Requisito Temático de terceiros

Public Consultation Draft

O Framework Internacional de Práticas Profissionais (International Professional Practices Framework®) comprehende as Normas Globais de Auditoria Interna (Global Internal Audit Standards™), os Requisitos Temáticos 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.

Terceiros

Um terceiro é um indivíduo, grupo ou entidade externa com quem uma organização tem um relacionamento comercial. Um relacionamento com terceiros pode ser formalizado por meio de um contrato, acordo ou outro meio para fornecer produtos ou serviços à organização. O uso do termo "terceiros" pode variar de acordo com o setor ou outros contextos. Este guia usa o termo "terceiro" para se referir a vendedores ou fornecedores, contratados ou subcontratados, prestadores de serviços terceirizados, outras agências e consultores e inclui acordos entre um terceiro e seus subcontratados, geralmente conhecidos como subcontratados "downstream".

Este Requisito Tópico não se destina a abordar relacionamentos, interesses ou envolvimentos indiretos com a organização principal, como funcionários, parceiros financeiros, reguladores, agentes ou curadores.

Embora a organização principal possa contratar um terceiro para ajudar a atingir um ou mais de seus objetivos comerciais, a organização principal mantém a responsabilidade pelos riscos associados à realização desses objetivos. Se o contrato ou acordo de um terceiro com a organização permitir a subcontratação de uma quarta parte ou de outra parte "a jusante", este Requisito Tópico se aplica ao fornecimento de garantia sobre a governança e a supervisão desses relacionamentos subcontratados também. Nesses casos, os auditores internos devem aplicar todos os requisitos conforme indicado pelos resultados de uma avaliação de riscos. As exclusões devem ser documentadas.

Trabalhar com terceiros introduz riscos que devem ser identificados, avaliados e gerenciados por meio de processos adequados de governança, gerenciamento de riscos e controle, conforme descrito neste Requisito Tópico. Se um terceiro não cumprir o que foi contratado, participar de práticas antiéticas ou sofrer uma interrupção nos negócios, a organização principal poderá sofrer repercussões. Categorias e exemplos de riscos relacionados a terceiros incluem:

- Operacional, como interrupções de serviço ou não atingir os objetivos comerciais.
- Segurança cibernética, como o comprometimento de dados confidenciais.
- Financeiro, como a insolvência do fornecedor.
- Conformidade com os requisitos regulatórios locais, nacionais e internacionais aplicáveis.
- Jurídico, como conflitos de interesse, disputas e litígios por violações de contrato.
- Reputacional, como danos causados ao meio ambiente ou aos clientes, consumidores ou acionistas da organização principal.

O ciclo de vida de terceiros consiste em selecionar, contratar, integrar, monitorar e retirar. Os auditores internos devem considerar essas fases ao avaliar os requisitos dos processos de governança, gerenciamento de riscos e controle.

Avaliação e análise de processos de Governança, gerenciamento de riscos e processos de controle de terceiros

Este requisito tópico fornece uma abordagem consistente e abrangente para avaliar o projeto e a implementação de governança de terceiros, gerenciamento de riscos e processos de controle. Os requisitos representam uma linha de base mínima para essa avaliação em uma organização.

Governança: Avaliação e análise da governança de terceiros

Requisitos:

Os auditores internos devem avaliar os seguintes aspectos da governança de terceiros da organização, incluindo a supervisão do conselho :

A. Uma abordagem formal é estabelecida, implementada e revisada periodicamente para determinar se é necessário contratar um terceiro para ajudar a atingir um objetivo comercial por meio do fornecimento de um produto ou serviço. A abordagem inclui critérios adequados para definir e avaliar os recursos disponíveis para atingir os objetivos.

B. Políticas, procedimentos e processos são estabelecidos para definir, avaliar e gerenciar relacionamentos e riscos com terceiros durante todo o ciclo de vida do terceiro. As políticas, os

procedimentos e os processos estão alinhados com os requisitos regulamentares aplicáveis e são periodicamente revisados e atualizados para fortalecer o ambiente de controle.

C. As funções e responsabilidades de gerenciamento de terceiros dentro da organização são definidas, detalhando quem seleciona, dirige, gerencia, se comunica e monitora terceiros, bem como quem deve ser informado sobre as atividades de terceiros. Existe um processo para garantir que os indivíduos designados para funções e responsabilidades de terceiros tenham o conhecimento, as competências e as habilidades adequadas.
D. Os protocolos de comunicação com as partes interessadas relevantes são definidos e incluem a comunicação do status do desempenho, dos riscos e da conformidade de terceiros priorizados. As partes interessadas relevantes podem incluir a diretoria, a gerência sênior, as operações, o gerenciamento de riscos, os recursos humanos, a segurança das informações, o jurídico, a conformidade, as compras e outros.

GERENCIAMENTO DE RISCOS: Avaliação e análise do gerenciamento de riscos de terceiros

Requisitos:

Os auditores internos devem avaliar os seguintes aspectos do gerenciamento de riscos de terceiros da organização:

A. Os processos de gerenciamento de riscos para terceiros são padronizados e abrangentes, incluem funções e responsabilidades definidas e abordam suficientemente os principais riscos (como financeiros, operacionais, estratégicos, de segurança cibernética, de conformidade, de reputação, éticos, de sustentabilidade, geopolíticos e jurídicos). A adesão aos processos é monitorada e ações corretivas são implementadas para quaisquer desvios.

B. Os riscos relacionados a terceiros em todo o ciclo de vida são identificados e avaliados. A avaliação de riscos é usada para classificar e ordenar terceiros e priorizar as respostas aos riscos. A avaliação é revisada e atualizada periodicamente.

C. As respostas aos riscos são adequadas e precisas, de acordo com a classificação. As respostas aos riscos são implementadas, revisadas, aprovadas, monitoradas, avaliadas e ajustadas conforme necessário.

D. Existem processos para gerenciar e escalonar, se necessário, os problemas que surgem de terceiros, garantindo a responsabilidade pelos resultados e aumentando a probabilidade de cumprir os termos dos contratos ou outros acordos. Se um terceiro não responder às preocupações escaladas, há processos em vigor para remediação, inclusive rescisão.

CONTROLES: Avaliação e análise de processos de controle de terceiros

Requisitos:

Os auditores internos devem avaliar os seguintes controles para terceiros priorizados, incluindo os processos da gerência para avaliação e monitoramento contínuos dos terceiros da organização:

A. Um caso de negócios documentado e aprovado ou outro documento relevante descreve e justifica a necessidade e a natureza do relacionamento com um terceiro.

B. Existe um processo robusto de due diligence para o fornecimento e a seleção de terceiros. O processo inclui critérios para aspectos importantes, como a revisão de protocolos de segurança cibernética, a realização de verificações de antecedentes financeiros e a verificação de dados bancários.

C. A contratação e a aprovação são realizadas de acordo com as políticas, os procedimentos e os processos de gerenciamento de riscos de terceiros da organização e incluem a colaboração com as partes apropriadas da organização.

D. Os contratos ou acordos finais são revisados e aprovados por todas as partes interessadas relevantes, inclusive as áreas jurídica e de conformidade, quando aplicável; assinados por indivíduos autorizados de ambas as partes; e armazenados de forma segura. Todos os contratos são atribuídos a um gerente ou administrador de contratos para responsabilidade.

E. Uma lista precisa, completa e atualizada de todos os relacionamentos com terceiros é mantida, por exemplo, em um sistema centralizado de gerenciamento de contratos.

F. Processos de integração documentados são estabelecidos e seguidos para permitir que terceiros cumpram os termos do contrato ou acordo.

G. Existem processos de monitoramento contínuo para avaliar se os terceiros priorizados atuam de acordo com os termos do contrato ou acordo durante todo o ciclo de vida e cumprem as obrigações contratuais. Os processos incluem a verificação da confiabilidade das informações fornecidas e a reavaliação do desempenho periodicamente e sempre que o contrato for alterado.

H. São estabelecidos protocolos para iniciar ações corretivas caso um terceiro não atenda às expectativas ou represente um risco maior ou inesperado. Os protocolos incluem o escalonamento de incidentes com base na gravidade, a realização de revisões pós-incidente e a análise da causa raiz dos incidentes.

I. As datas de renovação dos contratos são monitoradas, e as ações de renovação são tomadas conforme necessário.

J. Para os terceiros priorizados, é implementado e seguido um plano formalizado de desligamento. Os processos incluem como:
    - Rescindir o terceiro.
    - Substitua o terceiro, se necessário.
    - Reatribuir a custódia e devolver ou destruir os dados confidenciais da organização armazenados
      com o terceiro.
    - Revogar o acesso do terceiro a sistemas, ferramentas e instalações.

Fevereiro de 2025