Versão Preliminar para Consulta Pública
Requisito Tópico de Resiliência Organizacional

A Estrutura Internacional de Práticas Profissionais® do IIA compreende as Normas Globais de Auditoria Interna™, os Requisitos Temáticos e a Orientação Global. 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 áreas de risco específicas. 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:

1. Assunto de um trabalho no plano de auditoria interna.
2. Identificado durante a execução de um trabalho.
3. O assunto de um trabalho solicitado que não estava no plano original de auditoria interna.

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 os requisitos forem excluídos, uma justificativa deve ser documentada e mantida. A conformidade com o Requisito Temático é obrigatória e será avaliada durante as avaliações de qualidade.

Para obter mais informações, consulte o Guia do Usuário do Requisito Tópico de Resiliência Organizacional.

Resiliência organizacional

A resiliência organizacional é definida como a "capacidade de uma organização de absorver e se adaptar em um ambiente em constante mudança", na ISO 22316:2017, Security and resilience - Organizational resilience - Principles and attributes (Segurança e resiliência - Resiliência organizacional - Princípios e atributos), emitida pela International Organization for Standardization (Organização Internacional para Padronização). A resiliência organizacional é um tópico amplo, que abrange importantes elementos estratégicos, operacionais, tecnológicos, humanos, sociais e financeiros. A resiliência organizacional trata dos riscos que podem interromper ou

prejudicar significativamente a capacidade de uma organização de fornecer seus principais produtos e serviços, manter a confiança das partes interessadas ou cumprir seus objetivos estratégicos. Esses riscos podem resultar de eventos de início repentino (como desastres naturais, ataques cibernéticos e conflitos geopolíticos), pressões ambientais prolongadas (como escassez de recursos e crises de saúde pública) ou mudanças no contexto externo (como interrupções tecnológicas, mudanças regulatórias e erosão da reputação). Esses riscos também podem ser mudanças graduais ou pressões de desenvolvimento lento que, com o tempo, comprometem a estabilidade e a capacidade de adaptação de uma organização. Riscos incrementais como esses podem ser rotineiramente ignorados. As organizações resilientes antecipam e se adaptam a riscos súbitos e sutis para serem bem-sucedidas.

Os fatores de risco inerentes que elevam a ameaça à resiliência incluem alta complexidade operacional, cadeias de suprimentos globalizadas, infraestrutura centralizada ou sistemas de dados, disponibilidade limitada de mão de obra, condições voláteis de mercado e forte dependência de terceiros ou localizações geográficas críticas. As organizações em setores de alta confiabilidade ou aquelas que operam sob intenso escrutínio regulatório também podem enfrentar riscos que são inerentemente maiores devido ao impacto público e às obrigações de conformidade.

Os auditores internos geralmente avaliam os processos e controles de tecnologia da informação (TI) relacionados à continuidade dos negócios e à recuperação de desastres. Um plano de continuidade de negócios detalha as medidas que uma organização toma para retornar às funções operacionais normais quando ocorre um desastre. Um plano de recuperação de desastres descreve como as organizações protegerão seus sistemas de TI e dados críticos durante uma interrupção. A resiliência organizacional também requer planejamento estratégico, gerenciamento de riscos corporativos, liderança e cultura eficazes e processos de controle em toda a organização. Ter processos de controle sólidos para a resiliência organizacional não só permite que as organizações se antecipem, se preparem, respondam e se adaptem continuamente às mudanças, mas também que sobrevivam e prosperem.

Avaliação e avaliação da resiliência organizacional Processos de governança, gerenciamento de riscos e controle

Este requisito tópico oferece uma abordagem consistente e abrangente para avaliar o projeto e a implementação da governança da resiliência organizacional, do gerenciamento de riscos e dos processos de controle. Os requisitos representam uma linha de base mínima para avaliar a resiliência organizacional.

Governança

Requisitos:

Os auditores internos devem avaliar os seguintes aspectos da governança da resiliência organizacional:

A. Uma estratégia formal de resiliência organizacional é estabelecida e documentada pela diretoria, com objetivos que se alinham e apoiam a missão e a visão da organização. A estratégia aborda os elementos operacionais, tecnológicos e financeiros necessários para resistir e continuar as operações em meio a crises, interrupções e emergências e como se recuperar e se adaptar posteriormente. A estratégia se alinha à abordagem geral da organização para o gerenciamento de riscos e é testada e atualizada periodicamente.

B. Atualizações sobre a realização da estratégia e dos objetivos de resiliência organizacional são periodicamente comunicadas ao conselho para análise, garantindo que a resiliência seja incorporada à

supervisão estratégica, aos processos de planejamento de longo prazo e à cultura da organização, inclusive nas considerações orçamentárias e de recursos necessárias para apoiar as atividades comerciais essenciais.

C. Foram identificados processos operacionais, tecnológicos e financeiros críticos relacionados à resiliência organizacional. Políticas e procedimentos para processos críticos foram estabelecidos e são revisados periodicamente e atualizados conforme necessário para fortalecer o ambiente de controle.

D. É estabelecida uma estrutura de comando de incidentes, que inclui hierarquias de tomada de decisão, protocolos de comunicação e escalonamento, além de funções e responsabilidades operacionais e de liderança. A estrutura é usada para supervisionar e apoiar o estabelecimento de objetivos de resiliência organizacional.

E. É estabelecido um processo para reavaliar periodicamente as competências dos indivíduos que desempenham funções essenciais nos processos de resiliência. Existe um plano de sucessão que identifica os principais cargos e os possíveis candidatos para substituição.

F. É estabelecido um processo para envolver as partes interessadas internas e externas relevantes na identificação, análise e resposta às vulnerabilidades existentes e às ameaças emergentes que possam afetar a realização dos objetivos de resiliência da organização. As partes interessadas podem incluir a gerência sênior, operações, gerenciamento de riscos, TI, cadeia de suprimentos/procurement, instalações, recursos humanos, finanças, jurídico, conformidade, relações públicas, fornecedores críticos, clientes, reguladores e outros.

GERENCIAMENTO DE RISCOS

Requisitos:

Os auditores internos devem avaliar os seguintes aspectos do gerenciamento de riscos da resiliência organizacional:

A. Os processos de avaliação e gerenciamento de riscos da organização incluem a identificação, análise, mitigação e monitoramento de ameaças que podem interromper as operações. A estratégia de gerenciamento de riscos para a resiliência organizacional é comunicada a toda a organização e revisada periodicamente.

B. Os riscos relacionados à resiliência organizacional são avaliados e gerenciados periodicamente em toda a organização. A avaliação e o gerenciamento de riscos podem incluir as seguintes áreas: operações, gerenciamento de riscos corporativos, TI, cadeia de suprimentos/compras, instalações, recursos humanos, finanças, jurídico, conformidade, regulatório, relações públicas, fornecedores críticos, reputação, riscos emergentes e outros.

C. São estabelecidas a prestação de contas e a responsabilidade pelo gerenciamento de riscos de resiliência organizacional. Um indivíduo ou equipe é identificado para monitorar e relatar periodicamente como os riscos de resiliência organizacional estão sendo gerenciados, incluindo os recursos necessários para mitigar os riscos e identificar ameaças emergentes à resiliência organizacional.

D. Um processo é estabelecido para monitorar os níveis de risco de resiliência organizacional (emergentes ou previamente identificados) e escalar rapidamente aqueles que atingem um nível considerado inaceitável, conforme definido pelas diretrizes de gerenciamento de risco e tolerância a risco

estabelecidas pela organização ou pelos requisitos legais e regulamentares aplicáveis. São considerados os impactos financeiros e não financeiros do risco de resiliência organizacional.

E. A gerência implementou e testa periodicamente um processo para responder e se recuperar de ocorrências de crises, interrupções e emergências. O processo de resposta e recuperação de incidentes inclui detecção, contenção, recuperação e análise pós-incidente. A abordagem de resposta a incidentes inclui análises de cenários e testes periódicos de estresse em relação a uma série de eventos de interrupção plausíveis. Os resultados desses exercícios são analisados pela diretoria e pela gerência sênior, com ações de melhoria monitoradas e relatadas periodicamente. As recomendações são acionáveis, com propriedade e cronogramas claros.

CONTROLES

Requisitos:

Os auditores internos devem avaliar os seguintes aspectos dos processos de controle relacionados à resiliência organizacional.

A. Um processo é estabelecido para identificar fornecedores terceirizados críticos (fornecedores e vendedores) e níveis mínimos de estoque necessários para dar continuidade às operações vitais. O processo inclui a manutenção de uma lista de fornecedores alternativos.

B. Os dados essenciais para as operações são identificados e classificados. A classificação dos dados inclui a identificação de onde os dados residem, quem precisa acessá-los, como são acessados e se há backup e capacidade de recuperação durante uma emergência.

C. Controles críticos de TI e monitoramento contínuo são estabelecidos para mitigar os riscos de segurança da informação (incluindo riscos cibernéticos) e garantir que os dados confidenciais sejam protegidos durante crises, interrupções e emergências. Os controles e o monitoramento contínuo incluem inteligência de ameaças em tempo real e restrição de acesso apenas a usuários autorizados.

D. Os ativos críticos de TI são inventariados. Eles incluem o hardware, o software e os serviços necessários para dar suporte às operações durante crises, interrupções e emergências.

E. São estabelecidos planos de continuidade dos negócios e de recuperação de desastres. Os planos incluem funções definidas para o pessoal designado e para as equipes de recuperação. Os planos são testados periodicamente (por exemplo, um "exercício de mesa"), e os resultados dos testes, inclusive as oportunidades de melhoria, são informados à diretoria e à gerência sênior.

F. É estabelecido um processo para modificar o ambiente de trabalho durante crises, interrupções e emergências. As modificações podem incluir o uso de locais de trabalho alternativos, como trabalhar em casa ou montar um escritório temporário de maneira oportuna e eficiente.

G. Um processo é estabelecido para monitorar e relatar continuamente as ameaças e vulnerabilidades emergentes relacionadas à resiliência organizacional e para identificar, priorizar e implementar oportunidades para melhorar as operações de resiliência organizacional. O processo pode incluir sistemas de denúncia de irregularidades ou coleta de informações sobre riscos.

H. É estabelecido um processo para educar e treinar o pessoal em relação à resiliência organizacional, garantindo que eles estejam cientes das políticas e dos procedimentos a serem seguidos e das ações a

serem tomadas quando ocorrerem crises, interrupções e emergências. O processo inclui exercícios de treinamento nos quais são simulados cenários perturbadores.

I. Um processo é estabelecido para garantir que os recursos humanos, tecnológicos e financeiros necessários sejam orçados e estejam disponíveis durante crises, interrupções e emergências. O processo pode incluir financiamento pré-aprovado.

J. Os recursos financeiros necessários para apoiar a resiliência organizacional são analisados periodicamente e comunicados à diretoria. A análise inclui a avaliação da liquidez, da cobertura de seguro e dos acordos de financiamento de contingência.

K. É estabelecido um processo para analisar crises, interrupções e emergências depois que elas ocorrem e analisar as análises pós-incidente por meio de um processo de lições aprendidas, incluindo a integração das lições no futuro planejamento da resiliência organizacional.

Sobre o Instituto de Auditores Internos

O IIA é uma associação profissional internacional que atende a mais de 265.000 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 em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para obter mais informações, acesse www.theiia.org.

Direitos Autorais

Setembro de 2025