IPPF

International Professional Practices Framework

Supplemental Guidance

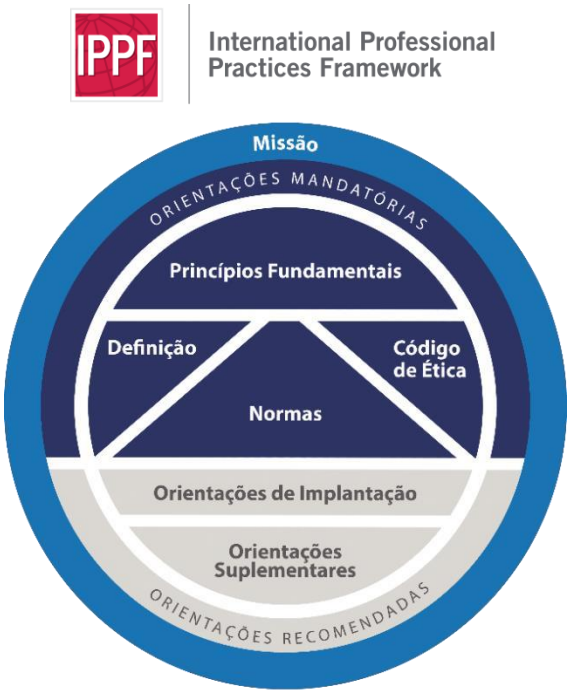
Practice Guide

Desenvolvendo um Plano de Auditoria Interna Baseado em Riscos

The Institute of Internal Auditors | Global

Sobre o IPPF

O *International Professional Practices Framework*® (IPPF®) é o framework conceitual que organiza as orientações fidedignas promulgadas pelo The IIA para profissionais de auditoria interna do mundo.



As **Orientações Mandatórias** são desenvolvidas seguindo um processo de diligência devida estabelecido, que inclui um período de exposição pública para contribuição dos stakeholders. Os elementos mandatórios do IPPF são:

- Princípios Fundamentais para a Prática Profissional de Auditoria Interna.
- Definição de Auditoria Interna.
- Código de Ética.
- Normas Internacionais para a Prática Profissional de Auditoria Interna.

As **Orientações Recomendadas** incluem orientações de implantação e suplementares. As Orientações de Implantação foram desenvolvidas para ajudar os auditores internos a entender como aplicar e estar em conformidade com os requisitos das Orientações Mandatórias.

Sobre as Orientações Suplementares

As Orientações Suplementares fornecem informações adicionais, aconselhamento e práticas recomendadas para a prestação de serviços de auditoria interna. Apoiam as *Normas*, abordando tópicos específicos e questões específicas do setor em mais detalhes do que as Orientações de Implantação, e são endossadas pelo The IIA por meio de processos formais de revisão e aprovação.

Guias Práticos

Os Guias Práticos, um tipo de Orientação Suplementar, oferecem abordagens detalhadas, processos passo-a-passo e exemplos que se destinam a apoiar todos os auditores internos. Guias Práticos específicos concentram-se em:

- Serviços Financeiros.
- Setor Público.
- Tecnologia da Informação (GTAG®).

Para uma visão geral dos materiais de orientação fidedignos oferecidos pelo The IIA, por favor, acesse www.globaliia.org/standards-guidance.

Índice

Sumário Executivo

No ambiente de negócios atual, a auditoria interna eficaz exige um planejamento preciso, combinado com uma resposta flexível às mudanças rápidas dos riscos. Para agregar valor e melhorar a eficácia de uma organização, as prioridades de auditoria interna devem se alinhar aos objetivos da organização e devem abordar os riscos com maior potencial de afetar a capacidade da organização de atingir esses objetivos.

Obs.: O **Anexo A** lista outros recursos do IIA que são relevantes para este guia. Os termos em negrito são definidos no glossário do **Anexo B**.

Garantir esse alinhamento é a essência das Normas 2010 – Planejamento, 2010.A1, 2010.A2 e 2010.C1, que atribuem ao chefe executivo de auditoria (CAE) a responsabilidade de desenvolver um plano de trabalho de auditoria interna com base em uma avaliação de riscos realizada pelo menos anualmente.

Este guia prático descreve uma abordagem sistemática para criar e manter um plano de auditoria interna baseado em riscos. O CAE e os auditores internos designados trabalham juntos para:

- Entender a organização.
- Identificar, avaliar e priorizar os riscos.
- Coordenar com outros fornecedores.
- Estimar recursos.
- Propor um plano e solicitar feedback.
- Finalizar e comunicar o plano.
- Avaliar os riscos continuamente.
- Atualizar o plano e comunicar as atualizações.

A orientação é geral o suficiente para ser aplicada às circunstâncias, necessidades e requisitos de cada organização. Ao aplicar a orientação, os auditores internos devem levar em consideração o nível de maturidade de sua organização, especialmente o grau de integração da governança e do gerenciamento de riscos. Os auditores podem precisar adaptar a orientação às especificidades das indústrias, localizações geográficas e jurisdições políticas em que suas organizações operam.

Introdução

O planejamento abrangente baseado em riscos permite que a atividade de auditoria interna alinhe e concentre adequadamente seus recursos limitados para prestar avaliação e assessoria perspicazes, proativos e focados no futuro nas questões mais prementes da organização. Garantir que as prioridades da auditoria interna sejam baseadas em riscos requer planejamento avançado, e o CAE é responsável por desenvolver um plano de **trabalho** de auditoria interna baseado em uma **avaliação de riscos** realizada pelo menos anualmente (Norma 2010 – Planejamento e Norma 2010.A1).

Embora a avaliação anual de riscos seja o requisito mínimo articulado nas *Normas*, o cenário atual de risco em rápida mudança exige que os auditores internos avaliem os riscos com frequência, até continuamente. Os planos de auditoria interna baseados em riscos devem ser dinâmicos e ágeis. Para alcançar essas qualidades, alguns CAEs atualizam seu plano de auditoria interna trimestralmente (ou um cronograma periódico semelhante), e outros consideram seus planos "contínuos", sujeitos a pequenas alterações a qualquer momento.

Comunicando o Plano Baseado em Riscos

Ao preparar um plano de auditoria interna, o CAE deve pensar em como envolver os stakeholders e criar um plano de auditoria interna que gere o maior valor possível. As considerações incluem:

- Quais tipos de trabalhos de auditoria interna darão à alta administração e ao **conselho** avaliação e assessoria adequadas sobre se os riscos significantes foram mitigados de forma eficaz?
- Como a atividade de auditoria interna comunicará suas avaliações de riscos e o plano de auditoria interna baseado em riscos? Que tipos de representações visuais ajudariam a apoiar uma comunicação eficaz?

Quem É Responsável Pelo Plano de Auditoria Interna Baseado em Riscos?

- Embora o CAE seja responsável pelo plano de auditoria interna, gerentes de auditoria interna experientes e a equipe de auditoria interna podem executar atividades do processo de planejamento. Este guia fala sobre as funções e responsabilidades do CAE, gerentes de auditoria interna, auditores internos e a atividade de auditoria interna como um todo. No entanto, nenhuma abordagem única se ajusta a todas as organizações e as disposições variam de acordo com a organização (p. ex., com base no tamanho e recursos disponíveis para a atividade de auditoria interna).
- As *Normas* expressam requisitos relacionados ao plano de trabalho baseado em riscos do CAE (série 2000) e aos planos de trabalhos individuais (série 2200). Este guia aborda apenas o plano de auditoria interna baseado em riscos do CAE. O Guia Prático "Planejamento do Trabalho: Estabelecendo Objetivos e Escopo" descreve como planejar trabalhos individuais.

- O que a alta administração e o conselho esperam da atividade de auditoria interna? Com antecedência, o CAE deve discutir com a alta administração e o conselho com que frequência esperam receber relatórios e os critérios que justificam reporte e aprovação de alterações ao plano de auditoria (ou seja, importância e urgência das questões), conforme descrito na Norma 2060 – Reportando à Alta Administração e ao Conselho. As políticas e procedimentos de auditoria interna devem tratar de questões de confidencialidade, de acordo com o Código de Ética e as *Normas* (Norma 2040 – Políticas e Procedimentos, a série que começa com a Norma 2330 – Documentando Informações e a série que começa com a Norma 2440 – Disseminação dos Resultados).

Mudando o Plano

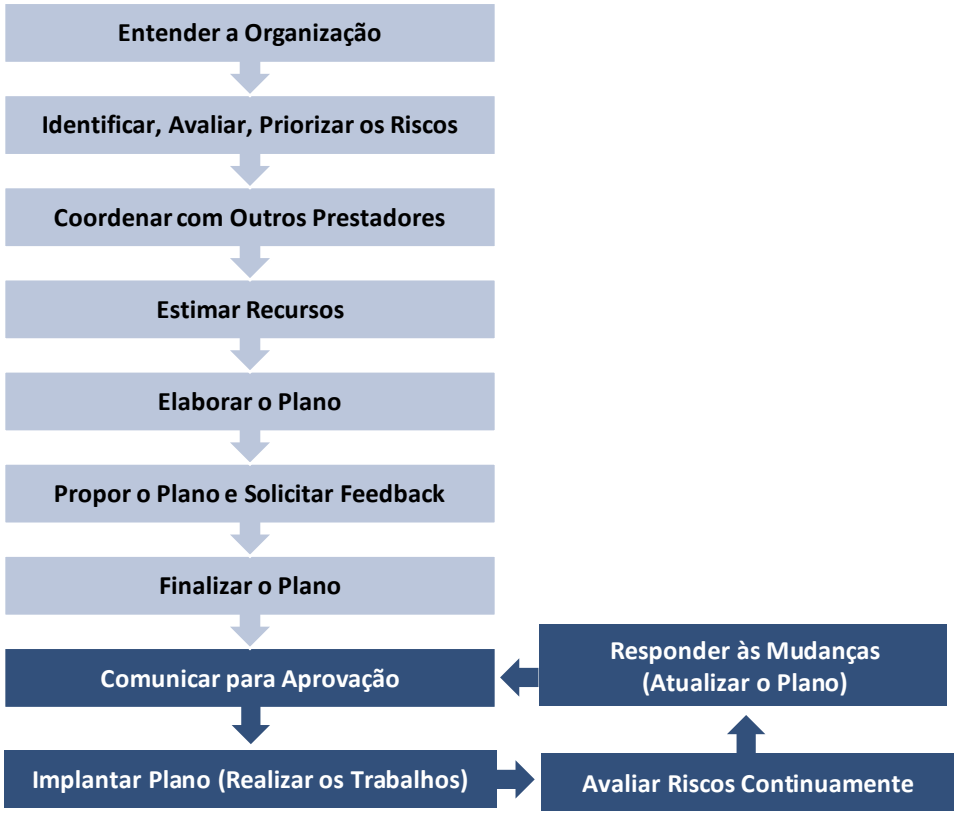
Este guia explica os passos que levam à criação inicial de um plano de auditoria interna, bem como os requisitos para aprovação formal do plano, que podem ocorrer em intervalos programados e predeterminados. Além disso, a atividade de auditoria interna deve responder rapidamente às mudanças internas e externas que afetam os objetivos e prioridades de risco da organização. As organizações e as condições externas estão mudando continuamente, e informações de risco novas ou mais detalhadas podem surgir durante a realização de qualquer trabalho. Os auditores internos e externos podem descobrir novas informações durante um trabalho que demandem alterações na avaliação abrangente da auditoria interna sobre os riscos e no plano de auditoria interna.

Essas mudanças destacam a necessidade de avaliar continuamente os riscos, reavaliar as prioridades de risco e ajustar o plano para acomodar as novas prioridades. A Norma 2010 – Planejamento recomenda que o CAE revise e ajuste o plano em resposta a mudanças nos negócios, riscos, operações, programas, sistemas e controles da organização. As seções posteriores do guia fornecem detalhes adicionais sobre como o CAE deve gerenciar as alterações ao plano.

Visão Geral do Desenvolvimento do Plano de Auditoria

O processo de estabelecimento do plano de auditoria interna geralmente inclui as fases a seguir. No entanto, os leitores devem interpretar livremente o conceito de fases, pois os detalhes do planejamento de auditoria interna variam de acordo com a atividade de auditoria interna e sua organização. Vários auditores internos podem estar trabalhando simultaneamente para preparar o plano de auditoria interna, incluindo a avaliação de riscos que será considerada; assim, algumas das fases podem se sobrepor ocasionalmente. Os CAEs normalmente documentam sua abordagem preferida nas políticas e procedimentos da atividade de auditoria interna (Norma 2040). Este guia desconstrói as fases de planejamento mostradas na Figura 1. Os auditores internos devem ver todo o ciclo preparatório como um esforço abrangente que responde às mudanças organizacionais.

Figura 1: Ciclo de Desenvolvimento do Plano de Auditoria Interna



Entendendo a Organização

Identificando Objetivos, Estratégias e Estrutura

Compreender os processos de gerenciamento de riscos da organização requer identificar como as funções e responsabilidades do gerenciamento de riscos e governança são coordenadas. Normalmente, essa coordenação envolve:

- Implantação de sistemas de controle pela gestão operacional e de linha.
- Prestação de avaliação de que os sistemas de gerenciamento de riscos e controle foram projetados de forma eficaz e estão operando conforme projetado. Gerenciamento de riscos, conformidade, controle de qualidade e funções semelhantes fornecem essa avaliação.
- A prestação de avaliação e assessoria independentes sobre os processos de governança, gerenciamento de riscos e controle pela atividade de auditoria interna.

Revisando os Principais Documentos

Antes de iniciar a avaliação de riscos, o CAE pode revisar os principais documentos organizacionais, como o organograma e o plano estratégico. O CAE pode revisar esses documentos para obter informações sobre os processos de negócios da organização e os possíveis riscos e pontos de controle. Se a gestão implantou ferramentas automatizadas para monitoramento contínuo dos riscos, os auditores internos podem coletar informações a partir dos relatórios de riscos gerados automaticamente. Informações suplementares podem ser extraídas de avaliações e relatórios previamente produzidos por auditores internos e externos. Documentos semelhantes para **unidades auditáveis** individualmente podem detalhar os processos operacionais e as funções de serviços que os apoiam. A Figura 2 lista exemplos de informações e documentos que os auditores internos podem reunir.

Figura 2: Fontes de Documentos para Coleta de Informações

Informações a Coletar	Possíveis Fontes de Documentos
■ Quais funções de controle e avaliação estão operando na organização (isto é, primeira e segunda linhas)? Quais são as responsabilidades de cada um? ■ A organização implantou um framework de gerenciamento de riscos corporativos (ERM)?	■ Organograma. ■ Minutas das reuniões com a alta administração, gestão de segunda linha e comitês de risco.
■ Quais são os principais objetivos, estratégias e iniciativas da organização? ■ Existem grandes iniciativas e projetos de mudança propostos para o próximo período?	■ Plano estratégico da organização. ■ Planos estratégicos para áreas individuais críticas e grandes iniciativas. ■ Minutas das reuniões entre a alta administração e o conselho.
■ Quais são os principais processos de negócios da organização? ■ Quais são os riscos e controles em potencial de cada processo? ■ As estratégias, objetivos e planos são realistas? ■ Todos os riscos relevantes foram capturados?	■ Relatórios anuais e documentos públicos/regulatórios. ■ Registro de riscos de toda a organização (também conhecido como universo de risco).[1] ■ Registros de riscos da gestão (também conhecidos como inventários de risco) e avaliações de riscos, incluindo autoavaliações de riscos e controle realizadas pelos líderes de cada área de negócios (avaliações de riscos operacionais). ■ Resultados do monitoramento automatizado de riscos, se implantado. ■ Avaliações e relatórios anteriores de vários prestadores de avaliação (funções de segunda linha, auditores internos e externos). ■ Documentação operacional detalhada (p. ex., mapas de processos). ■ Relatórios anuais e documentos públicos/regulatórios.

1. Rick A. Wright, Jr., *The Internal Auditor's Guide to Risk Assessment*, 2ª ed. (Lake Mary, FL: Internal Audit Foundation, 2018), 51.

Consultando Principais Stakeholders

O CAE deve consultar os principais stakeholders para cumprir com os requisitos das normas relacionadas à Norma 2010 – Planejamento. A comunicação contínua é vital para permitir ajustes ágeis às mudanças. Além disso, a comunicação contínua ajuda a garantir que a alta administração, o conselho e a atividade de auditoria interna compartilhem um entendimento comum dos riscos e prioridades de avaliação da organização.

Reunindo-se com o Conselho e Comitês de Governança

O CAE deve participar de reuniões com o conselho e os principais comitês de governança (p. ex., comitê de auditoria, comitê de risco) e pode se reunir de forma independente com membros individuais. A participação em tais reuniões ajuda o CAE a aprender sobre as últimas ocorrências na organização e a estar alerta aos riscos potenciais que podem resultar das mudanças.

Reuniões com a Gestão

Além de reunir-se com o conselho, o CAE (ou auditores internos designados) deve participar das reuniões regulares (telefone, web ou pessoalmente) da alta administração e/ou daqueles que reportam diretamente à alta administração (isto é, funções de segunda linha, como conformidade, gerenciamento de riscos e controle de qualidade). O CAE deve falar com os executivos seniores individualmente. Em certos setores ou em indústrias altamente regulamentadas, o CAE também pode se reunir com auditores externos e/ou reguladores.

Consultando com Principais Stakeholders

Stakeholders a Considerar

- Conselho: comitê de auditoria, comitê de risco, comitês de governança, membros individuais do conselho.
- Alta administração, diretor de risco.
- Funções da segunda linha.
- Gestão operacional/de linha.
- Recursos humanos.
- Marketing.
- Funcionários que executam as principais tarefas operacionais.
- Auditores/reguladores externos, conforme indicado (de acordo com a indústria).

Métodos de Comunicação

- Reuniões presenciais.
- Conferências por telefone/online.
- Pesquisas.
- Entrevistas.
- Sessões de brainstorming em grupo, workshops.
- Comunicação contínua e informal.

Para entender melhor os processos de negócios e os desafios para cumprir com as prioridades de negócios, os auditores internos podem se reunir com os principais membros da gestão operacional ou de linha, como vice-presidentes e diretores de cada área de negócios, além de funcionários que executem tarefas operacionais.

Comunicação Informal

As informações obtidas informalmente podem completar o entendimento da auditoria interna sobre a organização, fornecendo detalhes realistas que não são divulgados formalmente. Os relacionamentos geralmente são aprimorados quando auditores internos são designados para trabalhar com linhas de negócios, funções, locais e/ou entidades legais específicas. A interação com a gestão e a equipe nas diversas unidades de negócios e áreas funcionais, incluindo departamentos como recursos humanos e marketing, ajuda a atividade de auditoria interna a construir uma imagem abrangente dos planos e do ambiente de controle da organização.

Interações informais que ocorram consistentemente criam confiança, aumentando a probabilidade da equipe se comunicar abertamente com os auditores internos e levantar preocupações que possam não ser mencionadas em reuniões formais. Essa abertura melhora a capacidade da atividade de auditoria interna de avaliar o ambiente de controle. Rotacionar auditores internos para dentro e fora de tais atribuições equilibra os benefícios da comunicação informal em relação à necessidade de proteger a independência e a objetividade dos auditores internos (Norma 1130 – Prejuízo à Independência ou à Objetividade).

Enquetes, Entrevistas, Brainstorming, Pesquisa

Outras ferramentas para obter informações incluem pesquisas, entrevistas e workshops em grupo (p. ex., sessões de brainstorming e grupos de foco). Essas ferramentas são especialmente úteis para identificar riscos emergentes e de fraude.

O CAE e os membros da atividade de auditoria interna também podem aumentar sua conscientização sobre riscos potencialmente emergentes pesquisando notícias, tendências e mudanças regulatórias na indústria; ao fazer networking com outros profissionais; e buscar educação continuada relevante.

As questões a serem consideradas incluem:

- Como os 10 principais objetivos da organização se relacionam com os principais objetivos departamentais?
- Quais estratégias são usadas para atingir esses objetivos?
- Quais riscos, se ocorrerem, podem interferir na capacidade da organização de atingir esses objetivos?

Fontes de Informações Sobre Riscos Emergentes

- Alterações nas prioridades de gerenciamento, processos de negócios, tecnologia (TI) e operações.
- Ética/sistema de denúncia de riscos de fraude.
- Acontecimentos geopolíticos.
- Mudanças legais e regulatórias.
- Solicitações da alta administração e do conselho.
- Novos projetos e programas de mudança.
- Avaliações de riscos anteriores da gestão e da atividade de auditoria interna (incluindo fraude, TI e controles financeiros).

Criando ou Revisando o Universo de Auditoria

Depois de identificar as principais estratégias e objetivos, o CAE pode querer criar ou revisar o universo de auditoria, que é uma lista ou catálogo de todas as unidades potencialmente auditáveis em uma organização. As unidades auditáveis podem ser qualquer "tópico, assunto, projeto, departamento, processo, entidade, função ou outra área que, devido à presença de risco, possa justificar um trabalho de auditoria".

Um universo de auditoria simplifica a identificação e avaliação de riscos em toda a organização. É um passo em direção à descoberta de quais unidades auditáveis têm níveis de risco que justifiquem uma revisão adicional em trabalhos dedicados de auditoria interna. O **Anexo C** oferece um exemplo de uma planilha usada para vincular objetivos organizacionais e iniciativas estratégicas a categorias no universo de auditoria.

Se não existe universo de auditoria, os auditores internos começam com seu entendimento de como a organização vê e categoriza suas atividades, riscos e controles, e como obtém avaliação sobre seus processos de gerenciamento de riscos e controle. Isso inclui considerar quaisquer frameworks usados pela organização. O uso da estrutura que mais se alinha à abordagem da gestão maximizará a sinergia entre a atividade de auditoria interna e outros prestadores internos de **serviços de consultoria** e avaliação, especialmente se a organização tiver implantado um processo de gerenciamento de riscos corporativos (ERM). Um universo de auditoria bem organizado aumenta a probabilidade de que a avaliação de riscos e o plano de auditoria da auditoria interna sejam úteis e valiosos para a organização.

Garantindo a Integralidade do Universo de Auditoria

Para garantir a integralidade do universo de auditoria, o CAE deve considerar as seguintes fontes de informações de risco:

- Estratégia da organização e cadeia de criação de valor.
- Todas as principais áreas, unidades, departamentos e projetos, e suas estratégias, objetivos e processos (em alto nível, a partir do organograma, framework legal e/ou ERM).
- Prestadores terceiros (de funções legais, de compras ou de gestão de contratos).
- Processos e subprocessos de todas as principais funções (das atividades de mapeamento de processos, como as exigidas pela ISO).
- Principais aplicativos de TI e ativos de sistemas de informação, incluindo hardware, software e as informações que eles contêm (da gestão de TI).
- Requisitos de conformidade regulatória e legal que se aplicam à organização.
- Indicadores de desempenho não financeiro (p. ex., ambiental, saúde e segurança, social, governança).

Garantir que o universo de auditoria capture todos os riscos é um desafio, porque existem alguns riscos na interface entre as unidades organizacionais ou entre a organização e o ambiente externo. Observar o universo de auditoria pelos processos de negócios geralmente ajuda a revelar

esses riscos. A barra ao lado “Garantindo a Integralidade do Universo de Auditoria” lista as fontes de informações de risco que os CAEs devem considerar.

O CAE deve consultar a alta administração para garantir que o universo reflita com precisão o modelo de negócios da organização. Uma vez que um universo de auditoria tenha sido construído, ele poderá ser usado para uso futuro. No entanto, o universo deve ser atualizado com frequência para incorporar mudanças internas e externas nos negócios, que podem introduzir novos riscos a qualquer momento. O universo de auditoria ajuda a organizar as áreas auditáveis para uma avaliação abrangente dos riscos e da cobertura de avaliação.

Avaliação de Riscos da Auditoria Interna

Entendendo a Importância da Avaliação Independente

Essa avaliação de riscos de toda a organização permite que o CAE se concentre nos riscos que se classificam entre os mais significantes e identifique trabalhos gerenciáveis, tempestivos e de valor agregado, que reflitam as prioridades da organização. Isso normalmente resulta em um plano que aborda em média cerca de 15 unidades auditáveis.

As organizações que implantaram o ERM podem ter criado um registro abrangente de riscos (também conhecido como inventário ou universo de riscos). Os auditores internos podem usar as informações da gestão como fonte para a avaliação de riscos da auditoria interna sobre toda a organização. No entanto, alinhados ao princípio da objetividade do Código de Ética e à Norma 1100 – Independência e Objetividade, os auditores internos devem fazer seu próprio trabalho para validar que todos os principais riscos tenham sido documentados e que o significado relativo dos riscos seja refletido com precisão.

Entendendo os Objetivos, Estratégias e Riscos de Negócios

Riscos Relativos aos Objetivos de Negócios

Para identificar riscos críticos ou principais, a atividade de auditoria interna deve identificar e entender não apenas os objetivos e estratégias organizacionais de alto nível, mas também os objetivos de negócios específicos e as estratégias usadas para atingi-los. Algumas organizações podem categorizar os objetivos de negócios em nível estratégico, funcional ou de processo.[2] Outros podem usar as categorias de objetivos identificadas em *Controle Interno – Estrutura Integrada*, do *Committee of Sponsoring Organizations* (COSO): operações, reporte e conformidade.

Alavancando a Oportunidade

Os frameworks contemporâneos de gerenciamento de riscos e governança enfatizam a importância de alavancar oportunidades para garantir inovação, crescimento e viabilidade financeira.

O framework de ERM do COSO define oportunidade como uma "ação ou ação potencial que cria ou altera metas ou abordagens para criar, preservar e realizar valor".

2. Wright, T*he Internal Auditor’s Guide*, 60.

Riscos Incluem Oportunidades

Os auditores internos devem considerar a natureza multifacetada dos riscos ao decidir como identificá-los e avaliá-los. Como cada organização possui suas próprias estratégias e objetivos de negócios, não existe um checklist único de riscos para cada organização; os inventários de risco variam de acordo com a organização e mudam com o tempo.

Além disso, os auditores internos devem considerar que "os riscos representam as barreiras para atingir com êxito os objetivos, bem como as oportunidades que podem ajudar a atingir esses objetivos". De fato, "os riscos podem estar relacionados à prevenção de coisas ruins (redução de riscos) ou a não garantir que as coisas boas aconteçam (isto é, explorar ou buscar oportunidades)".

Documentando Riscos

Categorias de Riscos

Cada unidade ou função de negócios da organização pode ter uma maneira diferente de visualizar e mensurar objetivos, processos e riscos de negócios. A criação de categorias de risco introduz confiabilidade e consistência em toda a organização, ao identificar, comunicar e analisar riscos e os processos de gerenciamento de riscos.

Frameworks, abordagens e setores específicos podem recomendar ou exigir o uso de determinadas categorias de risco. Se a organização usa um framework de gerenciamento de riscos, a atividade de auditoria interna deve alinhar suas categorias com as do framework. Se não houver framework ou categoria de risco, os auditores internos podem debater com a gestão os riscos relevantes para a organização, começando com uma taxonomia de categorias de risco comuns à maioria das organizações, como riscos estratégicos, operacionais, de conformidade e financeiros.[3]

Riscos Internos, Externos e Estratégicos

Dentro de cada categoria ampla, os auditores internos consideram fontes internas e externas de risco, o que gera uma lista extensa. Os auditores internos avaliarão esses riscos para restringir a lista e priorizarão os que devam ser incluídos no planejamento da auditoria interna. Os **riscos estratégicos**, se não forem gerenciados devidamente, têm o maior potencial de afetar a capacidade da organização de atingir seus objetivos.[4]

Riscos de TI

Um plano abrangente de auditoria interna inclui a TI, o que significa que os riscos de TI devem ser incluídos na avaliação geral dos riscos. Os riscos de TI podem ser classificados em subcategorias, incluindo infraestrutura, operações e aplicativos, e nem sempre estão vinculados a um único processo de negócios específico. Praticamente toda atividade comercial depende, até certo ponto, da tecnologia. A tecnologia apoia processos de negócios e geralmente faz parte do controle de processos. Com a crescente automação dos processos de controle interno, as deficiências no suporte às tecnologias podem afetar significativamente as operações e os objetivos de negócios da organização.

3. Wright, *The Internal Auditor's Guide*, 13.
4. Wright, *The Internal Auditor's Guide*, 21.

De acordo com a Norma 2110.A2, a atividade de auditoria interna deve avaliar se a **governança da tecnologia da informação** — que é sua liderança, estruturas organizacionais e processos — apoia as estratégias e objetivos da organização. A compreensão do plano estratégico de TI deve ajudar os auditores internos a identificar como a TI apoia a organização para implantar suas estratégias e atingir seus objetivos.

A atividade de auditoria interna deve avaliar a flexibilidade da estratégia de TI — como sua capacidade de apoiar o crescimento futuro da organização — e a capacidade de resposta dos processos de gerenciamento de riscos e controle de TI para prevenir, detectar e responder a ameaças de cibersegurança.

Riscos Ambientais, Sociais e de Governança

Investidores, consumidores e o público esperam que as organizações mensurem e reportem seus esforços ambientais, sociais e de governança (*environmental, social and governance* – ESG). Como parte de suas decisões de investimento, os investidores buscam cada vez mais divulgações não regulatórias sobre questões de ESG; seja em relatórios de sustentabilidade independentes, declarações públicas sobre o gerenciamento de riscos não financeiros em registros financeiros ou declarações diretamente a outros stakeholders (agências de classificação). Os relatórios não financeiros podem afetar a reputação de uma organização perante investidores, parceiros de negócios e possíveis funcionários.

Os requisitos ambientais e os riscos de conformidade aplicam-se à cadeia de suprimentos, produtos e serviços. A fraude ambiental, como desobedecer às normas de emissões, está recebendo não apenas atenção regulatória, mas também maior escrutínio público. Os riscos sociais envolvem o impacto que uma organização tem sobre funcionários, clientes, fornecedores e comunidades. Manter relacionamentos positivos com esses stakeholders sustenta a confiança do público na organização. Os riscos de governança estão relacionados a estratégias, políticas e supervisão em relação à sustentabilidade, estrutura e composição do conselho, remuneração dos executivos, lobby político, suborno, corrupção e fraude.

Os auditores internos devem participar do diálogo de ESG da organização e entender seus esforços de ESG, especialmente como esses esforços se alinham às expectativas dos stakeholders. Nas organizações que não possuem critérios e relatórios de ESG, a atividade de auditoria interna tem a oportunidade de ajudar a organização a aumentar sua conscientização de ESG. Critérios e métricas eficazes de ESG, combinados com um processo para monitorar e verificar os dados de ESG da organização, compõem um processo de controle importante sobre os relatórios de ESG. Organizações globais, incluindo as Nações Unidas, a *Organisation for Economic Co-operation and Development* e o *Sustainability Accounting Standards Board* fornecem critérios de ESG mensuráveis e informações detalhadas sobre riscos, oportunidades e reporte de ESG.

Riscos de Terceiros

Algumas estruturas, processos e aplicativos organizacionais podem existir, pelo menos em parte, em um ambiente virtualizado e/ou com prestadores terceiros de serviços. A revisão da atividade de auditoria interna deve considerar os riscos associados aos prestadores terceiros de serviços nos quais a organização confia (p. ex., serviços de armazenamento na nuvem e sistemas de gestão

de dados). O Guia Prático do IIA "Auditando o Gerenciamento de Riscos de Terceiros" fornece informações úteis sobre a avaliação de riscos de terceiros.

Riscos de Fraude

A atividade de auditoria interna é responsável por avaliar os processos de gerenciamento de riscos da organização e sua eficácia, incluindo aqueles relacionados a riscos de fraude (2120.A2). Como novos riscos de fraude podem surgir a qualquer momento, os auditores internos também devem avaliar os riscos de fraude ao planejar cada trabalho de avaliação (Normas 2210.A1 e 2210.A2). O brainstorming com vários stakeholders da organização é uma parte vital da avaliação dos riscos de fraude, porque atividades fraudulentas envolvem contornar os controles existentes. Muitos CAEs realizam uma avaliação independente e dedicada dos riscos de fraude. Qualquer informação descoberta através de qualquer um desses processos deve ser incorporada à avaliação abrangente de riscos e ao plano de auditoria interna. O Guia Prático do IIA "Planejamento do Trabalho: Avaliando Riscos de Fraude" oferece uma abordagem sistemática para avaliar riscos de fraude.

Abordagens de Avaliação de Riscos

Alguns métodos comuns para identificar, documentar e avaliar riscos são a “abordagem de risco específico”, “abordagem de risco por processo” e “abordagem de **fator de risco**”. Os CAEs podem personalizar sua abordagem para a avaliação de riscos em toda a organização e muitos usam uma híbrida (ou seja, uma combinação de abordagens). O feedback da alta administração e do conselho (e comitês relevantes de cada um) deve ser levado em consideração ao selecionar uma abordagem e critérios para a avaliação abrangente dos riscos.

As avaliações de riscos normalmente incluem metodologias quantitativas e qualitativas. Uma grande variedade de programas de software está disponível para ajudar a atividade de auditoria interna a realizar avaliações de riscos que resultem em dados quantitativos e qualitativos.

Uma abordagem de risco específico pode ser considerada *bottom-up*, porque envolve a identificação de riscos associados a cada unidade auditável específica no universo da auditoria. Os riscos são identificados em relação aos objetivos de negócios, normalmente através de reuniões com a gestão relevante especificamente para esse fim. Com base nos critérios combinados (p. ex., impacto, probabilidade), as pontuações de risco compostas são calculadas para as unidades auditáveis individuais. Essa abordagem é frequentemente usada para avaliações de riscos relacionadas a trabalhos de auditoria individuais, mas pode se tornar complicada quando estendida ao nível organizacional, onde o número de unidades e riscos auditáveis se torna bastante grande. Uma versão simples dessa abordagem é mostrada no **Anexo D.**

Uma abordagem de risco por processo é semelhante a uma abordagem de risco específico. Os auditores internos e a gestão começam considerando os processos de negócios de toda a organização como unidades auditáveis. Os principais riscos são mapeados para cada processo. Além disso, os auditores internos trabalham para determinar quais processos desempenham papéis importantes no atingimento dos objetivos e a eficácia com que os riscos a esses processos são gerenciados. Os processos de maior grau de risco residual são priorizados para inclusão no plano de auditoria interna.[5]

5. Anderson, *Internal Auditing: Assurance and Advisory Services,* 120.

Uma abordagem de fator de risco é considerada *top-down*, porque analisa condições de alto nível comuns à maioria das unidades auditáveis. Essa abordagem é comumente usada ao executar uma avaliação de riscos abrangente de toda a organização, pois fornece uma visão de nível macro. Os auditores internos identificam os fatores comuns a todas as unidades auditáveis que afetam a capacidade da organização de atingir seus objetivos. Os fatores de risco não são os próprios riscos, mas condições que provavelmente estão associadas à presença de um risco; isto é, condições que indicam uma maior probabilidade de consequências significativas de risco.

A lista potencial de fatores de risco pode se tornar grande, complicando o processo de avaliação de riscos. Os CAEs podem simplificar, agrupando os fatores em categorias, como estratégicos, de conformidade, operacionais e financeiros. Em algumas organizações, a alta administração e o conselho podem aconselhar a atividade de auditoria interna sobre os fatores de risco que acreditam ser mais relevantes. Alguns fatores de risco podem estar vinculados a várias categorias. No entanto, a categorização dos fatores de risco pode ser conveniente ao resumir a avaliação de riscos para a alta administração e o conselho.

Exemplos de fatores de risco e categorias de fatores de risco incluem:

- Nível relativo de atividade (p. ex., número de transações).
- Materialidade (magnitude da receita ou despesa).
- Liquidez dos ativos envolvidos.
- Impacto sobre a marca (percepção do público, reputação).
- Falha no cumprimento das metas.
- Competência gerencial, desempenho, rotatividade.
- Deficiências conhecidas (resultados de trabalhos anteriores insatisfatórios).
- Grau de mudança nos sistemas, políticas, procedimentos, contratos, relacionamentos.
- Suscetibilidade a fraude.
- Complexidade das operações.
- Grau de confiança em terceiros.
- Força dos controles internos, ambiente de controle.
- Grau de envolvimento regulatório, preocupações com conformidade.
- Tempo desde a última avaliação ou auditoria.[6]

O **Anexo E** fornece um exemplo de avaliação de riscos usando a abordagem de fator de risco.

Mensurando Riscos

Risco Inerente

Em suas avaliações de riscos, os auditores internos devem estimar o risco inerente — o risco que existe se nenhum controle estiver em vigor — e o risco residual. A distinção é importante, porque a gestão tende a pensar principalmente em termos de risco residual, mas os auditores internos precisam considerar se as técnicas de mitigação de riscos foram criadas e funcionam com eficácia.

6. Wright, *The Internal Auditor's Guide*, 68 e 98.

As avaliações de riscos da auditoria interna começam considerando o risco inerente, a combinação de riscos internos e externos em seu estado puro e não controlado.

Estratégias de Gerenciamento de Riscos e Risco Residual

Risco residual, ou risco líquido, é a parte do risco inerente que permanece após a gestão executar suas estratégias de gerenciamento de risco.[7] Com a ajuda da gestão, os auditores internos identificam as estratégias de gerenciamento de riscos e os processos de controle e os convertem em termos operacionais, ou mensuráveis, para ajudar a determinar o risco residual. O CAE ou os auditores internos designados devem documentar os motivos de sua determinação do risco residual. Essa lógica dá suporte à visão da auditoria interna das prioridades de risco, o que é especialmente importante nos casos em que o julgamento da auditoria interna possa estar em conflito com uma interpretação estrita dos resultados da classificação de risco.

A classificação do risco associado a cada unidade permite que o CAE priorize a cobertura de auditoria interna dessa unidade.[8] A mensuração geralmente exige a padronização da terminologia, definições e especificações de todo o universo da auditoria (p. ex., classificações de risco, materialidade, etc.). Essa padronização pode envolver o alinhamento com o framework de gerenciamento de riscos da organização, se houver.

Classificações de Impacto e Probabilidade

Impacto e probabilidade são duas métricas reconhecidas na definição de risco do IIA. Além disso, o CAE pode considerar ou incluir outras métricas de impacto ou gravidade, como as reconhecidas no Framework do COSO ERM (ou seja, adaptabilidade, complexidade, persistência, capacidade de recuperação e velocidade). As classificações de risco podem ser numéricas (p. ex., escala de 1 a 3 ou 1 a 5) ou categóricas (p. ex., classificações de impacto podem ser insignificante, material e extremo; e as classificações de probabilidade podem ser baixa, moderada e alta).

Independentemente do formato escolhido, cada métrica deve ser definida por critérios específicos. Por exemplo, os critérios de impacto podem incluir critérios legais, de conformidade/regulatórios, de reputação, operacionais e materialidade nos critérios financeiros (valor em que o impacto sobre a receita pode afetar o atingimento dos objetivos organizacionais). Os critérios para definir a probabilidade incluem a eficácia do controle e a complexidade dos processos operacionais.

Exemplos de escalas de impacto e probabilidade com critérios aparecem no **Anexo D**. As classificações de impacto e probabilidade são combinadas para criar uma classificação de risco abrangente, representando a significância geral de cada risco em cada unidade/área auditável.

Fatores de Risco e Pontuação Total de Risco

Fatores de risco são elementos que geralmente aumentam o impacto ou a probabilidade de risco para a unidade auditável relacionada e, na abordagem de fator de risco, as classificações de risco são atribuídas aos próprios fatores de risco, e não ao nível de impacto ou probabilidade. No entanto, os fatores podem ser agrupados por sua influência sobre o impacto ou a probabilidade.

7. Anderson, *Internal Auditing*, 487.
8. Wright, *The Internal Auditor's Guide*, 85.

Ponderação, pontuação total de risco – Alguns fatores são mais significantes para atingir objetivos do que outros e, portanto, podem ser ponderados (numericamente). Cada unidade auditável é classificada em cada fator de risco e as classificações de fator de risco são agregadas para criar uma pontuação de risco agregada única para a unidade auditável, denominada pontuação de risco total. Essa pontuação fornece uma base de comparação para priorizar ou classificar unidades auditáveis.

Cálculos regulamentados – Em certas indústrias, os reguladores podem determinar um framework de risco específico, com um modelo e/ou metodologia formal de classificação de risco.[9] O CAE pode se referir às classificações de risco da gestão como mensuradas em relação ao framework e, em seguida, o CAE pode opinar se a atividade de auditoria interna concorda ou discorda da classificação de risco da gestão.

As categorias e fatores de risco devem ser revisados e atualizados periodicamente, para garantir que sejam apropriados ao tamanho e complexidade da organização. As evidências da revisão devem ser mantidas com outros registros de planejamento de auditoria interna.

Mapa de Calor

Os resultados da avaliação de riscos com níveis de risco para cada unidade auditável podem ser representados graficamente em um mapa de calor ou gráfico semelhante, para ajudar a mostrar a classificação das prioridades. Os mapas de calor são especialmente úteis quando determinados critérios são mais pesados do que outros e em apresentações visuais para o conselho e a alta administração.

Validando a Avaliação de Riscos com a Gestão

A atividade de auditoria interna considera a contribuição dos stakeholders durante todo o processo de desenvolvimento do plano de auditoria interna, e esse feedback informa a avaliação de riscos da atividade de auditoria interna. Ao mesmo tempo, a atividade de auditoria interna deve permanecer independente e objetiva — imparcial em relação à gestão — inclusive em sua avaliação de riscos. Os CAEs devem se reunir com a alta administração para revisar a avaliação da auditoria interna, garantir precisão e compreensão mútua e discutir os motivos de quaisquer diferenças significativas nas percepções ou classificações de risco. Os CAEs podem responder pelo nível de conscientização de risco da gestão, representando-o como um fator de risco e adicionando ou subtraindo pontos da pontuação total de risco para aumentar ou diminuir a significância relativa do risco em relação a uma unidade auditável.

9. Por exemplo, na indústria bancária americana, nove categorias de risco devem ser consideradas e classificadas para cada área de trabalho ou processo sob revisão.

Considerações Adicionais de Planejamento

Acomodando Pedidos da Gestão e do Conselho

A alta administração e/ou o conselho podem solicitar serviços de avaliação e consultoria, e o CAE deve atender a essas solicitações. Serviços de consultoria/assessoria podem ser solicitados em áreas ou processos que não apareceram entre as principais prioridades na avaliação de riscos; frequentemente, são oportunidades para a atividade de auditoria interna fornecer conselhos que reduzirão a probabilidade de ocorrência de riscos no futuro. Por exemplo, pode-se solicitar que os auditores internos determinem a causa raiz de uma auditoria externa falha ou revisem a implantação de um novo processo ou tecnologia.

Assim, muitos CAEs reservam uma porcentagem de seu plano de auditoria para realizar trabalhos de consultoria solicitados, bem como trabalhos *ad hoc* que surjam entre o momento da avaliação de riscos e o das revisões do plano. Os investimentos em recursos de auditoria interna em trabalhos de consultoria devem ser registrados no orçamento e no plano de auditoria interna.

Requisitos do IPPF para o Plano

Norma 2010.A2 – O chefe executivo de auditoria deve identificar e considerar as expectativas da alta administração, do conselho e de outros stakeholders em relação às opiniões e outras conclusões da auditoria interna.

Norma 2010.C1 – O chefe executivo de auditoria deveria considerar aceitar trabalhos de consultoria propostos, de acordo com o potencial desses trabalhos de melhorar o gerenciamento dos riscos, agregar valor e melhorar as operações da organização. Os trabalhos aceitos devem ser incluídos no plano.

Frequência e Momento do Trabalho

Nem todas as áreas auditáveis podem ser revisadas em todos os ciclos de auditoria, nem deveriam. Idealmente, a frequência da auditoria é baseada na avaliação de riscos. Os CAEs devem considerar quais trabalhos melhoram a capacidade da organização de atingir seus objetivos e quais têm o potencial de agregar mais valor.

Determinando a Frequência com Base no Risco

Em um plano de auditoria interna puramente baseado em riscos, os CAEs podem aplicar uma das duas estratégias para chegar à frequência ideal dos trabalhos planejados.

1. O plano de auditoria pode se basear em uma avaliação contínua de riscos, sem uma frequência predefinida para os trabalhos. Dada a taxa acelerada de mudança no cenário de risco atual, muitas organizações estão implantando a auditoria contínua, o que lhes permite responder de forma ágil e dinâmica às mudanças ao longo do ano, fazendo alterações periódicas no plano de auditoria conforme necessário. Esses planos de auditoria são identificados como "contínuos", "fluidos" e/ou "dinâmicos".

2. A frequência da auditoria é baseada no nível de risco residual determinado na avaliação de riscos. Por exemplo, as unidades auditáveis classificadas como de alto risco podem ser auditadas pelo menos anualmente (ou uma vez a cada 12 a 18 meses), as classificadas com um nível moderado de risco programado podem ser revisadas a cada 19 a 24 meses e as classificadas como de baixo risco poderiam ser auditadas apenas uma vez a cada 25 a 36 meses (ou poderiam não ser auditadas).

Para garantir que o plano de auditoria interna cubra todos os trabalhos obrigatórios e baseados em riscos, os auditores internos devem considerar:

- Trabalhos exigidos por lei ou regulamentos.
- Trabalhos críticos.
- O tempo e os recursos necessários para trabalhos obrigatórios e prioridades baseadas em riscos.
- Se todos os riscos significantes têm cobertura suficiente pelos prestadores de avaliação.
- A porcentagem do plano que deve ser reservada para projetos especiais, consultoria ou solicitações *ad hoc*.

Frequência Cíclica em Indústrias Altamente Regulamentadas

Em algumas indústrias, como serviços financeiros, as organizações estão sujeitas a regulamentos que exigem que estabeleçam um universo de auditoria/risco, pontuações de risco e classificações de risco, e mantenham um ciclo mínimo de auditoria. Mesmo que o risco inerente de não conformidade seja pequeno, esses trabalhos devem ser incluídos no universo de auditoria, para garantir o desempenho da atividade de auditoria interna com *due diligence* e competência profissional.

Quando a lei, regulamento ou as normas da indústria exigem que determinados trabalhos sejam realizados ciclicamente, o CAE pode elaborar planos de auditoria plurianuais para documentar o momento e quaisquer recursos especializados ou adicionais que possam ser necessários. Além de coordenar as informações coletadas, os auditores internos devem trabalhar com auditores externos para sincronizar o cronograma dos trabalhos, a fim de garantir uma disrupção mínima das operações da organização.

Embora esses trabalhos cíclicos sejam necessários, eles competem por recursos com trabalhos priorizados pelo nível de risco. Até certo ponto, podem parecer conflitar com o conceito de auditoria baseada em riscos, especialmente quando a atividade de auditoria interna e a gestão estabeleceram processos para gerenciar riscos e prestar avaliação sobre as áreas de risco exigidas.

Para enfrentar esse desafio, os CAEs podem:

- Reduzir o escopo de trabalhos obrigatórios, abordando áreas necessárias sem investir além do requisito mínimo.
- Estender o cronograma do plano de longo prazo (para sete anos, por exemplo) para contabilizar trabalhos obrigatórios, enquanto avalia continuamente os riscos e ajusta os planos de curto prazo com mais frequência, para priorizar trabalhos vinculados a riscos significantes.
- Coordenar e confiar em outros prestadores de avaliação.

Embora os trabalhos cíclicos sejam uma entrada de dados no plano de auditoria interna, os CAEs devem ter cuidado para não confiar muito em seus planos de longo prazo diante do cenário atual de risco em rápida mudança. Quando os planos plurianuais são estabelecidos, o ano atual deve ser planejado com alguns detalhes, revisado pelo menos trimestralmente e modificado conforme apropriado.

Estimando Recursos

O CAE deve determinar os recursos necessários para implantar o plano. Os recursos podem incluir pessoas (p. ex., horas e habilidades de trabalho), tecnologia (p. ex., ferramentas e técnicas de auditoria), momento/cronograma (disponibilidade de recursos) e financiamento. O CAE deve estimar o escopo dos trabalhos e as habilidades, tempo e orçamento necessários para realizá-los. O CAE pode refletir sobre a natureza e complexidade de cada trabalho, os recursos gastos em trabalhos comparáveis realizados anteriormente e a data da auditoria mais recente da área ou processo.

Avaliando Habilidades

A Norma 2030 descreve "recursos apropriados" em termos de conhecimento, habilidades e competências. A competência da atividade de auditoria interna recebe atenção significativa nas *Normas* e é um dos quatro princípios do Código de Ética do IIA.

Como parte do planejamento da auditoria interna, os CAEs devem conhecer as competências da equipe de auditoria interna. Os CAEs podem elaborar e manter um inventário das habilidades e conhecimentos especializados de cada auditor, juntamente com uma referência de habilidades necessárias para atender às expectativas, necessidades e demandas da organização e da indústria. Algumas indústrias altamente regulamentadas podem até fornecer uma lista de habilidades mínimas esperadas e exigir que a análise de habilidades seja realizada regularmente.

A referência de benchmarking estabelecida pode ser ajustada para identificar as habilidades específicas necessárias para executar o plano de auditoria interna. O CAE deve alinhar o inventário de habilidades presentes entre a equipe de auditoria interna com as necessárias para atender às expectativas e realizar os trabalhos no plano.

Requisitos para Recursos de Auditoria Interna

Norma 2030 – Gerenciamento de Recursos

O chefe executivo de auditoria deve assegurar que os recursos de auditoria interna sejam apropriados, suficientes e aplicados de forma eficaz para o cumprimento do plano aprovado.

Interpretação:

O termo "apropriado" refere-se à combinação de conhecimentos, habilidades e outras competências necessários para executar o plano. O termo "suficiente" refere-se à quantidade de recursos necessária para cumprir com o plano. Os recursos são "aplicados de forma eficaz" quando são utilizados de forma a otimizar o cumprimento do plano aprovado.

Coordenando com Outros Prestadores de Serviços de Avaliação e Consultoria

A atividade de auditoria interna agrega o máximo de valor ao prestar serviços de avaliação e consultoria onde há o maior risco residual. Entretanto, em organizações maduras e altamente regulamentadas, algumas áreas de alto risco podem ser controladas com eficácia pela primeira linha e podem ter cobertura de avaliação suficiente fornecida pela segunda linha, como funções de gerenciamento de riscos e conformidade, além de cobertura adicional por auditores externos. O *chief information officer* ou o *chief information security officer* da organização pode avaliar os riscos de TI e a atividade de auditoria interna pode corroborar os resultados.

Para fazer o melhor uso dos valiosos recursos, o CAE deve coordenar atividades, compartilhar informações e considerar confiar no trabalho de outros prestadores internos e externos de serviços de avaliação e consultoria (Norma 2050 – Coordenação e Confiança). Contar com o trabalho de outros prestadores, em vez de repetir a cobertura, minimiza a duplicação de trabalho e maximiza a eficiência com que a avaliação é prestada.

Mapas de Avaliação

Um mapa de avaliação documenta a coordenação da cobertura de avaliação. Ele lista todas as categorias de risco significantes e as vincula a fontes relevantes de avaliação. Com base nas informações compiladas, o grau ou nível de cobertura de avaliação fornecida pode ser classificado como adequado ou inadequado, e as lacunas e duplicações se tornam claras.

A criação de um mapa de avaliação envolve os vários prestadores de avaliação que colaboram de uma perspectiva holística em toda a organização. Identificar onde o trabalho de outros prestadores se sobrepõe à cobertura da auditoria interna ajuda a justificar a decisão do CAE sobre quais trabalhos incluir e excluir do plano de auditoria interna. O mapa também fornece evidências claras de lacunas na avaliação, onde possam ser necessários recursos adicionais.

Aprenda Sobre os Mapas de Avaliação

O Guia Prático do IIA "Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação" fornece orientações detalhadas e recomendadas, com exemplos para criar e usar mapas de avaliação.

Suprindo a Demanda por Habilidades Adicionais

Se a atividade de auditoria interna não possuir o conhecimento ou as habilidades necessárias para concluir um trabalho específico de avaliação, o CAE poderá solicitar a um especialista de dentro da organização que forneça conhecimento técnico e traga simultaneamente novos conhecimentos à equipe de auditoria interna.

Outras opções incluem o *co-sourcing*, onde especialistas de fora da organização realizam trabalho especializado sob a supervisão de um auditor interno experiente, e a terceirização, onde o trabalho é realizado inteiramente por uma empresa externa. O CAE deve contabilizar esses acordos de estruturação de equipe no orçamento do plano.

Calculando Horas no Plano

Para calcular as horas "disponíveis" dos recursos de auditoria interna, o CAE calcula o número total de horas que cada membro da equipe de auditoria interna pode contribuir para a conclusão do plano de auditoria em um determinado período (normalmente, um ano). O total de horas disponíveis leva em consideração os resultados da avaliação de habilidades, o uso de recursos externos e de equipe de suporte e as tarefas que não contribuem para a conclusão do plano.

Como exemplo, o CAE pode começar com a suposição de que um funcionário em período integral representa o equivalente a 2.080 horas totais (ou seja, 40 horas por semana, 52 semanas por ano).[10] Em seguida, o CAE pode subtrair o seguinte para determinar as horas disponíveis restantes:

- Subtrair o tempo não dedicado a auditoria, ou tempo improdutivo, relativo a atividades que não contribuam para a conclusão dos trabalhos e o cumprimento com o plano de auditoria.
  - Férias remuneradas (feriados, férias, licença médica paga).
  - Treinamento e desenvolvimento pessoal.
  - Reuniões (da equipe de auditoria interna e com a gestão e o conselho).
  - Iniciativas da atividade de auditoria interna para a avaliação e melhoria da qualidade.
  - Taxas reduzidas de uso para novas contratações previstas no ano.
  - Tempo gasto em consultoria com especialistas para desenvolver estratégias/frameworks de auditoria.
  - Rotatividade imprevista durante o ano (isto é, "fator de vaga", normalmente usado para uma grande equipe).
  - Reserva para tarefas de não auditoria ainda não atribuídas.
- Subtrair o tempo gasto na assistência a outros prestadores de avaliação, por exemplo, auditoria externa, se aplicável.
- Subtrair as horas do CAE reservadas para atividades de supervisão e afins (p. ex., estimativa de 80%).
- Subtrair horas produtivas a serem gastas em requisitos contínuos, monitoramento, análise de dados, acompanhamento de trabalhos já realizados e uma reserva para solicitações ad hoc. Obs.: alguns CAEs incluem monitoramento/auditoria contínuos como parte das horas produtivas disponíveis.
- O que resta são horas disponíveis (tempo de auditoria ou tempo cobrável) a serem gastas na realização de trabalhos (incluindo avaliações de riscos, análise e avaliação, documentação e reporte) para cumprir com o plano de auditoria interna baseado em riscos.

10. Os CAEs devem ajustar as suposições para refletir as circunstâncias atuais de sua equipe de auditoria interna e de sua organização.

Rascunhando o Plano de Auditoria Interna

Todo o trabalho preparatório culmina em uma versão preliminar do plano de auditoria interna a ser apresentado, discutido, revisado e finalizado para aprovação. O plano de auditoria interna proposto pode incluir as seguintes seções:

Sumário executivo – Essa breve visão geral dos principais pontos geralmente inclui um resumo de uma página dos riscos mais significantes, trabalhos planejados, cronograma básico e o plano de estruturação de equipe.

Políticas e processos – Esta visão geral fornece ao conselho uma compreensão de *due diligence* e abrangência das políticas e da abordagem de planejamento da auditoria interna, com descrições básicas dos processos usados para estabelecer o universo de auditoria, executar a avaliação de riscos, coordenar a cobertura de avaliação e estruturar a equipe para o plano. Quaisquer alterações nas políticas e procedimentos podem ser destacadas para discussão.

Resumo da avaliação de riscos – Uma descrição do processo e dos resultados da avaliação de riscos aprimora o entendimento do conselho sobre as prioridades da auditoria interna. As informações podem incluir:

- Estratégia organizacional, principais áreas de foco, principais riscos e estratégias de avaliação associadas no plano de auditoria.
- Resumo dos riscos.
- Análises (ou resumo) dos níveis de risco inerente e/ou residual das unidades auditáveis.
- Pontuações/classificações de risco das unidades auditáveis.
- Mapa de calor para todo o universo de auditoria, indicando prioridades, inclusões e exclusões.

Visão geral dos trabalhos no plano –

- Uma lista de trabalhos propostos de auditoria (especificando se os trabalhos são de natureza de avaliação ou consultoria).
- Escopos e objetivos provisórios dos trabalhos.
- Momento e duração provisórios (cronograma mostrando o trimestre em que o trabalho será realizado e quanto tempo levará para ser concluído).

Cobertura de avaliação e exclusões – Esta seção pode incluir um mapa, resumo ou outra ferramenta de avaliação para comunicar a cobertura de avaliação em áreas de risco significante. As exclusões reconhecem unidades auditáveis ou áreas de risco que não são abordadas e, se alguma área de alto risco não for coberta (p. ex., devido a limitações de recursos), esta seção poderá incluir recomendações ao conselho para obter avaliação, como por meio de co-sourcing ou terceirização.

Justificativa para inclusões e exclusões – Essa explicação é importante, especialmente se classificações de risco ou determinações de frequência forem substituídas. Os motivos podem incluir alteração na classificação de risco, período desde a última auditoria, alteração na gestão e mais.

Plano de recursos – Esta seção identifica o tipo e a quantidade de recursos que serão necessários para executar o plano. A descrição pode incluir o número de funcionários necessários para concluir o plano de auditoria (capacidade), o número de funcionários de suporte necessários, um resumo dos resultados da avaliação de habilidades e um plano de ação para corrigir as lacunas de habilidades.

Requisitos de orçamento financeiro – O plano inclui um orçamento financeiro para cobrir a folha de pagamento da equipe de auditoria interna, bem como o custo de serviços de co-sourcing e/ou terceirizados, ferramentas (isto é, tecnologia), treinamento e outras despesas.

IPPF e normas relevantes – As referências de conformidade com as normas e orientações relevantes do IPPF apoiam uma discussão com a alta administração e o conselho sobre a importância do plano baseado em riscos da auditoria interna, bem como outros aspectos de planejamento (p. ex., comunicação, coordenação e dependência).

Área de aprovação – A alta administração e o conselho devem aprovar o plano.

Subseções ou subplanos – Dentro do plano geral, os riscos de todas as áreas auditáveis podem ser consolidados em categorias de risco, com cobertura de avaliação relevante para cada área de risco especificada.

- Operacional.
- Financeira.
- Conformidade.
- TI/cibersegurança.
- Cultura.
- Serviços de consultoria (p. ex., iniciativas estratégicas; avaliação preliminar de um novo sistema).
- Tarefas especiais solicitadas (p. ex., investigações).
- Acompanhamento (isto é, acompanhamento da implantação das recomendações).

O Anexo F mostra um exemplo de resumo executivo de um plano de auditoria interna de três anos, no qual o segundo e o terceiro anos estão sujeitos a alterações com base nos resultados das avaliações de riscos.

Propondo o Plano e Solicitando Feedback

Depois que um plano provisório baseado em riscos é desenvolvido, o CAE ou o gerente de auditoria interna normalmente discute o plano com a alta administração antes de formalizá-lo para apresentação ao comitê de auditoria e/ou conselho completo. O CAE normalmente implanta um processo padrão para essa revisão mútua e pode se reunir com cada gerente sênior individualmente. O CAE também pode consultar comitês específicos, como os responsáveis pelo gerenciamento de riscos, conformidade, ética e outros. Também podem ser agendadas reuniões com proprietários de processos individuais, para discutir o escopo e o cronograma inicial dos trabalhos.

Nas discussões, o CAE deve comunicar os resultados da avaliação de riscos, como os riscos significantes podem afetar os objetivos da organização e como os resultados ajudam a determinar

o plano dos trabalhos de auditoria. O CAE também deve descrever a atribuição de recursos, como as áreas sobre as quais a atividade de auditoria interna prestará avaliação e aquelas para as quais confiará em outros prestadores de avaliação. Durante as reuniões, o CAE pode abordar quaisquer preocupações da alta administração. O plano pode ser alterado com base nas discussões sobre **apetite a risco** e no escopo e/ou momento da cobertura de avaliação (com base na coordenação com outros prestadores). Juntos, o CAE e a alta administração refletem sobre questões como:

- Todos os riscos e unidades auditáveis foram considerados exaustivamente?
- Há mudanças futuras que não consideramos metodicamente – p. ex., aquisições, fusões, atualizações de sistema, fornecedores terceirizados ou implantação de software?
- Como os trabalhos do plano se relacionam com os objetivos e os principais riscos da organização?
- Como os trabalhos agregam valor à alta administração e à organização?
- A coordenação da cobertura de avaliação e o cronograma/momento dos trabalhos fazem sentido?
- Se algum pedido não foi atendido, por que não?

Limitações da Cobertura de Avaliação por Orçamento

Ao comunicar os planos da atividade de auditoria interna e os requisitos de recursos, o CAE deve expressar a relação entre os riscos enfrentados pela organização e o orçamento disponível para a cobertura de avaliação. O CAE deve chamar atenção para áreas de alto risco que não terão cobertura de avaliação suficiente e deve estar preparado para solicitar recursos adicionais, se necessário.

Comunicando Para Finalizar o Plano

Apresentação ao Comitê de Auditoria

O CAE avalia o feedback da alta administração e incorpora informações relevantes para garantir que o plano reflita devidamente as prioridades da organização e que a gestão apoie a implantação do plano. O plano revisado é apresentado ao comitê de auditoria para revisão adicional. O comitê de auditoria pode sugerir ajustes ao plano com base em sua visão do apetite a risco da organização. A reunião também oferece ao CAE a oportunidade de explicar o orçamento e sua relação com a cobertura de avaliação, observando lacunas significativas na cobertura.

Apresentação ao Conselho Completo

Para se comunicar com o conselho, o CAE normalmente cria uma apresentação que resume os trabalhos no plano, explica a avaliação de riscos por trás das seleções e expressa o valor da avaliação e assessoria independentes e objetivas prestadas pela atividade de auditoria interna. O presidente do comitê de auditoria pode apresentar o resumo de informações ao conselho inteiro para aprovação final. Depois que a alta administração e o conselho aprovam o plano formalmente, todas as áreas de negócios afetadas da organização geralmente recebem uma cópia.

Comunicação Contínua

Em algumas organizações, o CAE se comunica trimestralmente através de um relatório formal. O momento das apresentações para a alta administração e o conselho (comitê de auditoria) pode afetar a forma como os dois grupos de stakeholders percebem a atividade de auditoria interna. Muitas informações fornecidas de uma só vez (p. ex., o final do trimestre) podem reduzir a receptividade dos stakeholders à atividade de auditoria interna. Os auditores internos devem ter o cuidado de se comunicar regularmente com a alta administração e preparar quaisquer alterações ao plano de auditoria interna com antecedência suficiente para permitir oportunidades de discussão.

Comunicando Propostas de Mudança

Se o plano de auditoria interna e/ou os requisitos de recursos mudarem significativamente, o CAE deve comunicar essas mudanças à alta administração e ao conselho e obter sua aprovação, de acordo com a Norma 2020 – Comunicação e Aprovação. Mesmo quando os ajustes ao plano são pequenos, podem oferecer oportunidades para as três partes discutirem suas percepções de riscos, melhorar a precisão das informações compartilhadas e alinhar suas prioridades de gerenciamento de riscos.

Alguns CAEs ou gerentes de auditoria interna revisam seu plano de auditoria interna mensalmente. Eles avaliam se alguma alteração ao perfil de risco justifica a substituição de trabalhos agendados e se há recursos suficientes disponíveis para adicionar novos trabalhos ao plano.

Embora a comunicação trimestral dessas alterações não seja necessária, muitos CAEs escolhem esse cronograma por consistência. O diálogo pode envolver a solicitação de recursos. Os auditores internos contemplam questões como: "uma mudança no plano de auditoria seria um evento único ou exigiria um ajuste de longo prazo no orçamento?" Para acomodar novos trabalhos dentro do orçamento existente, a atividade de auditoria interna pode ter que eliminar algo do plano. O CAE ou o gerente de auditoria interna pode defender os negócios das mudanças desejadas ou pode perguntar à alta administração e ao conselho qual projeto eles estão dispostos a cancelar para liberar os recursos para a mudança.

Motivos Para Ajustar o Plano de Auditoria

- As alterações organizacionais que podem alterar o perfil de risco da organização incluem (mas não estão limitadas a):
- Aquisição ou venda de uma unidade ou ativo de negócios.
- Mudança nos membros do conselho, propriedade organizacional ou liderança.
- Alterações nas leis, regulamentos ou normas da indústria, que podem apresentar novos riscos de conformidade.
- Mudanças nas iniciativas estratégicas, incluindo a busca de novas oportunidades.
- Descoberta de indicadores de riscos imprevistos durante trabalhos de auditoria interna ou externa.
- Mudanças externas, como acontecimentos políticos ou ambientais.
- Implantação de novos sistemas.

Anexo A. Normas e Orientações Relevantes do IIA

Os seguintes recursos do IIA foram citados ao longo deste guia prático. Para obter mais informações sobre a aplicação das *Normas Internacionais para a Prática Profissional de Auditoria Interna*, consulte as Orientações de Implantação do IIA.

Código de Ética
Princípio 1: Integridade
Princípio 2: Objetividade
Princípio 3: Confidencialidade
Princípio 4: Competência
Normas
Norma 1000 – Propósito, Autoridade e Responsabilidade
Norma 1100 – Independência e Objetividade
Norma 1130 – Prejuízo à Independência ou à Objetividade
Norma 2010 – Planejamento
Norma 2020 – Comunicação e Aprovação
Norma 2030 – Gerenciamento de Recursos
Norma 2040 – Políticas e Procedimentos
Norma 2050 – Coordenação e Confiança
Norma 2060 – Reportando à Alta Administração e ao Conselho
Norma 2110 – Governança
Norma 2330 – Documentando Informações
Norma 2440 – Disseminação dos Resultados
Orientações
Global Technology Audit Guide (GTAG), "*Auditing IT Governance*," 2018
Guia Prático "Avaliando o Processo de Gerenciamento de Riscos," 2019
Guia Prático "Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação," 2018
Guia Prático "Demonstrando os Princípios Fundamentais para a Prática Profissional de Auditoria Interna," 2019
Guia Prático "Planejamento do Trabalho: Estabelecendo Objetivos e Escopo," 2017
Guia Prático "Planejamento do Trabalho: Avaliando Riscos de Fraude," 2017
Guia Prático "A Auditoria Interna e a Segunda Linha de Defesa," 2016

Anexo B. Glossário

As definições de termos marcadas com asterisco foram retiradas do "Glossário" do *International Professional Practices Framework*® do IIA, edição de 2017. Outras fontes são identificadas nas notas de rodapé.

apetite a risco* – O nível de risco que uma organização está disposta a aceitar.

atividade de auditoria interna* – Um departamento, divisão, equipe de consultores ou outros profissionais que prestem serviços independentes e objetivos de avaliação e de consultoria, criados para agregar valor e melhorar as operações de uma organização. A atividade de auditoria interna auxilia a organização a atingir seus objetivos, aplicando uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, gerenciamento de riscos e controle.

avaliação de riscos – A identificação e análise (geralmente em termos de impacto e probabilidade) de riscos relevantes para o atingimento dos objetivos de uma organização, formando uma base para determinar como os riscos devem ser gerenciados.[11]

chefe executivo de auditoria* – Chefe executivo de auditoria descreve a função de uma pessoa em posição sênior, responsável pelo gerenciamento eficaz da atividade de auditoria interna, de acordo com o estatuto de auditoria interna e com os elementos mandatórios do *International Professional Practices Framework*. O chefe executivo de auditoria ou outros que reportem a ele devem ter certificações e qualificações profissionais apropriadas. O título específico do cargo e/ou responsabilidades do chefe executivo de auditoria podem variar entre as organizações.

conformidade* – Cumprimento com as políticas, planos, procedimentos, leis, regulamentos, contratos ou outros requisitos.

conselho* – O corpo administrativo de mais alto nível (p. ex.: um conselho de administração, conselho supervisor ou um conselho de gestores ou curadores) que detém a responsabilidade de dirigir e/ou supervisionar as atividades da organização e de cobrar prestação de contas por parte da alta administração. Embora os sistemas de governança variem entre jurisdições e setores, o conselho normalmente inclui membros que não fazem parte da gestão. Se não houver um conselho, a palavra "conselho" nas *Normas* se refere a um grupo ou pessoa responsável pela governança da organização. Além disso, "conselho" nas *Normas* pode se referir a um comitê ou outro órgão ao qual o corpo administrativo tenha delegado certas funções (p. ex.: um comitê de auditoria).

fator de risco – Condição associada a uma maior probabilidade de consequências de risco (isto é, um indicador principal da presença de incerteza).[12]

fraude* – Qualquer ato ilegal caracterizado por engano, dissimulação ou quebra de confiança. Esses atos independem de ameaça de violência ou de força física. As fraudes são perpetradas por partes e organizações, a fim de se obter dinheiro, propriedades ou serviços; para evitar pagamento ou perda de serviços; ou para garantir vantagem pessoal ou de negócios.

11. Anderson, *Internal Auditing*, 495.
12. Wright, *The Internal Auditor's Guide*, 66.

gerenciamento de riscos* – Processo para identificar, avaliar, gerenciar e controlar potenciais eventos ou situações, para fornecer uma garantia razoável do atingimento dos objetivos da organização.

governança* – Combinação de processos e estruturas implantadas pelo conselho para informar, dirigir, gerenciar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos.

governança da tecnologia da informação* — Consiste na liderança, estruturas organizacionais e processos que asseguram que a tecnologia da informação corporativa apoie as estratégias e os objetivos da organização.

perfil de risco – Uma visão composta do risco assumido em um nível específico da entidade ou aspecto do negócio que posiciona a gestão para considerar os tipos, gravidade e interdependências de riscos e como eles podem afetar o desempenho em relação à estratégia e aos objetivos de negócios.[13]

processos de controle* – Políticas, procedimentos (manuais e automatizados) e atividades que fazem parte de um framework de controle, criados e operados para assegurar que os riscos sejam contidos no nível que uma organização esteja disposta a aceitar.

risco* – A possibilidade de ocorrer um evento que venha a ter impacto sobre o atingimento dos objetivos. O risco é mensurado em termos de impacto e probabilidade.

risco estratégico – A possibilidade de ocorrência de um evento ou condição que melhore ou ameace a prosperidade e a existência de uma organização a longo prazo.[14]

riscos (plural) – "Refere-se a um ou mais eventos em potencial que podem afetar o atingimento dos objetivos. 'Risco' (no singular) refere-se a todos os eventos potenciais, coletivamente, que podem afetar o atingimento dos objetivos".[15]

serviços de consultoria* – Atividades de assessoria ao cliente ou serviços relacionados, cuja natureza e escopo são acordados com o cliente e destinam-se a agregar valor e melhorar os processos de governança, gerenciamento de riscos e controle da organização, sem que o auditor interno assuma responsabilidade de gestão. Exemplos incluem orientação, assessoria, facilitação e treinamento.

trabalho de auditoria* – Uma atribuição, tarefa ou atividade de revisão específica de auditoria interna, tais como uma auditoria interna, revisão de autoavaliação de controle, investigação de fraude ou consultoria. Um trabalho de auditoria pode incluir múltiplas tarefas ou atividades, criadas para cumprir com um conjunto específico de objetivos relacionados.

unidade auditável – Qualquer tópico, assunto, projeto, departamento, processo, entidade, função ou outra área em particular que, devido à presença de risco, possa justificar um trabalho de auditoria.[16]

13. COSO, *Enterprise Risk Management,* 109.
14. Wright, *The Internal Auditor's Guide*, 13.
15. PwC for Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrating Strategy with Performance,* 110.
16. Wright, *The Internal Auditors Guide*, 149.

Anexo C. Ligando Objetivos, Estratégias e o Universo de Auditoria

Figura C.1: Objetivos Organizacionais, Estratégias em Relação ao Universo de Auditoria

Objetivos da Organização	
Objetivo 1	…
Objetivo 2	…
Objetivo 3	…
Objetivo 4	…
Objetivo 5	…
Objetivo 6	…

Estratégia	Ligações com os Objetivos	Iniciativas	Ligações com o Universo de Auditoria
Estratégia 1	Objetivos 1, 6	1.1	Desenvolvimento de operações/serviços, TI
		1.2	Jurídico, finanças, conformidade
		1.3	Governança
		1.4	Operações, TI
Estratégia 2	Objetivos 1, 2, 3, 4	2.1	Operações, finanças
		2.2	Governança, jurídico
		2.3	Operações
Estratégia 3	Objetivo 4	3.1	Governança
		3.2	Suporte/recursos humanos
		3.3	Suporte/marketing
		3.4	Desenvolvimento de operações/serviços, TI
		3.5	Operações, TI
Estratégia 4	Objetivos 5, 6	4.1	Governança, suporte/marketing
		4.2	Governança, gerenciamento de riscos
		4.3	Suporte/compras
		4.4	Suporte/instalações

Anexo D. Avaliação de Riscos: Abordagem de Risco Específico

Passo 1. Definir a escala e critérios de mensuração do risco.

Neste exemplo da abordagem de risco específico, o primeiro passo é definir os critérios pelos quais classificar cada risco em termos de impacto e probabilidade. Os três critérios escolhidos para este exemplo são regulatório, operacional e financeiro. O impacto é pontuado em uma escala que varia de 5, representando catastrófico, a 1, representando baixo. A probabilidade é classificada em uma escala que varia de 5, representando muito alto, a 1, representando muito baixo.

Figura D.1: Escala e Critérios do Impacto do Risco

Descrição do Impacto	Pontuação do Impacto	Critérios Regulatórios	Critérios Operacionais	Critérios Financeiros
Catastrófico	5	Ambiente complexo e altamente regulamentado, com aplicação rigorosa; consequências por não conformidade que possam causar passivos legais e multas que possam resultar em fechamento parcial ou completo. Impactos financeiro e reputacional significativos.	Uma ou mais unidades de negócios ou toda a organização podem não conseguir operar. Impacto sobre a reputação.	Maior do que $25 milhões
Altamente Significante	4	Ambiente regulatório complexo; passivos legais e multas por não conformidade podem receber atenção do público e ter impacto duradouro em termos financeiros e de reputação.	Várias unidades de negócios podem ser significativamente afetadas. A capacidade da organização de operar ou atender clientes pode ser severamente reduzida. Impacto sobre a reputação.	$10 a $25 milhões
Significante	3	Leis e regulamentos são aplicados de maneira consistente. Passivos legais e multas por não conformidade são materiais.	Uma ou mais unidades de negócios podem ser materialmente afetadas. A capacidade da organização de operar ou atender clientes pode ser significativamente reduzida.	$5 a $10 milhões (material)
Moderado	2	Ambiente regulatório ativo com penalidades pequenas a moderadas por não conformidade.	A eficácia e eficiência operacionais são moderadamente prejudicadas.	$1 a $5 milhões
Baixo	1	O ambiente regulatório é fraco ou a penalidade por não conformidade é pequena.	A eficácia ou eficiência operacional pode ser melhorada, mas as operações seguem ininterruptas.	Menor do que $1 milhão

Figura D.2: Escala e Descrições da Probabilidade do Risco

Classificação	Pontuação	Descrição	Critérios
Muito alta	5	A probabilidade de ocorrência do risco é relativamente muito alta.	Os processos operacionais são complexos e os controles não são eficazes.
Alta	4	A probabilidade de ocorrência do risco é relativamente alta.	Os processos operacionais são complexos e algumas deficiências de controle são observadas.
Moderada	3	A probabilidade de ocorrência do risco é relativamente moderada.	Os processos operacionais são moderadamente complexos; pequenas fraquezas de controle são observadas.
Baixa	2	A probabilidade de ocorrência do risco é relativamente baixa.	Os processos operacionais não são complexos; os controles são eficazes.
Muito baixa	1	A probabilidade de ocorrência do risco é relativamente muito baixa.	Os processos operacionais não são complexos. Os controles são eficazes.

Passo 2. Listar as unidades auditáveis verticalmente e os riscos específicos horizontalmente e avaliar o impacto e a probabilidade de cada risco específico para cada unidade auditável.

A Figura D.3 mostra um exemplo personalizado com cada unidade auditável em uma linha e cada risco em uma coluna. Cada coluna de risco é subdividida em classificações de impacto e de probabilidade específicas da unidade auditável. As classificações nesta tabela não são ponderadas; portanto, as classificações de impacto e probabilidade de cada risco são somadas em cada unidade auditável para obter a pontuação de risco total de cada unidade. A pontuação total do risco indica o nível relativo de risco para cada unidade. Este é apenas um exemplo simplificado. Na prática, os formatos variam muito; e, geralmente, o impacto deve ter maior peso do que a probabilidade.

Figura D.3: Abordagem de Risco Específico com Pontuação Total de Risco

P = probabilidade I = impacto	Risco 1		Risco 2		Risco 3		Risco 4		Risco 5		Risco 6		Risco 7		Risco 8		Pont. Total	Nível
	P	I	P	I	P	I	P	I	P	I	P	I	P	I	P	I		
Unid. Auditável 1	3	2	2	4	3	5	2	3	1	5	1	3	1	2	2	5	44	M
Unid. Auditável 2	2	3	1	4	1	5	2	2	1	3	1	1	2	3	2	2	35	M
Unid. Auditável 3	1	3	1	3	2	3	3	3	2	1	1	1	3	4	1	4	36	M
Unid. Auditável 4	4	4	3	5	2	5	1	2	1	5	3	2	2	5	2	5	51	A
Unid. Auditável 5	1	3	2	4	3	4	3	3	4	4	2	4	2	5	1	4	49	A
Unid. Auditável 6	1	1	1	2	2	1	1	3	2	1	2	2	2	3	1	2	27	B
Unid. Auditável 7	4	5	4	5	4	5	4	4	4	5	4	5	3	5	3	5	60	E
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
Classificação dos Intervalos de Pontuação																		

Baixa (B) = 0 a 32	Moderada (M) = 33 a 45	Alta (A) = 46 a 59	Extrema (E) = mais de 60

Passo 3. Eficácia da pontuação do gerenciamento de riscos e controles.

Figura D.4: Critérios para Avaliar Processos de Gerenciamento de Riscos e Controle

Avaliação da Criação	Critérios para Processos de Gerenciamento de Riscos e Controle
Adequada	▪ Os processos de gerenciamento de riscos, controle e governança estão operando com eficácia. Podem ser eficientes ou ter espaço para melhoria. ▪ A propriedade do risco está claramente definida e ativa. ▪ A gestão corrige deficiências de controle ou outras questões descobertas pelos auditores e reguladores. ▪ A gestão é proativa na identificação e mitigação de riscos.
Precisa de Melhoria	▪ Alguns processos de gerenciamento de riscos e controle estão operando com eficácia, mas muitos não são documentados ou monitorados. ▪ A maioria dos principais riscos é mitigada a um nível aceitável. ▪ Alguns riscos, mas não todos, têm proprietários.
Inadequada	▪ Os processos de gerenciamento de riscos e controle são mal projetados, executados inconsistentemente ou não existem. ▪ As informações de risco não são documentadas e os riscos não são totalmente remediados. ▪ O gerenciamento de riscos é reativo.

Passo 4. Determinar o risco residual.

A avaliação do risco inerente, da eficácia do controle e do risco residual pode ser mostrada como um gráfico (ou "matriz") que inclua uma coluna quantificando os riscos em sua forma inerente, uma coluna quantificando a eficácia das respostas a risco e controles correspondentes e uma coluna para o risco residual correspondente. A Figura D.5 mostra um gráfico de amostra.

Figura D.5: Determinação do Risco Residual

Unidade Auditável	Nível Inerente de Risco	Eficácia do Controle	Nível Residual de Risco
Unid. Auditável 1	Moderado	Precisa de melhorias	Moderado
Unid. Auditável 2	Moderado	Adequado	Baixo
Unid. Auditável 3	Moderado	Inadequado	Alto
Unid. Auditável 4	Alto	Adequado	Baixo
Unid. Auditável 5	Alto	Precisa de melhorias	Alto
Unid. Auditável 6	Baixo	Adequado	Baixo
Unid. Auditável 7	Extremo	Precisa de melhorias	Extremo
...	...	...	...

Anexo E. Exemplo: Avaliação de Riscos Usando a Abordagem de Fator de Risco

Figura E.1: Exemplo de Definição de Fatores, Critérios e Classificações de Risco

Nome do Fator de Risco	Considerações/Critérios	Classificações e Definição
Perda/Exposição Material	■ Valor em dólar em risco. ■ Despesas operacionais anuais. ■ Número de transações. ■ Impacto sobre outras áreas da organização. ■ Grau de confiança na TI.	5 = alta exposição. 4 = exposição acima da média. 3 = exposição média. 2 = exposição abaixo da média. 1 = pouca exposição.
Risco Estratégico	■ Percepção do público/reputação. ■ Condições econômicas locais. ■ Volatilidade. ■ Significância da estratégia. ■ Grau de regulação externa. ■ Mudanças recentes na legislação ou escrutínio regulatório. ■ Mudanças nas linhas de negócios ou serviços. ■ Novos contratos significantes.	5 = alto risco. 4 = risco acima da média. 3 = risco médio. 2 = risco abaixo da média. 1 = baixo risco.
Ambiente de Controle (AC)	■ Grau de isolamento do processo. ■ Grau de formalização e alinhamento de objetivos. ■ Implantação nova de processo/sistema. ■ Processo interno vs. terceirizado. ■ Rotatividade da gestão operacional. ■ Grau do monitoramento de desempenho em vigor. ■ Tom no topo. ■ Formalidade de processos/procedimentos. ■ Impacto sobre os clientes.	5 = alto risco (AC muito fraco). 4 = risco acima da média (AC fraco). 3 = média (AC média). 2 = risco abaixo da média (AC forte). 1 = baixo risco (AC muito forte).
Complexidade	■ Grau de automação. ■ Grau de especialização necessário para executar. ■ Nível de detalhe técnico. ■ Complexidade da estrutura, arquitetura envolvida. ■ Frequência de mudanças.	5 = altamente complexo. 4 = complexidade acima da média. 3 = complexidade média. 2 = complexidade abaixo da média. 1 = simples.

Figura E.1: Exemplo de Definição de Fatores, Critérios e Classificações de Risco (continuação)

Nome do Fator de Risco	Considerações/Critérios	Classificações e Definição
Cobertura de Avaliação	▪ Tipo de trabalho. ▪ Outras revisões (externas, regulatórias). ▪ Cobertura da segunda linha. ▪ Acompanhamento já em vigor.	5 = não revisado nos últimos 4 anos (3 anos para riscos de conformidade ou alto impacto). 4 = não revisado nos últimos 3 a 4 anos (2 a 3 anos para riscos de conformidade ou alto impacto). 3 = revisado nos últimos 2 a 3 anos (1 a 2 anos para riscos de conformidade ou alto impacto). 2 = revisado nos últimos 1 a 2 anos (1 ano para riscos de conformidade, alto impacto). 1 = revisado no ano passado ou iniciativa atualmente em vigor.
Consciência da Gestão	▪ Preocupações comunicadas em respostas a pesquisas. ▪ Preocupações comunicadas em entrevistas. ▪ Nível de conscientização de riscos.	5 = gestão preocupada, tem questão e motivo específicos. 4 = gestão tem preocupações gerais. 3 = gestão é neutra. 2 = gestão não tem preocupações específicas. 1 = gestão pode demonstrar controle eficaz sobre os riscos.

Figura E.2: Exemplo de Determinação da Pontuação Total do Risco

	Fatores de Risco Relacionados a Impacto			Fatores de Risco Relacionados a Probabilidade					
Unidade auditável	Perda/ Exposição material	Risco estratégico	Subtotal	Ambiente de controle	Complexi-dade	Cobertura de auditoria	Consciência da gestão	Subtotal	Pontuação total de risco
Peso	*50%*	*50%*		*35%*	*35%*	*20%*	*10%*		
Unid. 1	1	2	1,5	2	1	3	1	1,75	**3,25**
Unid. 2	5	5	5	3	1	5	1	2,5	**7,5**
Unid. 3	1	5	3	4	5	4	2	4,15	**7,15**
Unid. 4	5	5	5	5	4	5	4	4,15	**9,15**
Unid. 5	5	2	3,5	4	2	2	4	2,9	**6,4**
…	…	…	…	…	…	…	…	…	…

Legenda da Pontuação Total de Risco	2 a 4 = Baixa	4,1 a 6,5 = Moderada	6,6 a 8,5 = Alta	8,6 a 10 = Muito Alta

Escala de classificação: 1 é a mais baixa; 5 a mais alta. Menor pontuação total possível = 2. Maior pontuação total possível = 10.

Anexo F. Exemplo: Sumário do Plano de Auditoria Interna

Este exemplo básico de um resumo do plano de auditoria interna mostra as áreas auditáveis por linha. Cada linha é estendida para incluir informações de riscos que indicam a prioridade da unidade auditável e do ano e trimestre em que o trabalho será conduzido. Os cronogramas propostos para os anos seguintes ao atual estão sujeitos a alterações, dependendo das atualizações das avaliações de riscos. Cada quadrado que representa um trabalho é codificado por cores, com uma legenda indicando o tipo de trabalho. Os numerais dentro de cada bloco indicam o número de horas que o trabalho exigirá. As horas são resumidas na parte inferior de cada coluna, mostrando claramente o total de recursos necessários. Os cálculos de resumo também mostram as horas necessárias para tarefas de auditoria interna não relacionadas a trabalhos de auditoria.

Figura F.1: Resumo de Três Anos de um Plano de Auditoria Interna Baseado em Riscos

(Subject to Change Based on Risk Assessment) — Full audit | Limited audit

Current Risk Assessment				Year of Recent Reviews			Proposed Staff Hours Current Year			Proposed Schedule Current Year					Proposed Schedule Next Year					Proposed Schedule Two Years from Current				
Rank	Auditable Unit	Residual Risk Rating	Priority	Three Years Ago	Two Years Ago	Last Year	Service Provider	IAA	TOTAL	Q1	Q2	Q3	Q4	Total Annual Effort	Q1	Q2	Q3	Q4	Total Annual Effort	Q1	Q2	Q3	Q4	Total Annual Effort
1	Auditable unit 6	4.5	High	✓	✓		15	20	35	20	15					5	15							
2	Auditable unit 3	4.4	High	✓		✓	20	20	40	20	20												25	
3	Auditable unit 7	4.2	High	✓	✓		20	20	40		20	20			15	5								
4	Auditable unit 5	3.1	Medium	✓		✓		30	30			20	10									25		
5	Auditable unit 11	3.0	Medium		✓											30	10							
6	Auditable unit 8	2.8	Medium		✓										5	10								
7	Auditable unit 9	2.6	Medium		✓												15	15						
8	Auditable unit 1	2.2	Medium		✓											25	10							
9	Auditable unit 2	2.1	Medium			✓														10	20			
10	Auditable unit 4	1.2	Low			✓																15	5	
11	Auditable unit 10	1.0	Low		✓																	15	5	
							55	90	145	40	55	40	10	145	20	75	50	15	160	10	20	55	35	120
Nonauditable Areas																								
1	Preparation for Audit & Risk Committee Meetings							90	90	9	7	7	7		9	7	7	7		9	7	7	7	
2	Updating Risk Assessment and Internal Audit Plan							150	150		15	15	20			15	15	20			15	15	20	
3	Consulting Assignments and Other Projects							45	45	10	5				10	5				10	5			
4	Follow-up Audits							240	240	20	20	20	20		20	20	20	20		20	20	20	20	
5	Staff Training							90	90	10	10	10			10	10	10			10	10	10		
6	Strategic Initiatives						20	125	145	20	20	0	25		10	10	10	10		10	10	10	10	
7	Engagements Carried Forward							30	30	10					10					10				
8	Quality Assurance							45	45				15					15					15	
Total Effort Required in a Year							75	905	980	119	132	92	97	440	89	142	112	87	430	79	87	117	107	390

Anexo G. Visão Geral da Documentação de Auditoria Interna

Documentar as informações obtidas em cada etapa do planejamento faz parte da abordagem sistemática e disciplinada que define a atividade de auditoria interna. Os auditores internos e o CAE podem desenvolver os seguintes documentos e compilá-los em uma base abrangente e coesa para apoiar o plano de auditoria interna.

Figura G.1: Documentação de Auditoria Interna Relacionada a Cada Fase do Planejamento

Fase do Planejamento	Documentação de Auditoria Interna
Entender a Organização	▪ Estatuto de auditoria interna, observando as expectativas da gestão e do conselho e os requisitos para conformidade da auditoria interna com o IPPF, bem como a conformidade com leis, regulamentos e outros requisitos da indústria. ▪ Estrutura de gerenciamento de riscos da organização (categorias de risco e riscos individuais com descrições). ▪ Registro de riscos abrangente e consolidado (universo de riscos).
Identificar, Avaliar, Priorizar Riscos	▪ Universo de auditoria que lista unidades auditáveis. ▪ Anotações de brainstorming e avaliação de riscos emergentes e de fraude. ▪ Avaliação de riscos, incluindo análise da significância dos riscos. ▪ Lista e descrição dos fatores e métricas de risco. ▪ Gráfico/matriz de riscos e controles, mostrando classificações dos riscos. ▪ Mapa de calor. ▪ Classificação das unidades auditáveis para inclusão no plano. ▪ Critérios para prioridade e frequência de revisão com base no nível de risco residual.
Coordenar com Outros Prestadores	▪ Mapa de Avaliação
Estimar Recursos	▪ Plano de estruturação da equipe de auditoria interna, incluindo o Inventário de habilidades da equipe. o Cálculo das habilidades necessárias para concluir o plano. o Anotações sobre premissas e cálculos. o Resumo de horas por pessoa dedicadas a responsabilidades e tarefas que não sejam de auditoria.
Propor Plano e Solicitar Feedback	▪ Pautas e minutas das reuniões, ▪ Memorandos documentando reuniões informais ▪ Pesquisas
Finalizar e Comunicar Plano	▪ Unidades auditáveis no universo de auditoria. ▪ Classificações de risco inerente e residual de cada unidade. ▪ Descrição indicando a prioridade do trabalho de cada unidade. ▪ Cronograma de trabalhos (calendário plurianual e de curto prazo). ▪ Escopo e objetivos propostos para o trabalho.

	■ Horas/pessoa e recursos necessários para cada trabalho. ■ Tarefas da equipe. ■ Resumo dos recursos: total de horas/pessoa e número de trabalhos por ano.
Avaliar Riscos Continuamente	■ Avaliações trimestrais de riscos e/ou tecnologias que permitem atualizações do monitoramento contínuo de riscos.
Atualizar Plano e Comunicar Atualizações	■ Estatuto de auditoria interna, observando os critérios acordados para as mudanças que devem ser comunicadas.

Anexo H: Referências e Leituras Adicionais

Referências

Wright, Rick A., Jr. *Internal Auditor's Guide to Risk Assessment*. 2ª ed. Lake Mary, FL: Internal Audit Foundation. 2018. https://bookstore.theiia.org/the-internal-auditors-guide-to-risk-assessment-2nd-edition.

Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick e Paul J. Sobel. *Internal Auditing: Assurance and Advisory Services*, 4ª ed. Lake Mary, FL: Internal Audit Foundation. 2017. https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition-2.

Leituras Adicionais

Orientação do Committee of Sponsoring Organizations of the Treadway Commission (COSO)

- *Enterprise Risk Management — Integrating Strategy and Performance*. 2017. https://www.coso.org/Pages/erm.aspx.
- *Internal Control – Integrated Framework*. 2013. https://www.coso.org/Pages/ic.aspx.

Recursos da ISACA

- *COBIT 2019 Framework: Introduction and Methodology*. https://www.isaca.org/resources/cobit.
- *COBIT 2019 Framework: Governance and Management Objectives*. https://www.isaca.org/resources/cobit.
- *The Risk IT Framework*. https://www.isaca.org/bookstore/bookstore-risk-digital/writf.

Agradecimentos

Equipe de Desenvolvimento de Orientações

Alp Buluc, CIA, CCSA, CRMA, Turquia
David Dominguez, CIA, CRMA, Estados Unidos
Susan Haseley, Estados Unidos
Charlotta Hjelm, CIA, QIAL, Suécia
Hazem Keshk, CIA, CRMA, Canadá
Suzan Sgaier, CIA, Estados Unidos
Faris Theyab, CIA, Emirados Árabes Unidos

Contribuintes das Orientações Globais

Awad Elkarim Mohamed Ahmed, CIA, CCSA, CRMA, Emirados Árabes Unidos
Travis Finstad, Estados Unidos
Renee Jaenicke, CIA, Estados Unidos
James Paterson, CIA, Reino Unido

Normas e Orientações Globais do The IIA

Anne Mercer, CIA, CFSA, Diretora (Líder do Projeto)
Jim Pelletier, CIA, CGAP, Vice-Presidente
Cassian Jae, Diretor Geral
Michael Padilla, CIA, Diretor
Christopher Polke, CGAP, Diretor
Jeanette York, CCSA, Diretora
Shelli Browning, Editora Técnica
Lauressa Nelson, Editora Técnica
Vanessa Van Natta, Especialista em Normas e Orientações

O The IIA gostaria de agradecer aos seguintes órgãos supervisores por seu apoio: Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, e International Professional Practices Framework Oversight Council.

Sobre o The IIA

The Institute of Internal Auditors (The IIA) é o mais reconhecido advogado, educador e fornecedor de normas, orientações e certificações da profissão de auditoria interna. Fundado em 1941, o The IIA atende, atualmente, mais de 200.000 membros de mais de 170 países e territórios. A sede global da associação fica em Lake Mary, na Flórida, EUA. Para mais informações, visite www.globaliia.org.

Isenção de Responsabilidade

O The IIA publica este documento para fins informativos e educacionais e, como tal, este material deve ser usado apenas como guia. Este material de orientação não tem o objetivo de fornecer respostas definitivas a específicas circunstâncias individuais. O The IIA recomenda que você sempre busque conselhos especializados independentes, relacionados diretamente a qualquer situação específica. O The IIA não aceita qualquer responsabilidade pela confiança depositada unicamente nesta orientação.

Copyright

Maio de 2020

The Institute of Internal Auditors | Global

Sede Global
The Institute of Internal Auditors
1035 Greenwood Blvd., Suíte 401
Lake Mary, FL 32746, EUA
Tel.: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org