve ser aplicado, mas nem todos os casos serão tão claros.

Tomemos, por exemplo, uma equipe de auditoria interna que realiza uma auditoria de contas a pagar e descobre sobre os riscos cibernéticos associados a um processo de solicitação de pedido de compra baseado na Web. Mesmo que a cibersegurança não tenha sido identificada como um risco organizacional geral no plano de auditoria, a auditoria interna ainda aplicaria o Requisito Temático, mas de forma mais restrita. A equipe poderia passar mais tempo na parte da auditoria relativa aos controles de cibersegurança do que na parte relativa à governança ou ao gerenciamento de riscos. Os auditores internos documentariam sua justificativa para limitar o trabalho de auditoria a uma parte específica.

Sobre o The IIA

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

The IIA

1035 Greenwood Blvd.
Suíte 401
Lake Mary, FL 32746 EUA

Assinaturas Gratuitas

Visite **theiia.org/Tone** para se cadastrar para uma assinatura gratuita.

Feedback do Leitor

Envie perguntas/comentários para **T**one@theiia.org**.**

Governança, Gerenciamento de Riscos e Controles de Cibersegurança

Conforme observado, os Requisitos Temáticos abrangerão a governança, o gerenciamento de riscos e os controles de cada área temática. Sob o guarda-chuva da governança, os auditores internos devem avaliar se os processos de governança da organização abordam devidamente a cibersegurança. A governança da cibersegurança define objetivos e estratégias relacionados que promovem as metas, políticas e procedimentos da empresa.

A seção de comunicação do requisito abrange os tipos de materiais que o conselho recebe sobre estratégia, risco, objetivos e controles de cibersegurança, e considera se as iniciativas estratégicas apoiam a cibersegurança. Essa seção também abrange as políticas e os procedimentos, os papéis e as responsabilidades criados para concretizar as metas de cibersegurança, o trabalho de auditoria com os stakeholders e os requisitos de recursos para atingir as metas de cibersegurança.

A seção de gerenciamento de riscos de cibersegurança estabelece a necessidade de um processo para identificar, analisar, gerenciar e monitorar as ciberameaças, incluindo um processo para escalar rapidamente o reconhecimento dos riscos cibernéticos. O principal objetivo é assegurar que o gerenciamento de riscos de cibersegurança seja uma prioridade do ponto de vista do gerenciamento de riscos corporativos.

Os controles de cibersegurança são processos que são avaliados periodicamente para mitigar os riscos cibernéticos. Os sete processos de controle abrangem aspectos importantes e básicos que os auditores internos devem avaliar ao realizar uma auditoria de cibersegurança.

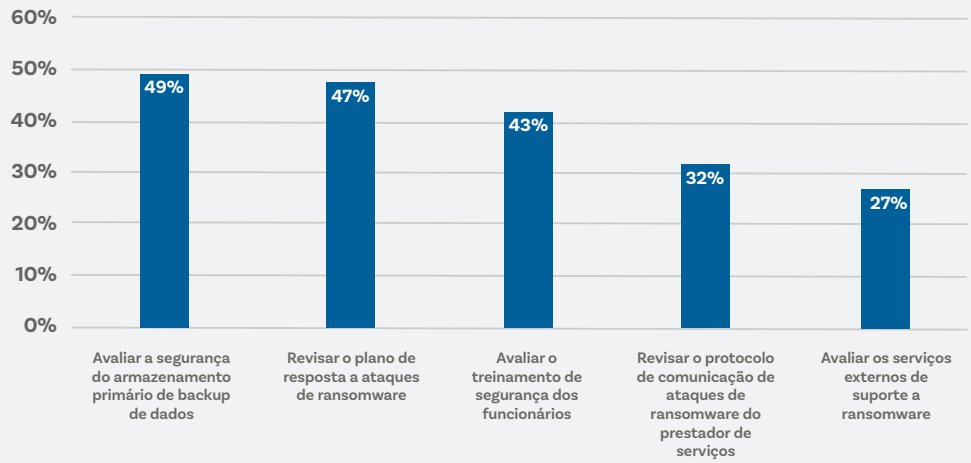
Abordando Riscos Comuns e em Evolução

Devido ao seu conhecimento profundo e holístico, os auditores internos são qualificados de forma única para reconhecer certos riscos que têm maior probabilidade de impactar a organização. O gráfico "Envolvimento da Auditoria Interna na Cibersegurança" mostra muitas das áreas em que a auditoria interna já está envolvida, fornecendo avaliação e informações.

Desenvolvidos por um grupo global de líderes de auditoria interna e outros especialistas de diversos setores, os Requisitos Temáticos promoverão o trabalho da profissão de auditoria interna, permitindo que os auditores abordem melhor os riscos comuns e em evolução.

Envolvimento da Auditoria Interna na Cibersegurança

"A prática das equipes de auditoria interna de avaliar independentemente a segurança da informação, seja internamente ou com a ajuda de terceiros, permaneceu consistente ano após ano," de acordo com a empresa de consultoria e recrutamento Jefferson Wells. No entanto, o gráfico abaixo, que mostra a porcentagem de empresas que usam equipes de auditoria interna para determinados trabalhos relacionados à cibersegurança, indica que muitas organizações não estão aproveitando ao máximo as informações e os conselhos que a auditoria interna pode oferecer.



Fonte: Pesquisa Anual *Internal Audit Priorities* de 2024, Jefferson Wells.

Requisitos Temáticos Vinculados ao Modelo das Três Linhas

O The IIA usou o Modelo das Três Linhas no desenvolvimento dos Requisitos Temáticos. Os elementos de governança e supervisão dos requisitos estão relacionados ao órgão de governança da organização, o elemento de gerenciamento de riscos à segunda linha, os controles e processos de controle à primeira linha e a função de auditoria interna, como terceira linha, prestando avaliação independente.

Modelo das Três Linhas do The IIA

PERGUNTAS A SEREM FEITAS PELOS MEMBROS DO CONSELHO

1. Quais são as nossas maiores vulnerabilidades?
2. Quais tipos de ciberataques a organização pode sofrer?
3. Quais tipos de adversários podem estar por trás deles?
4. O que o adversário estaria tentando realizar — disrupção dos negócios, roubo de dados ou ativos de informações comerciais, cobrança de resgate ou algum outro propósito?
5. Como ele poderia executar um ataque?
6. Como saberemos que ocorreu um ataque? Estamos preparados para uma resposta imediata?
7. Fazemos o melhor uso possível da avaliação e da orientação que a auditoria interna pode oferecer para lidar com os riscos de cibersegurança?
8. Estamos usando a IA para ajudar na cibersegurança? Se sim, de que forma? Se não, já consideramos o uso de IA?