IPPF

International Professional Practices Framework

Supplemental Guidance

Practice Guide

Avaliando o Processo de Gerenciamento de Riscos

Traduzido por: IIA Brasil

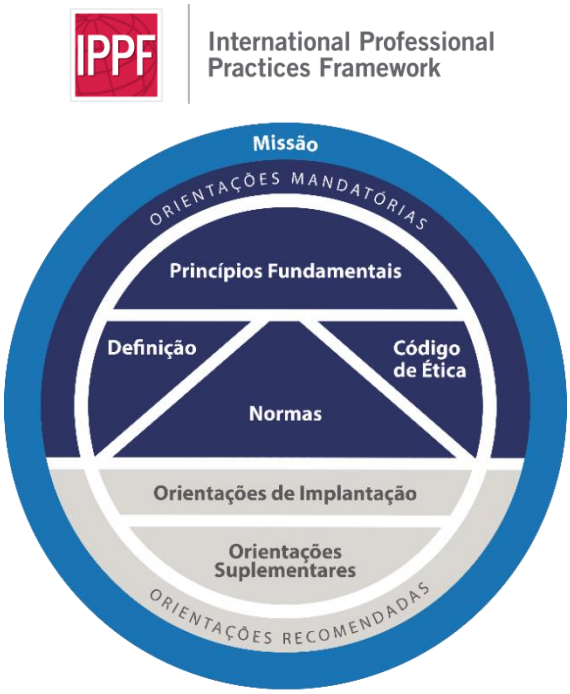
The Institute of Internal Auditors | Global

Sobre o IPPF

O *International Professional Practices Framework®* (IPPF®) é o framework conceitual que organiza as orientações fidedignas promulgadas pelo The IIA. Órgão confiável, global e criador de orientações, o The IIA oferece aos profissionais de auditoria interna do mundo todo orientações fidedignas, organizadas no IPPF como Orientações Mandatórias e Orientações Recomendadas.

As Orientações Mandatórias são desenvolvidas seguindo um processo de diligência devida estabelecido, que inclui um período de exposição pública para contribuição das partes interessadas. 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.*



Sobre as Orientações Suplementares

As Orientações Suplementares fazem parte do *International Professional Practices Framework®* (IPPF®) do The IIA e fornecem orientações adicionais e não mandatórias para a condução de atividades de auditoria interna. Ao mesmo tempo em que apoia as *Normas,* as Orientações Suplementares destinam-se a abordar tópicos específicos, assim como questões específicas de determinados setores, em maior detalhe processual do que as *Normas*. As Orientações Suplementares são apoiadas pelo The IIA, por meio de processos formais de revisão e aprovação.

Guias Práticos

Os Guias Práticos são um tipo de Orientação Suplementar, que oferece abordagens passo-a-passo, com processos, procedimentos, ferramentas e programas, assim como exemplos de entregáveis.

Os Guias Práticos destinam-se a apoiar os auditores internos. Também estão disponíveis Guias Práticos para apoiar:

- 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

Em todo o mundo, as atividades e iniciativas de gerenciamento de riscos são necessárias e esperadas pelos órgãos reguladores, agências de classificação e uma série de outros stakeholders nas principais indústrias, incluindo serviços financeiros, governo, manufatura, energia, serviços de saúde e mais. No entanto, o gerenciamento de riscos é impulsionado por mais do que regulamentos e forças externas. A implantação de um gerenciamento de riscos eficiente e eficaz beneficia organizações de qualquer tipo e tamanho, ajudando-as a alcançar seus objetivos operacionais e estratégicos e a aumentar seu valor e sustentabilidade, salvaguardando ainda mais, em última análise, os stakeholders.

Os auditores internos devem avaliar a eficácia e contribuir para a melhoria do processo de gerenciamento de riscos (Norma 2120 – Gerenciamento de Riscos). O benchmarking do estado atual do gerenciamento de riscos da organização em relação a um modelo de maturidade de gerenciamento de riscos é uma boa forma de iniciar esse tipo de avaliação. O benchmarking pode ajudar a atividade de auditoria interna a se comunicar com a alta administração e com o conselho sobre o nível de maturidade do gerenciamento de riscos da organização e sobre a aspiração de melhorar o processo e aumentar a maturidade. Essas informações também permitem que os auditores internos ajustem adequadamente cada trabalho, levando em consideração a maturidade da área ou o processo sob revisão.

Este guia fornece exemplos de modelos de maturidade de gerenciamento de riscos e uma metodologia básica que os auditores internos podem usar para prestar avaliação independente de que o processo de gerenciamento de riscos da organização é eficaz. A aplicação da orientação ajudará os auditores internos a proteger e aprimorar o valor organizacional e atender às expectativas do conselho e da alta administração.

Introdução

Os esforços de **gerenciamento de riscos** da organização geralmente são referidos coletivamente como seu programa de gerenciamento de riscos. No entanto, o termo "programa" pode ser interpretado como limitado ou finito. Este guia prático trata o gerenciamento de riscos como um processo, em vez de um programa, implicando que é um esforço contínuo e uma função contínua.

Obs.: Os termos em negrito são definidos no glossário no Anexo B.

Em muitas jurisdições, o **conselho** é encarregado de supervisionar a implantação de um processo de gerenciamento de riscos e de responder com eficácia ao panorama de riscos em constante mudança. Por sua vez, espera-se que o ***chief audit executive*** (CAE) e a **atividade de auditoria interna** prestem avaliação independente de que os processos de gerenciamento de riscos da organização são eficazes, de acordo com a Norma 2120 – Gerenciamento de Riscos, que lista diversos critérios para fazer tal avaliação.

A avaliação dos processos de gerenciamento de riscos de uma organização é um desafio crescente, pois existem diversas normas, frameworks e modelos de gerenciamento de riscos, e outros são

criados com frequência. O gerenciamento de riscos pode abranger as políticas, procedimentos e controles que asseguram a identificação, avaliação, tratamento, monitoramento e reporte adequados, oportunos e contínuos dos riscos à organização.

Embora este guia não defenda que uma organização deva usar qualquer programa, framework ou modelo específico de gerenciamento de riscos, os seguintes atributos comuns de um gerenciamento de riscos amadurecido são discutidos:

- Cultura de risco: Integração do risco em todas as tomadas de decisão, compensações, estruturas de recompensa e estabelecimento de metas.
- Governança do risco: Participação, no processo de gerenciamento de riscos em toda a organização, de uma equipe com conhecimento, qualificação e competência em gerenciamento de riscos.
- Processo de gerenciamento de riscos: Identificação de riscos agregados, avaliação de prioridades, tratamento, monitoramento e reporte em toda a organização.

Além disso, os níveis de maturidade, abordagens, estratégias e foco das funções relacionadas ao gerenciamento de riscos geralmente dependem do tamanho e da complexidade da organização, e do setor e das jurisdições em que opera. Este guia fornece informações básicas, metodologia e ferramentas para permitir que os auditores internos prestem avaliação de que os processos de gerenciamento de riscos da organização são eficazes e contribuem para a melhoria desses processos.

Esta orientação ajudará os auditores internos a:

- Aplicar os princípios do Código de Ética do The IIA e as *Normas Internacionais para a Prática Profissional de Auditoria Interna* para melhorar e proteger o valor organizacional, oferecendo avaliação, orientação e conhecimentos objetivos e baseados em riscos.
- Compreender a necessidade de avaliar as atividades de gerenciamento de riscos.
- Entender os principais componentes de um processo eficaz de gerenciamento de riscos.
- Desenvolver uma abordagem de avaliação que leve em consideração os ambientes comerciais e regulatórios da organização e seu nível de maturidade.
- Coletar as informações necessárias para determinar o escopo de um trabalho de avaliação das atividades de gerenciamento de riscos.
- Avaliar a eficácia do processo de gerenciamento de riscos.
- Contribuir para a melhoria do processo de gerenciamento de riscos.

Importância para o Negócio: Riscos e Oportunidades

O gerenciamento de riscos, como disciplina, há muito desempenha um papel vital nas organizações. Ele evoluiu para diversos formatos e é conhecido por muitos nomes, de "gerenciamento de riscos de projeto" a "gerenciamento de riscos corporativos", ou ERM. O gerenciamento de riscos continua atraindo atenção, conforme o mundo se torna mais interconectado e a interrupção se acelera em todas as indústrias. No entanto, a adoção do gerenciamento de riscos documentado, como um esforço de toda a organização, ainda precisa se tornar a norma universal.

O fracasso da governança, sistemas e processos de gerenciamento de riscos pode levar a passivos, multas, sanções e exposições relacionadas. Revisões e avaliações contínuas do gerenciamento de riscos ajudarão as organizações a evitar a perda de ativos, propriedade intelectual, participação de mercado, oportunidades de receita, fidelidade do cliente, reputação da marca e mais, por conta da ocorrência de eventos de risco que poderiam ter sido prevenidos, evitados ou mitigados (compartilhados ou transferidos). O Anexo C descreve os cenários de riscos relacionados ao processo de gerenciamento de riscos.

As organizações bem-administradas e bem-sucedidas usam o processo de gerenciamento de riscos para coordenar a direção e o controle da exposição a risco de uma forma que permita à organização atingir seus objetivos. Mensurar os benefícios de um processo amadurecido de gerenciamento de riscos pode ser desafiador, porque pode ser difícil obter dados confiáveis,

Norma 2120 – Gerenciamento de Riscos

A atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de risco.

Interpretação:

Determinar se os processos de gerenciamento de risco são eficazes é um julgamento que resulta da avaliação do auditor interno quanto a se:

- *Os objetivos da organização dão suporte e estão alinhados à missão da organização.*
- *Os riscos significativos são identificados e avaliados.*
- *Respostas apropriadas aos riscos são selecionadas de forma a alinhar os riscos ao apetite a risco da organização.*
- *As informações relevantes sobre o risco são capturadas e comunicadas de forma tempestiva através da organização, permitindo que colaboradores, administração e conselho cumpram suas responsabilidades.*

A atividade de auditoria interna pode capturar informações para apoiar essa avaliação através de múltiplos trabalhos de auditoria. Os resultados desses trabalhos de auditoria, vistos em conjunto, proporcionam uma compreensão dos processos de gerenciamento de risco da organização e da eficácia desses processos.

Os processos de gerenciamento de risco são monitorados através de atividades permanentes de gerenciamento, de avaliações independentes ou de ambos.

se houver. Pode ser difícil que as organizações analisem objetivamente a maturidade de seu próprio processo de gerenciamento de riscos.

No entanto, um processo amadurecido de gerenciamento de riscos geralmente demonstra benefícios, como:

- Permitir a tomada de decisões e a definição de estratégias com base nos riscos.
- Aumentar a comunicação e consultas em toda a organização.
- Estabelecer conexões e conhecimentos entre os riscos, oportunidades e estratégias, por meio de uma linguagem comum de risco.
- Possibilitar a documentação e o reporte tempestivo das atividades de gerenciamento de riscos, para que a alta administração e o conselho estejam bem informados sobre a direção da administração.
- Aumentar a probabilidade de que a organização atinja seus objetivos estratégicos.
- Criar e proteger o valor para os stakeholders.

Ao propor melhorias no processo de gerenciamento de riscos, os auditores internos podem encontrar objeções, tais como:

- As avaliações de riscos levam muito tempo.
- As informações de risco coletadas não são relevantes.
- As informações de risco não são usadas para tomar decisões.

Quando a atividade de auditoria interna elabora uma avaliação do processo de gerenciamento de riscos da organização, é importante entender o nível de maturidade do gerenciamento de riscos da organização e sua cultura de risco, para desenvolver questionamentos apropriados. Se a organização ainda não desenvolveu completamente sua perspectiva ou filosofia de gerenciamento de riscos, a atividade de auditoria interna deve entender as razões para isso, antes de formular as conclusões e recomendações. São importantes as opiniões sobre se o processo de gerenciamento de riscos produz as informações corretas. Se a administração acreditar que o processo de gerenciamento de riscos é um exercício burocrático que não vale os recursos necessários para executá-lo, recomendar melhorias em larga escala pode ser prematuro e recebido com ceticismo, ou rejeitado completamente. Em vez disso, os auditores internos podem ser mais eficazes ao fazer recomendações relacionadas à cultura de risco da organização.

Maturidade do Gerenciamento de Riscos

Há vários frameworks de gerenciamento de riscos disponíveis. Cada um oferece princípios que as organizações devem considerar ao desenvolver um processo abrangente de gerenciamento de riscos. Alguns frameworks se concentram em controles internos e em sua relação com os riscos de uma organização. Outros se concentram apenas nos riscos de TI, estratégicos ou seguráveis, por exemplo. Uma organização pode reconhecer que nenhum framework único de gerenciamento de riscos abrange todas as áreas de risco que ela precisa considerar. Em vez de adotar um framework única, a organização pode se beneficiar da combinação dos elementos de diversos frameworks,

para criar um que seja adaptado exclusivamente às suas características e necessidades específicas. Independentemente de qual framework é usado como base para um processo de gerenciamento de riscos, certos elementos podem ajudar a organização a mensurar sua maturidade.

A **Figura 1** é um exemplo de um **modelo de maturidade** do gerenciamento de riscos, ilustrando cinco estágios de desenvolvimento que podem caracterizar um processo de gerenciamento de riscos. Vários elementos dentro da mesma organização podem estar em diferentes estágios de maturidade a qualquer momento; por exemplo, o nível de maturidade da cultura de uma organização pode diferir da maturidade de sua governança e do processo. Ao planejar trabalhos de auditoria, os auditores internos podem usar um modelo de maturidade para adequar cada trabalho devidamente à maturidade do elemento sob revisão.

Figura 1: Exemplo de Modelo de Maturidade do Gerenciamento de Riscos

Estágio	Cultura	Governança	Processo
1 – Inicial	O risco pertence à atividade de auditoria interna.	CAE/presidente do comitê de auditoria.	Auditoria baseada em riscos.
2 – Repetível	O risco é considerado conforme a necessidade.	Gerentes de negócios.	Processo de autoavaliação de riscos e controle conforme necessário.
3 – Definido	As informações de risco são compartilhadas entre as funções de auditoria interna e controle.	C-suíte/membros do conselho.	A linguagem comum de risco e o processo de avaliação de riscos são usados pelas funções de auditoria interna e controle.
4 – Gerenciado	O risco é integrado ao planejamento estratégico; o apetite a risco é declarado e comunicado.	Todos os níveis de gestão e o conselho.	Uma linguagem comum de risco e um processo consistente de avaliação de riscos estão em vigor em toda a organização.
5 – Otimizado	O risco é integrado em todas as decisões, compensações e metas.	Participação total.	Uma linguagem comum de risco e o reporte agregado de riscos estão estabelecidos em toda a organização.

Para averiguar a posição de uma organização no modelo de maturidade do gerenciamento de riscos e avaliar a eficácia com que o processo de gerenciamento de riscos está servindo à organização, os auditores internos devem considerar diversos elementos.

Todas as organizações praticam alguma forma de gerenciamento de riscos, embora possam não estar cientes disso e não estar formalmente documentando seus esforços.

A forma mais simples de gerenciamento de riscos documentado é um exercício anual, para criar um registro de riscos organizacionais no nível superior. Isto pode ser referido como uma "avaliação estratégica de riscos", na qual a alta administração desenvolve e documenta uma lista de riscos e a avaliação não é abordada novamente até o ano seguinte. No outro extremo do espectro, as organizações com o processo de gerenciamento de riscos mais robusto ou maduro consideram os fatores de risco, incluindo os de natureza cultural ou de governança, em toda a organização, em um formato estruturado e sistemático.

Considerações de Auditoria

Quão madura deve ser uma organização? Considere uma escala de 1 a 5, sendo 5 a mais madura. Não é necessariamente ideal ou prático que todas as organizações estejam operando no mais alto nível de maturidade. Conseguir um 2 ou 3 de qualidade pode ser aceitável. Cada organização deve determinar qual nível de maturidade é ideal para suas circunstâncias.

Apetite a Risco

O International Professional Practices Framework do The IIA define o apetite a risco como o nível de risco que uma organização está disposta a aceitar. Para muitas organizações, o apetite a risco é difícil de articular para uso prático em discussões. Uma forma comum de apetite a risco é uma declaração de "tolerância a perda", que pode ser aprovada pela alta administração e/ou pelo conselho, com uma ressalva de que o limite de perda pode ser excedido com a aprovação daqueles com níveis apropriados de autoridade.

Enquadrar o apetite a risco como uma "tolerância a perda" pode ser interpretado como um plano organizacional para atingir o nível declarado de perda (quantidade monetária) por sua exposição a risco, o que poderia levar os gerentes a assumir níveis de exposição a risco superiores aos necessários ou desejados. Além disso, ter um apetite a risco expresso em termos de estratégias amplas pode levar a diferentes interpretações de como as tolerâncias funcionam, à medida que a declaração de apetite a risco é aplicada aos níveis inferiores da organização.

Os auditores internos devem encorajar a organização a adotar uma metodologia e um formato de apetite a risco que auxiliem a administração e o conselho na priorização de estratégias e alocações de recursos. O apetite a risco pode ser dinâmico e, muitas vezes, é um equilíbrio entre as estratégias. A definição de níveis estáticos para a exposição a risco do nível superior da organização pode resultar no esquecimento do apetite a risco como ferramenta para a tomada de decisões informadas de forma consistente em toda a organização.

Estrutura: Papéis e Responsabilidades

Dependendo do nível de maturidade do processo de gerenciamento de riscos da organização e dos recursos aos quais a atividade de auditoria interna tem acesso, as funções e responsabilidades pelo gerenciamento de riscos serão distribuídas de forma diferente na organização.

Com base em seu nível de desenvolvimento e acesso a recursos, uma organização pode se encontrar em diferentes áreas do processo de maturidade:

1 – Inicial. Em organizações nas quais o processo de gerenciamento de riscos está em estágios iniciais de desenvolvimento, a atividade de auditoria interna pode estar mais ativamente envolvida do que quando o processo é mais maduro. Nesse nível de maturidade, as atividades de gerenciamento de riscos específicos podem não ser executadas pela gerência de linha/operacional ou por funções com papéis de controle, conformidade, jurídico, gerenciamento de riscos ou avaliação interna de qualidade. Em vez disso, essas funções podem se basear nas avaliações de riscos da atividade de auditoria interna e na avaliação e consultoria com base em riscos.

2 – Repetível. Nesse nível, a atividade de auditoria interna é organizada de melhor forma e provida de recursos, e desempenha um papel instrumental em realizar avaliações baseadas em riscos, talvez de maior alcance. A atividade de auditoria interna pode trabalhar com as funções de controle, conformidade, jurídico, gerenciamento de riscos e avaliação interna de qualidade, agregando sua expertise em auditoria interna para auxiliar os proprietários dos riscos nas funções de gestão de linha/operacional a construir e monitorar controles operacionais. Esse estágio é suficiente para muitas organizações, se o processo estiver operando de forma consistente, eficiente e fornecendo resultados acionáveis, que auxiliem na conquista das metas e objetivos da organização.

3 – Definido. As organizações que estão na metade do modelo podem ter uma mistura de níveis de maturidade, com algumas unidades de negócios operando em níveis mais altos de maturidade do que outras. Nessa estrutura, as funções de controle, conformidade, jurídico, gerenciamento de riscos e avaliação interna de qualidade da organização podem ser proprietárias do processo de gerenciamento de riscos e ter responsabilidades que permaneçam consistentemente nos níveis Gerenciado e Otimizado, por exemplo. As funções de controle e avaliação podem desempenhar um papel ativo na assistência à gerência de linha/operacional, para avaliar os riscos e executar outras atividades de gerenciamento de riscos. A atividade de auditoria interna pode continuar operando funcionalmente no nível Repetível.

4 – Gerenciado. Subindo no modelo de maturidade, em organizações que tenham atingido um nível significativo de maturidade, a gerência de linha/operacional é proprietária e gerencia os riscos em toda a organização, e é responsável pela implantação de ações corretivas para abordar as atividades de processo e controle. A atividade de auditoria interna atua principalmente como uma função de avaliação independente, avaliando a eficácia do processo de gerenciamento de riscos entre as outras funções de gerenciamento e avaliação.

5 – Otimizado. Em organizações que tenham atingido esse nível de integração, sofisticação e maturidade, a gerência de linha/operacional é proprietária do processo de gerenciamento de riscos. As funções de conformidade e/ou gerenciamento de riscos da organização realizam avaliações de riscos para uso próprio. Também podem monitorar as avaliações de riscos e relatórios produzidos pela gerência de linha/operacional e podem questionar as informações de risco conforme necessário. Os riscos são monitorados e gerenciados em diversos processos de negócios.

Recurso

Para mais informações sobre a determinação de papéis e responsabilidades de gerenciamento de riscos, consulte o Guia Prático do The IIA "Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação".

A atividade de auditoria interna, como uma função de avaliação independente, conduz trabalhos para avaliar se os processos de gerenciamento de riscos são eficazes em áreas individuais e gerais na organização. Além disso, a atividade de auditoria interna pode comparar suas avaliações de riscos com as informações de risco produzidas pela administração e verificadas pelas funções internas de avaliação (conformidade/gerenciamento de riscos), para avaliar a exatidão e a integralidade da avaliação da administração. Por outro lado, a atividade de auditoria interna pode usar as informações de risco da administração para informar as avaliações de riscos da auditoria interna, ou pode fazer as duas coisas conforme apropriado. O CAE deve coordenar com outros prestadores de serviços de avaliação e consultoria e pode considerar confiar em seu trabalho (Norma 2050 – Coordenação e Confiança).

Cultura

A eficácia e abrangência de um processo de gerenciamento de riscos dependem da cultura de risco da organização. Se a cultura não for favorável à discussão aberta e à consideração do risco nos sentidos negativo e positivo da palavra, o processo de gerenciamento de riscos falhará. Os auditores internos devem perguntar: "se nenhuma política existisse, como a administração operaria?" Uma organização pode ter políticas e procedimentos afirmando que o gerenciamento de riscos será considerado, mas a cultura pode ofuscar a intenção e negar qualquer conversa ou ação séria.

As organizações podem ter processos sofisticados para mensurar e avaliar riscos, mas a cultura pode não ser favorável ao gerenciamento de riscos. Em indústrias reguladas, pode ser necessário um processo de gerenciamento de riscos operacionais, mas se o foco da administração estiver sobre simplesmente riscar itens em um checklist, é improvável que o processo de gerenciamento de riscos atinja um nível de maturidade onde as informações de risco sejam integradas à tomada de decisões (e ligadas à compensação e incentivos), agregadas e amplamente divulgadas em toda a organização.

Se os auditores internos estiverem envolvidos na criação de um processo de gerenciamento de riscos e determinarem que a cultura organizacional não apoia o esforço, devem levar a questão ao

CAE, que pode discutir a viabilidade do processo com a alta administração e o conselho. Mesmo que o tom no topo apoie o gerenciamento de riscos, pressionar a administração em uma organização resistente a cooperar com um programa de gerenciamento de riscos raramente vale a pena. A administração deve entender o valor do gerenciamento de riscos para que promova o processo.

Governança

Para que um processo de gerenciamento de riscos seja bem-sucedido, o apoio do topo deve ser estabelecido desde o início. Para conseguir a adesão e a alocação adequada de recursos, as informações de risco devem ser usadas na tomada de decisões nos níveis mais altos da organização. O interesse das entidades de alto nível, como o comitê de auditoria do conselho, é fundamental para criar demanda para a coleta, avaliação e fornecimento de informações de risco. Se o comitê de auditoria solicitar informações de risco regularmente, enquanto desempenham seu papel de supervisão, a administração deve encontrar uma forma de fornecê-las.

Em geral, o processo de gerenciamento de riscos é desenvolvido de cima para baixo, com a alta administração e o conselho exigindo avaliações de riscos e relatórios primeiro, geralmente levando a gerência comercial a adotar as mesmas práticas mais tarde, fornecendo informações de risco à alta administração. Uma vez que os principais gerentes comerciais, a alta administração e o conselho estejam envolvidos no processo de gerenciamento de riscos, a estrutura pode ser esclarecida e as políticas, procedimentos, relatórios e protocolos de escalonamento podem ser implantados.

Processo

O nível de integração das atividades de gerenciamento de riscos a outros processos de negócios é um indicador útil do nível de maturidade da organização. Quando as avaliações de riscos são comuns em toda a organização, o apetite a risco é comunicado com eficácia a todos os níveis e as informações de risco são usadas na tomada de decisões importantes, a organização é considerada mais madura do que uma organização que realiza avaliações de riscos uma vez por ano ou apenas conforme exigido pelos regulamentos. A **Figura 2** ilustra as diferenças. Este exemplo é representativo, não absoluto.

Figura 2: Amostra de Descrições para o Modelo de Maturidade

1 – Inicial	
Apetite a risco	O apetite a risco da organização está implícito, mas não está claramente definido ou documentado. A alta administração pode ter ideias semelhantes sobre o nível de risco que a organização está disposta a aceitar.
Avaliação de riscos	Os auditores internos podem conduzir avaliações de riscos para coletar informações de risco para seus trabalhos, para uso das funções de controle/conformidade/ avaliação interna e/ou para uso da administração. A administração não investiu na contratação ou treinamento de profissionais com habilidades de facilitação e avaliação de riscos, e os auditores internos podem ser a única equipe envolvida na avaliação de riscos. Os riscos são avaliados conforme necessário; por ex., a alta administração pode avaliar os riscos relacionados às estratégias propostas uma vez por ano. Projetos grandes e caros podem exigir avaliações de riscos conforme necessário.
Linguagem comum	A administração usa as informações de risco quando estão disponíveis, mas a terminologia não é consistente ou é mal interpretada em toda a organização. Diferentes registros e critérios de mensuração de riscos podem existir, dependendo do foco da avaliação de riscos. Os critérios de mensuração de riscos são simplistas, como classificações de alto, médio ou baixo.
Uso das informações de risco	As informações de risco não são agregadas ou comunicadas além do grupo específico que realizou a avaliação de riscos.
2 – Repetível	
1 – Inicial	O apetite a risco da organização foi abordado pela alta administração e pelo conselho e está documentado, mas não é compartilhado em toda a organização. O tópico é atualizado inconsistentemente.
2 – Repetível	Os auditores internos conduzem avaliações de riscos para coletar informações para seus trabalhos, para uso das funções de controle/conformidade/avaliação interna e/ou para uso da administração. A administração não investiu na contratação ou treinamento de profissionais com habilidades de facilitação e avaliação de riscos. Os riscos são avaliados de forma consistente, mas falta um plano estratégico abrangente. Projetos grandes e caros podem ser tratados como avaliações de riscos pontuais.
3 – Definido	A administração usa as informações de risco quando estão disponíveis, mas a terminologia é inconsistente na organização. Diferentes registros e critérios de mensuração de riscos podem existir, dependendo do foco das avaliações de riscos. Os critérios de mensuração de riscos podem considerar probabilidade e impacto e podem ser tão simples quanto as classificações de alta, média ou baixa.
4 – Gerenciado	As informações de risco são, algumas vezes, agregadas ou comunicadas além do grupo específico que realizou a avaliação de riscos.

Figura 2: Amostra de Descrições para o Modelo de Maturidade (continuação)

3 – Definido	
1 – Inicial	A alta administração e o conselho definiram vagamente um apetite a risco, que pode ou não ser bem compreendido por toda a organização.
2 – Repetível	As funções de controle/conformidade/gerenciamento de riscos/avaliação interna podem realizar avaliações de riscos para suas áreas ou para uso da administração. A administração não investiu na contratação ou treinamento de profissionais com habilidades de facilitação e avaliação de riscos. Avaliações de riscos podem ser conduzidas conforme necessário. Por exemplo, a alta administração pode solicitar uma avaliação de riscos para um grande projeto de capital, que apresente exposição a risco significativa para a organização.
3 – Definido	A administração usa as informações de risco quando estão disponíveis, e a terminologia é, em sua maioria, consistente na organização. Há múltiplos registros e critérios de mensuração de riscos.
4 – Gerenciado	Os riscos podem estar vinculados aos objetivos de um departamento ou equipe de projeto, mas nem sempre são considerados abertamente pelos níveis mais altos da organização.
4 – Gerenciado	
1 – Inicial	A alta administração e o conselho definiram um apetite a risco que é bem compreendido por toda a organização.
2 – Repetível	As funções de controle/conformidade/avaliação interna conduzem avaliações de riscos regularmente para suas áreas ou para uso da administração. A administração investiu na contratação e treinamento de profissionais com habilidades de facilitação e avaliação de riscos. As avaliações de riscos são conduzidas conforme necessário e podem abordar riscos significativos conforme surgem, em vez de depender de um plano de auditoria baseado em riscos.
3 – Definido	A alta administração solicita e usa consistentemente informações de risco, e a terminologia é bem conhecida e usada em toda a organização. Os critérios de gerenciamento de riscos são compreendidos e implantados em toda a organização.
4 – Gerenciado	Riscos significativos estão vinculados aos objetivos da organização. As informações de risco são comunicadas à alta administração de forma consistente, e a compensação e os incentivos da administração podem estar vinculados a indicadores chave de desempenho (*key performance indicators* – KPIs), orientados pelos riscos identificados e avaliados. As informações são usadas para contribuir para melhorar o processo de gerenciamento de riscos em toda a organização.

Figura 2: Amostra de Descrições para o Modelo de Maturidade (continuação)

5 – Otimizado	
1 – Inicial	Uma vez que o apetite a risco tenha sido aprovado pelo conselho, a administração e principais funcionários implantam-no em toda a organização, em um formato e nível de detalhes apropriados para a tomada de decisões.
2 – Repetível	A administração usa um processo comum para conduzir avaliações de riscos, documentar informações de risco e monitorar seu desempenho em relação aos KPIs ajustados pelo risco. A administração possui protocolos em vigor para garantir que riscos significativos sejam abordados quando surgirem, e não durante ou após a próxima avaliação de riscos programada.
3 – Definido	Toda a organização, desde o conselho até a gerência operacional e os funcionários, tem um entendimento comum dos termos usados no processo de gerenciamento de riscos (por ex., risco, fator contribuinte, controle, impacto, probabilidade) e usa uma linguagem comum para discutir o risco.
4 – Gerenciado	Os riscos estão vinculados aos objetivos da organização em todos os níveis. Além disso, as informações de risco são comunicadas a toda a organização de forma contínua, e a compensação e os incentivos da administração estão vinculados a KPIs orientados pelos riscos identificados e avaliados.

O Papel da Auditoria Interna no Gerenciamento de Riscos

A Norma 2120 - Gerenciamento de Riscos afirma que "a atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos." Especificamente, a norma exige que a atividade de auditoria interna avalie se:

- Os objetivos da organização dão suporte e estão alinhados à missão da organização.
- Os riscos significativos são identificados e avaliados.
- Respostas apropriadas aos riscos são selecionadas, de forma a alinhar os riscos ao apetite a risco da organização.
- As informações de risco relevantes são capturadas e comunicadas de forma tempestiva através da organização, incluindo o conselho.

Para realizar essa avaliação, a atividade de auditoria interna pode reunir as informações durante vários trabalhos e considerar os resultados desses trabalhos cumulativamente, para obter um entendimento completo dos processos de gerenciamento de riscos da organização e avaliar sua eficácia. A atividade de auditoria interna também deve garantir que a administração tenha atividades em andamento para monitorar os processos de gerenciamento de riscos.

A atividade de auditoria interna pode ser chamada para cumprir funções adicionais no gerenciamento de riscos. Se a atividade de auditoria interna for solicitada a ajudar na criação de processos de gerenciamento de riscos (por ex., condução e documentação de avaliações de risco), podem surgir dúvidas quanto à independência. Para ter clareza sobre os papéis

apropriados, os auditores internos devem revisar a série de normas que começa com a 1100 – Independência e Objetividade, prestando atenção especialmente à Norma 1130 – Prejuízo à Independência ou à Objetividade e suas normas associadas de avaliação e consultoria. Essas normas diferenciam as atividades apropriadas para trabalhos de avaliação daquelas apropriadas para trabalhos de consultoria. Por exemplo, presume-se que a objetividade esteja prejudicada se um auditor interno prestar serviços de avaliação sobre uma atividade pela qual teve responsabilidade no ano anterior (Norma 1130.A1).

A Norma 1112 – Funções do Executivo Chefe de Auditoria Além da Auditoria Interna reconhece que os CAEs podem ser convidados a assumir funções e responsabilidades além da auditoria interna, tais como atividades de conformidade ou gerenciamento de riscos. A norma afirma que "nos casos em que o executivo chefe de auditoria assumir, ou houver a expectativa de que assuma, funções e/ou responsabilidades que estejam além das de auditoria interna, salvaguardas devem ser colocadas em prática para limitar o prejuízo à independência ou à objetividade". As salvaguardas são atividades de supervisão, geralmente conduzidas pelo conselho, para tratar possíveis deficiências. Se o CAE tiver responsabilidade pelo gerenciamento de riscos ou funções relacionadas, então a avaliação sobre essas funções deve ser supervisionada por uma parte externa à atividade de auditoria interna (Norma 1130.A2).

Algumas organizações podem ver o papel da auditoria interna na criação de processos de gerenciamento de riscos como um serviço de consultoria, que não impactaria sua independência. Entretanto, a Norma 1130.C1 e a Norma 1130.C2 devem ser levadas em consideração, e os auditores internos devem divulgar possíveis prejuízos, se existirem. Outra opção é criar equipes de auditoria separadas, com uma equipe trabalhando em processos de gerenciamento de riscos, enquanto a outra avalia a eficácia desses processos. Outra opção é permitir que os auditores internos desenvolvam os processos de gerenciamento de riscos com um plano para entregar a operação e supervisão desses processos a profissionais treinados nas funções de conformidade/gerenciamento de riscos/avaliação interna ou para a gerência de linha/operacional.

Avaliando o Gerenciamento de Riscos da Organização

De acordo com a Norma 2200 - Planejamento do Trabalho de Auditoria, os auditores internos devem desenvolver e documentar um plano para cada trabalho, incluindo os objetivos, escopo, tempo e alocação de recursos para o trabalho. O plano deve considerar as estratégias, objetivos e riscos da organização que sejam relevantes para o trabalho.

Esta seção destina-se a orientar os auditores internos quanto ao processo de planejamento e execução de uma avaliação do gerenciamento de riscos da organização. Os exemplos fornecidos, embora não absolutos, devem ajudar os auditores internos a determinar as principais áreas a incluir, os tipos de documentos que podem ser solicitados e as evidências que podem ser obtidas.

Pode ser difícil avaliar um processo inteiro de gerenciamento de riscos; em vez disso, o escopo do trabalho pode ser definido usando critérios que atendam a um objetivo específico. Por

exemplo, o escopo pode ser definido por unidades organizacionais, locais, objetivos estratégicos ou por outros critérios que sejam significantes para a organização.

Entender o Contexto e o Propósito do Trabalho

Conforme ilustrado no modelo de maturidade do gerenciamento de riscos (**Figura 1**), as estruturas e processos definitivos de governança geralmente apoiam o processo de gerenciamento de riscos em uma organização com a cultura voltada para o risco. Por outro lado, uma organização pode não ter estruturas ou processos dedicados ao gerenciamento de riscos.

Em uma avaliação do gerenciamento de riscos da organização, o trabalho de auditoria interna consiste em duas partes: primeiro, identificar os princípios em funcionamento no processo de gerenciamento de riscos da organização e, em seguida, avaliar se esses princípios são apropriados e eficazes.

Ao planejar a avaliação, os auditores internos devem consultar o Guia de Implantação da Norma 2120 - Gerenciamento de Riscos, e considerar os seguintes elementos:

- Os planos estratégicos e de negócio, missões e objetivos da organização.
- Quaisquer frameworks de gerenciamento de riscos usados dentro da organização.
- Métodos atuais e nível de identificação, avaliação e provisão de supervisão dos riscos.
- Processos que possam ser usados para monitorar, avaliar e responder a riscos e oportunidades.
- Sofisticação da organização e de seus processos de gerenciamento de riscos, considerando seu porte, complexidade, ciclo de vida, maturidade, estrutura de stakeholders e ambiente legal e competitivo.
- Robustez das funções, responsabilidades e atividades de gerenciamento de riscos em toda a organização.
- Resultados atuais das atividades de monitoramento de riscos, e identificação e discussão sobre os riscos e respostas correspondentes que foram escolhidas.
- Riscos historicamente vivenciados.

Passos típicos para planejar um trabalho

- Entender o contexto e o propósito do trabalho.
- Coletar informações para entender a área ou processo sob revisão.
- Realizar uma avaliação preliminar de riscos da área ou processo sob revisão.
- Formular os objetivos do trabalho.
- Estabelecer o escopo do trabalho.
- Alocar recursos.
- Documentar o programa de trabalho.

O Guia Prático do The IIA "Planejamento do Trabalho: Estabelecendo Objetivos e Escopo" fornece orientação detalhada sobre como planejar e dimensionar um trabalho de auditoria.

- Quaisquer alterações (regulamentos, estruturação de equipe, processos, ou produtos e serviços) que possam ter introduzido novos riscos.
- Possíveis exposições e oportunidades de risco; incluindo avanços, tendências, riscos emergentes e possíveis disrupções relacionadas à organização (e à sua jurisdição e indústria).
- Quaisquer requisitos/expectativas regulatórias ou externas de outra natureza, que sejam relevantes para a organização e as jurisdições em que atua.
- As expectativas dos stakeholders em relação à atividade de auditoria interna e sua prestação de avaliação de que o processo de gerenciamento de riscos da organização é eficaz.

Uma questão fundamental para a atividade de auditoria interna explorar é se a administração articulou objetivos de gerenciamento de riscos. Os auditores internos devem buscar evidências de que a administração está executando atividades para atingir esses objetivos. Além disso, os auditores internos devem ter clareza sobre, entre outras coisas, a visão da administração para o processo de gerenciamento de riscos, seus planos e as metodologias de mensuração que emprega.

Ao desenvolver o plano do trabalho individual, os auditores internos coletam informações por meio de procedimentos como a revisão de avaliações anteriores (por ex., avaliações de riscos, relatórios de prestadores de serviços de avaliação e consultoria), entendimento e mapeamento dos fluxos e controles de processos de gerenciamento de riscos, e entrevistas com stakeholders relevantes. As informações obtidas através do planejamento devem ser bem documentadas, prontamente atualizadas e levadas em consideração durante todo o trabalho. As informações também podem ser úteis no planejamento de longo prazo do CAE para futuros trabalhos.

Coletar Informações Para Entender o Processo de Gerenciamento de Riscos

Depois que os auditores internos tiverem identificado os departamentos, funções e papéis na organização que são relevantes para o trabalho, eles devem coletar informações para apoiar uma avaliação preliminar de riscos e planejar o trabalho, conforme descrito na Norma 2201 – Considerações para o Planejamento.

Os elementos a seguir podem ajudar os auditores internos a identificar os riscos à organização e as estratégias usadas para gerenciar esses riscos:

- Estatutos, políticas e outras informações de mandato das entidades de governança responsáveis por estabelecer a estratégia de gerenciamento de riscos.
- Documentação do processo de gerenciamento de riscos, incluindo políticas, diretrizes e normas.
- Declaração(ões) de apetite a risco.
- Documentos de estratégia.
- Relatórios de controle ou outros relatórios gerenciais que contenham informações de desempenho.

- Ata das reuniões do conselho/comitê de auditoria e de outros comitês relevantes (por ex., comitê de riscos).
- Casos de negócio de projetos de capital significantes.
- Relatórios periódicos externos (isto é, declarações 10K de empresas públicas).
- Avaliações de riscos da administração.
- Inventário de riscos à organização, incluindo riscos estratégicos, operacionais, de recursos humanos, financeiros, de conformidade regulatória e de TI.
- Documentação de todas as fases do processo de gerenciamento de riscos, incluindo identificação, avaliação, tratamento e monitoramento dos riscos.
- Resultados das atividades de monitoramento de riscos.

Conforme observado no Guia Prático do The IIA "Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação", o gerenciamento de riscos em uma organização é responsabilidade de todos; portanto, as informações de risco devem estar disponíveis para todas as áreas de negócios, embora possam não estar oficialmente documentadas ou prontamente aparentes. Às vezes, os riscos podem ser avaliados abertamente, como durante o planejamento estratégico. No entanto, riscos podem ser identificados em lugares menos óbvios, como em uma citação em um caso de negócios (por ex., "esse projeto pode gerar menos receita do que o desejado, por causa desses fatores..."). Para identificar tantos riscos quanto possível, os auditores internos devem usar mais do que apenas relatórios de trabalhos anteriores ou avaliações limitadas a riscos óbvios.

Consideração de Auditoria

Os auditores internos podem escolher avaliar os processos de gerenciamento de riscos no contexto de trabalhos individuais dentro do plano de auditoria interna, ou como parte de uma avaliação especial de processos identificados como relacionados a riscos.

O Guia Prático do The IIA "Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação" pode ajudar os auditores internos a identificar processos relacionados aos riscos.

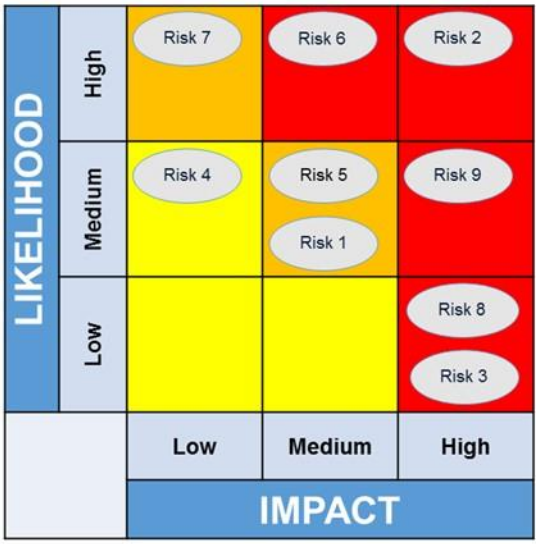
Realizar uma Avaliação Preliminar de Riscos

A Norma 2210.A1 declara que "os auditores internos devem conduzir uma avaliação preliminar dos riscos relevantes para a atividade sob revisão. Os objetivos do trabalho de auditoria devem refletir os resultados dessa avaliação". A abordagem para avaliar os riscos associados ao processo de gerenciamento de riscos de uma organização frequentemente difere da abordagem das avaliações preliminares de riscos conduzidas no planejamento de outros tipos de trabalhos.

Uma forma eficaz de realizar e documentar uma avaliação de riscos no nível do trabalho é criando uma matriz de riscos que liste os riscos relevantes e, depois, expandindo a matriz para incluir métricas de importância. O formato da matriz pode variar, mas normalmente inclui uma linha para cada risco e uma coluna para cada métrica de risco, como impacto e probabilidade.

Em organizações que têm um processo de gerenciamento de riscos amadurecido e extenso, a atividade de auditoria interna pode ser capaz de revisar e usar a avaliação de riscos da administração, em vez de recriar uma. Ao vincular a avaliação do processo de gerenciamento de riscos ao modelo de maturidade, os auditores internos deixam claro que a avaliação de riscos é um elemento essencial para a determinação da maturidade do gerenciamento de riscos. Se a administração ainda não o fez, os auditores internos podem desenvolver uma lista de riscos ao processo de gerenciamento de riscos que se enquadrem nas categorias do modelo de maturidade de cultura, governança e processo (veja, no Anexo D, um exemplo de matriz de riscos e controle que inclui essas categorias). Esses riscos podem, então, ser classificados em termos de impacto e probabilidade. O mapa de calor, como o exemplo na **Figura 3**, é uma ferramenta usada para representar visualmente a significância do risco em uma escala simples de alta, média e baixa.

Figura 3: Mapa de Calor



Além disso, o mapa de calor pode ser mantido como documentação de apoio ao plano de trabalho e ao programa de trabalho, em conformidade com a Norma 2240 – Programa de Trabalho de Auditoria.

Formular os Objetivos do Trabalho

A Norma 2210 – Objetivos do Trabalho de Auditoria afirma que "os objetivos devem ser estabelecidos para cada trabalho de auditoria". As normas de avaliação 2210.A1 e 2210.A2 acrescentam que os objetivos do trabalho de avaliação devem refletir os resultados de uma

avaliação preliminar de riscos e devem considerar a probabilidade de exposições significantes a risco, incluindo erros, fraude e não conformidade.

O objetivo geral de uma avaliação do processo de gerenciamento de riscos da organização é, tipicamente, fornecer informações para a alta administração e o conselho sobre a maturidade do gerenciamento de riscos da organização, e se corresponde às suas expectativas. Esse tipo de avaliação também pode incluir o benchmarking, ou comparação com as melhores práticas selecionadas ou endossadas pela alta administração e pelo conselho.

Para um trabalho de avaliação, de acordo com a Norma 2210.A3, são necessários critérios adequados para avaliar o gerenciamento de riscos e, se os auditores internos concluírem que a alta administração e o conselho já estabeleceram critérios adequados (ou seja, se houver um framework de gerenciamento de riscos), esses critérios devem ser usados para a avaliação. Se não houver critérios adequados de avaliação, os auditores internos trabalharão com a administração e/ou com o conselho para desenvolver as métricas. Os tipos de critérios de avaliação podem incluir:

- Internos (ex., políticas e procedimentos da organização).
- Externos (ex., leis e regulamentos impostos por órgãos estatutários).
- Práticas de liderança (ex., orientações industriais e profissionais).

Os auditores internos podem adaptar o modelo de maturidade apresentado anteriormente para refletir esses critérios conforme apropriado para suas organizações. Os requisitos externos podem ser combinados com práticas de liderança da indústria, integradas ao modelo de maturidade e comparadas às políticas e procedimentos internos da organização.

Para organizações menos amadurecidas, um trabalho de consultoria pode ser mais apropriado e os objetivos do trabalho podem ser acordados com a alta administração e/ou com o conselho. Em trabalhos de consultoria, o objetivo poderia de natureza mais consultiva; por ex., criar conscientização sobre o valor da implantação de processos mais formais de gerenciamento de riscos.

Estabelecer o Escopo do Trabalho

O CAE ou auditores internos designados pelo CAE devem estar envolvidos em reuniões de toda a organização relativas a riscos e gerenciamento de riscos, o que pode ajudar a orientar a abordagem da atividade de auditoria interna para o escopo de avaliação. Conforme exigido pela Norma 2220 - Escopo do Trabalho de Auditoria, o escopo deve ser suficiente para atingir os objetivos do trabalho.

No mínimo, o escopo de qualquer avaliação relacionada ao gerenciamento de riscos deve confirmar se quaisquer processos relacionados aos riscos identificados são seguidos e estão em conformidade com critérios externos (por ex., leis, regulamentos, requisitos da indústria). Quando definir o escopo de trabalhos, os auditores internos podem considerar:

1. A suficiência e a eficácia operacional das políticas, procedimentos e atividades que apoiam o processo de gerenciamento de riscos, incluindo o alinhamento com o apetite a risco da organização, as expectativas dos stakeholders e as normas do setor.
2. A eficácia das estruturas de governança que apoiam as políticas, procedimentos e atividades relacionados ao processo de gerenciamento de riscos.
3. A adequação dos recursos dedicados ao suporte do processo de gerenciamento de riscos.
4. A inclusão dos seguintes elementos no processo de gerenciamento de riscos:
    - Papéis e responsabilidades de gerenciamento de riscos claramente definidas em toda a organização.
    - Consideração explícita dos riscos na estratégia da organização.
    - Listas/registros de riscos, critérios de classificação de riscos e processos de avaliação de riscos.
    - Expectativas relacionadas ao tratamento dos riscos.
    - Reporte exigido das exposições a risco.
    - Processos de classificação, escalonamento e rastreamento das descobertas resultantes das atividades de monitoramento de riscos.

Embora todos esses elementos devam estar presentes de alguma forma como parte do processo de gerenciamento de riscos, os auditores internos podem personalizar o escopo para adequá-lo aos recursos e necessidades específicos da organização ou do trabalho individual.

Alocar Recursos

Depois que os objetivos e o escopo de um trabalho tiverem sido estabelecidos, o CAE ou os auditores internos designados para o trabalho devem considerar a natureza e a complexidade do trabalho, as restrições de tempo e os recursos disponíveis e, então, determinar se a quantidade de recursos e a combinação de competências disponíveis são suficientes para executar o trabalho com zelo profissional devido (Norma 2230 – Alocação de Recursos ao Trabalho de Auditoria).

Para avaliar a eficácia de um processo de gerenciamento de riscos, os auditores internos devem conhecer os requisitos de gerenciamento de riscos da indústria da organização, bem como estar familiarizados com uma variedade de frameworks de risco e controle, e entender a cultura da organização e outros controles informais do **ambiente de controle** da organização.

Como a avaliação do processo inteiro de gerenciamento de riscos de qualquer organização é um exercício intensivo, tanto de esforço quanto de tempo, o CAE deve desenvolver uma abordagem de trabalho que seja razoável em termos de recursos. Para garantir que os recursos sejam adequados, esses trabalhos podem ser abordados de diversas maneiras, conforme mostrado na **Figura 4**, dependendo da estrutura da organização. Essa lista não inclui todos os exemplos que podem ser apropriados.

Figura 4: Exemplos de Abordagens de Trabalho

Abordagem *Top-Down*	
Método(s) mais eficaz(es) de coleta de informações	■ Entrevistas. ■ Revisões de documentos.
Participantes típicos	■ Membros do conselho (por ex., presidentes do comitê de auditoria e/ou do comitê de riscos). ■ Alta administração. ■ Gerência do grupo/divisão.
Limitações	■ O nível de detalhes coletados é baixo. ■ A avaliação pode ter um foco sobre a governança, por conta do grupo de participantes. ■ As visões do conselho e da alta administração podem não representar as visões do restante da organização, principalmente quanto à cultura.
Abordagem *Bottom-Up*	
Método(s) mais eficaz(es) de coleta de informações	■ Entrevistas. ■ Pesquisas. ■ Revisões de documentos. ■ Apresentações de *walk-through*.
Participantes típicos	■ Gerentes de linha. ■ Supervisores.
Limitações	■ As pesquisas podem gerar confusão, se não tiverem uma linguagem ou um processo de risco comum. ■ O feedback pode ser distribuído inconsistentemente entre os participantes. ■ Muitos gerentes de linha e supervisores podem não conseguir participar, por conta de restrições de tempo/recursos (o que pode ser um indicador da prioridade dada ao processo de gerenciamento de riscos).
Abordagem Combinada	
Método(s) mais eficaz(es) de coleta de informações	■ Entrevistas (profissionais de níveis superiores). ■ Pesquisas (profissionais de níveis inferiores). ■ Revisões de documentos.
Participantes típicos	■ Membros do conselho (por ex., presidentes do comitê de auditoria e/ou do comitê de riscos). ■ Alta administração. ■ Gerência do grupo/divisão. ■ Gerentes de linha.
Limitações	■ Embora essa abordagem deva possibilitar uma visão mais abrangente, qualquer uma das limitações mencionadas acima ainda é aplicável.

Documentar o Programa de Trabalho

Durante o planejamento, os auditores internos documentam informações em papéis de trabalho. Essas informações tornam-se parte do programa de trabalho que deve ser criado para atingir os objetivos do trabalho (Norma 2240 – Programa de Trabalho de Auditoria).

O processo de estabelecer os objetivos e o escopo do trabalho pode produzir um ou todos os seguintes papéis de trabalho:

- Mapas de processo.
- Registros de riscos.
- Resumo de entrevistas e pesquisas.
- Justificativas das decisões relacionadas ao nível de maturidade do gerenciamento de riscos da organização.
- Critérios que serão usados para avaliar o processo de gerenciamento de riscos.

Realizar o Trabalho e Reportar os Resultados

O Anexo E lista, em um nível geral, as atividades que os auditores internos podem realizar como parte de uma avaliação do processo de gerenciamento de riscos de uma organização. A série de normas 2300 (Execução do Trabalho de Auditoria) descreve os requisitos para identificar, analisar, avaliar e documentar informações suficientes para atingir os objetivos do trabalho.

O trabalho deve culminar em recomendações adequadas ao status atual e desejado da administração, de acordo com o modelo de maturidade. Os auditores internos devem seguir os procedimentos estabelecidos da atividade de auditoria interna para comunicar os resultados dos trabalhos, o que é detalhado na série de normas 2400 (Comunicação dos Resultados) e nos guias de implantação associados. Os auditores internos devem observar que, para estar em conformidade com a Norma 2410 – Critérios para as Comunicações e Norma 2410.A1, a comunicação final dos resultados do trabalho deve incluir os objetivos do trabalho, escopo, resultados, conclusões aplicáveis, recomendações e/ou planos de ação.

Para estar em conformidade com a Norma 2440 – Disseminação dos Resultados, o CAE deve garantir que os resultados sejam comunicados às partes apropriadas. Para avaliações dos processos de gerenciamento de riscos, isso pode envolver a elaboração de um relatório para a alta administração, o conselho e outras partes que considerem apropriadas. As comunicações podem ser adaptadas ao público que as receberá.

Avaliar o Processo de Gerenciamento de Riscos da Atividade de Auditoria Interna

Para avaliar a eficiência e a eficácia da atividade de auditoria interna e identificar oportunidades de melhoria, em conformidade com a Norma 1300 - Programa de Garantia da Qualidade e Melhoria, o CAE pode aplicar as lições aprendidas com as avaliações de auditoria interna do gerenciamento de riscos à toda a organização. A aplicação de um modelo de maturidade do gerenciamento de riscos (**Figura 1**) pode ajudar o CAE a melhorar o processo de gerenciamento de riscos da atividade de auditoria interna, e trabalhar para atingir níveis mais altos de maturidade em todo o espectro de categorias. O aumento da maturidade melhora os recursos de avaliação e consultoria da atividade de auditoria interna, permitindo que ela proteja e aprimore melhor o valor organizacional.

Anexo A. Normas e Orientações Relacionadas do IIA

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

Código de Ética
Princípio 1: Integridade
Princípio 2: Objetividade
Princípio 3: Confidencialidade
Princípio 4: Competência
Normas
Norma 1100 – Independência e Objetividade
Norma 1112 – Funções do Executivo Chefe de Auditoria Além da Auditoria Interna
Norma 1130 – Prejuízo à Independência ou à Objetividade
Norma 2050 – Coordenação e Confiança
Norma 2120 – Gerenciamento de Riscos
Norma 2200 – Planejamento do Trabalho de Auditoria
Norma 2201 – Considerações para o Planejamento
Norma 2210 – Objetivos do Trabalho de Auditoria
Norma 2220 – Escopo do Trabalho de Auditoria
Norma 2230 – Alocação de Recursos para o Trabalho de Auditoria
Norma 2240 – Programa de Trabalho de Auditoria
Norma 2300 – Execução do Trabalho de Auditoria
Norma 2400 – Comunicação dos Resultados
Norma 2410 – Critérios para as Comunicações
Norma 2440 – Divulgação dos Resultados

Orientações
Guia Prático “Relatórios de Auditoria: Comunicando Resultados dos Trabalhos de Auditoria,” 2016.
Guia Prático “Coordenação e Confiança: Desenvolvendo um Mapa de Avaliação”, 2018.
Guia Prático “Planejamento do Trabalho: Estabelecendo Objetivos e Escopo,” 2017.

Anexo B. Glossário

Os termos identificados com um asterisco (*) foram retirados do "Glossário" do *International Professional Practices Framework*® (*IPPF*®) do The IIA, edição de 2017.

ambiente de controle* – Atitudes e ações do conselho e da administração em relação à importância do controle dentro da organização. O ambiente de controle proporciona a disciplina e a estrutura para a realização dos principais objetivos do sistema de controle interno. O ambiente de controle inclui os seguintes elementos:

- Integridade e valores éticos.
- Filosofia e estilo operacional da administração.
- Estrutura organizacional.
- Atribuição de autoridade e responsabilidade.
- Políticas e práticas de recursos humanos.
- Competência do pessoal.

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

atividade de auditoria interna* – Um departamento, divisão, time de consultores ou outros profissionais que prestam serviços independentes e objetivos de avaliação e de consultoria projetada para agregar valor e melhorar as operações de uma organização. A atividade de auditoria interna auxilia uma organização a concretizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de risco e de controle.

chief audit executive* – *Chief audit executive* descreve a função de uma pessoa em uma posição de alto nível 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* (IPPF). O *chief audit executive* ou outros subordinados ao *chief audit executive* devem ter certificações e qualificações profissionais apropriadas. O título específico do cargo e/ou responsabilidades do *chief audit executive* podem variar entre as organizações.

conselho* – O corpo diretivo de mais alto nível (p.ex.: um conselho de administração, conselho fiscal ou um conselho de gestores ou de curadores) que detém a responsabilidade de dirigir e/ou supervisionar as atividades da organização e de cobrar a prestação de contas por parte da alta administração. Ainda que os sistemas de governança variem entre jurisdições e setores, normalmente o conselho inclui membros que não fazem parte da administração. Se um conselho não existir, 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 diretivo delegou certas funções (p. ex.: um comitê de auditoria).

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

modelo de maturidade – Um indicador em referência ao qual o estado atual de uma organização é mensurado e progride em direção ao domínio de uma determinada área.

Anexo C. Possíveis Cenários de Risco

Para garantir o sucesso organizacional e criar valor, todos os riscos organizacionais significantes, incluindo o risco de perda de oportunidades, devem ser claramente compreendidos, devidamente priorizados e tratados. Fazer a análise e avaliação devidas do processo de gerenciamento de riscos ajuda as organizações a implantar ações adequadas para evitar ou abordar cenários de risco, como os listados aqui, que podem comprometer sua capacidade de alcançar suas metas e objetivos:

- A avaliação independente oferecida ao conselho e à alta administração é inadequada e leva a um falso senso, entre os dois grupos, de que os riscos estão sendo gerenciados dentro do apetite a risco da organização e que apoiam devidamente a capacidade da organização de atingir seus objetivos e estratégias.
- A governança, sistemas e processos de gerenciamento de riscos falham, resultando na má governança corporativa e más classificações nas agências relacionadas, que são então comunicadas aos stakeholders e ao mercado.
- Ocorrem eventos de risco evitáveis, resultando em passivos, multas, sanções regulatórias e exposições relacionadas, bem como na perda de ativos, propriedade intelectual, participação de mercado, oportunidades de receita, fidelidade do cliente e reputação da marca.
- A alocação de recursos e atribuições de funções não são otimizadas; portanto, o gerenciamento de risco operacionalmente sustentável não pode ser estabelecido.
- A cultura da organização inibe o progresso em direção a um nível mais alto de maturidade no gerenciamento de riscos.
- Os riscos são ignorados, não são priorizados devidamente ou não são mitigados de forma eficaz, levando à ocorrência de eventos de risco que impedem o alcance dos objetivos e estratégias de negócio e organizacionais.
- As restrições de tempo e as oportunidades não são atendidas, devido ao gerenciamento indevido dos riscos.
- As prioridades e estratégias organizacionais não são estabelecidas com a devida conscientização dos riscos ou dos fatores de risco por trás das iniciativas.
- Os riscos de TI, recursos humanos e financiamento não são considerados e resultam em perdas financeiras ou operacionais, ou em falhas estratégicas.

Anexo D. Matriz de Riscos e Controle

A tabela a seguir lista algumas das principais áreas de riscos e controles que os auditores internos devem considerar ao avaliar o processo de gerenciamento de riscos da organização. A lista não é absoluta, nem deve ser usada como programa de trabalho ou checklist.

Riscos de Cultura

Riscos	Controles
■ Nenhum recurso foi alocado para expandir o gerenciamento de riscos. ■ O risco é visto como "de propriedade" das funções de auditoria interna e de controle. ■ É difícil agendar entrevistas e receber feedback de pesquisas em tempo hábil. ■ Más notícias não transitam para cima na hierarquia da organização. ■ O desafio de engajar toda a organização não foi previsto ou é maior do que o previsto. ■ A organização não reconhece como as pessoas reagem à mudança. ■ A organização considera o processo de gerenciamento de riscos como prescritivo. ■ A atividade de auditoria interna não reporta e explica com eficácia os resultados e classificações de riscos. ■ A administração teme a exposição ao risco. ■ As tradições culturais se opõem às metas e objetivos de gerenciamento de riscos.	■ A atividade de auditoria interna realiza workshops ou entrevistas para orientar os funcionários quanto ao processo de gerenciamento de riscos. ■ O conselho garante um tom no topo eficaz. ■ Fóruns confidenciais permitem que a equipe expresse questões culturais ou bloqueios à comunicação de informações sobre riscos. ■ A alta administração incentiva reuniões e discussões regulares e a troca de informações entre todos os níveis da administração. ■ A administração garante que o reporte de informações de riscos para cima na hierarquia da organização não resulte em retaliação.

Riscos de Governança

Riscos	Controles
■ As entidades (conselho, administração, reguladores) têm requisitos diferentes para o gerenciamento de riscos. ■ Não há sistema padrão de reporte para questões de gerenciamento de riscos (por ex., tempestividade, formato). ■ A administração não fala sobre riscos regularmente nas reuniões. ■ O conselho não desempenha adequadamente seu papel de supervisão.	■ Os critérios internos e externos de gerenciamento de riscos são conhecidos e incorporados ao processo. ■ A organização investe em software de reporte de riscos. ■ O conselho e a alta administração criam demanda por informações de riscos em toda a organização.

Anexo D (continuação)

Riscos de Processo	
Riscos	**Controles**
▪ O processo de avaliação de riscos é inconsistente em toda a organização. ▪ Riscos demais foram identificados. ▪ Os resultados dos riscos não são monitorados. ▪ Os critérios de impacto e probabilidade diferem, mesmo para linhas de negócios semelhantes. ▪ Os tratamentos de riscos não são reportados além do nível do supervisor. ▪ A atividade de auditoria interna é a única entidade que realiza uma avaliação de riscos em toda a organização. ▪ O processo de gerenciamento de riscos envolve linguagem e termos que a equipe não entende. ▪ O nível exigido de quantificação (em números reais) da exposição a risco não é acordado. ▪ O foco sobre riscos emergentes é insuficiente.	▪ A organização concorda com o(s) framework(s) de gerenciamento de riscos a ser(em) usado(s). ▪ A organização investe recursos em agregar as informações de riscos e o reporte em intervalos regulares. ▪ As funções de controle (por ex., conformidade; jurídico; ambiental, saúde e segurança) são bem treinadas quanto ao processo de avaliação de riscos e o framework de gerenciamento de riscos adotado pela administração. ▪ Um glossário de termos relacionados ao gerenciamento de riscos e uma descrição do processo de avaliação de riscos são fornecidos antes que as avaliações de riscos sejam conduzidas. ▪ Matrizes de impacto e probabilidade são implantadas consistentemente em toda a organização.

Anexo E. Avaliando o Processo de Gerenciamento de Riscos

Em um nível geral, essas tabelas descrevem atividades que os auditores internos podem realizar como parte de uma avaliação do processo de gerenciamento de riscos da organização. Essas atividades não constituem um programa de trabalho completo para tal avaliação. Os auditores internos podem precisar criar análises mais detalhadas e etapas de teste adequadas às políticas e procedimentos exclusivos da organização. Para uma avaliação completa do processo de gerenciamento de riscos, os auditores internos também podem precisar criar programas de trabalho específicos para áreas relevantes (por ex., risco legal, risco de conformidade, planejamento estratégico), principalmente se a avaliação for dividida em trabalhos menores, conforme mencionado neste guia.

Cultura de Gerenciamento de Riscos

Reporte de Riscos

- Coletar documentação, incluindo:
  - Cartas, políticas e outras informações obrigatórias para as entidades de governança responsáveis por estabelecer e supervisionar o processo de gerenciamento de riscos.
  - Documentação de todas as fases do processo de reporte de risco.
- Compreender os principais riscos identificados relacionados aos objetivos da organização.
- Determinar se o reporte de risco comunica com precisão o status da exposição ao risco na organização (por ex., é complicado ou simples demais?).
- Classificar os riscos de acordo com a metodologia de avaliação de riscos estabelecida pela organização.
- Revisar as informações obtidas na avaliação preliminar de riscos, para avaliar o impacto e a probabilidade dos riscos relacionados à cultura de risco.

Comunicação

- Acompanhar o reporte dos riscos em várias áreas, para verificar se as informações de risco são comunicadas de forma fluida em todos os níveis da organização.
- Examinar as investigações sobre ética e conformidade relacionadas aos riscos, para determinar se a retaliação por comunicar informações sobre riscos é um problema.
- Usar pesquisas, entrevistas ou outros métodos, para determinar a participação dos funcionários em programas de comunicação e seu nível de compreensão dos objetivos de gerenciamento de riscos da organização.

Prestação de Contas

- Confirmar se os proprietários dos riscos são responsabilizados por exposições a risco em sua esfera de autoridade.
- Confirmar se o conselho e a alta administração são responsabilizados por solicitar e utilizar informações de risco na tomada de decisões.

Anexo E (continuação)

Governança do Gerenciamento de Riscos

Reporte de Riscos

- Usar as informações de risco reportadas para avaliar a cultura e examinar a adequação em termos de distribuição, monitoramento e retenção de dados.
- Revisar as informações obtidas na avaliação preliminar de riscos, para avaliar o impacto e a probabilidade dos riscos relacionados à governança do gerenciamento de riscos.

Reporte ao Conselho

- Revisar os relatórios relacionados a riscos que foram preparados para o conselho. Assegurar-se de que os relatórios contenham todas as informações pertinentes necessárias para que o conselho administrativo tome decisões informadas.
- Revisar os relatórios da alta administração sobre o status das exposições a risco quanto às estratégias e ao apetite a risco.

Apetite a Risco

- Revisar a integralidade e adequação do perfil de apetite a risco da organização, incluindo os seguintes componentes:
  - Capacidade de risco: O nível máximo de risco que a organização pode assumir, dadas suas obrigações e restrições atuais e seu nível de recursos disponíveis.
  - Limites de risco: A alocação de limites de apetite a risco agregado para as linhas de negócios, entidades legais, categorias de risco específicas e outros níveis granulares relevantes.
  - Tolerância a risco: A quantidade de variação das receitas e despesas etc., que a organização aceitará, dados os parâmetros definidos para a capacidade de risco e seus limites de risco associados.
- Revisar os planos e processos de comunicação do apetite a risco a todos os funcionários.
- Assegurar-se de que o plano cubra toda a organização e seja executado regularmente.
- Usar pesquisas, entrevistas ou outros métodos para determinar a participação dos funcionários em programas de comunicação e seu nível de entendimento do apetite a risco da organização.

Processo de Gerenciamento de Riscos

Políticas e Procedimentos

- Verificar se as políticas e procedimentos são atuais e atualizados em tempo hábil, quando ocorrem mudanças nos procedimentos.
- Confirmar se quaisquer atualizações solicitadas pelo conselho durante a revisão anual foram feitas adequadamente.
- Garantir que as políticas e procedimentos cubram todo o processo de gerenciamento de riscos em detalhes. Áreas específicas de importância incluem:
  - Relação com estratégias e apetite a risco.
  - Visão geral da governança.
  - Limites e tolerâncias a risco, com seus gatilhos associados e protocolos de escalonamento (revisar o processo desde a identificação de uma violação até sua resolução).
  - Papéis e responsabilidades.
  - Considerações de dados.
- Requisitos regulatórios.

Anexo E (continuação)

Processo de Avaliação de Riscos

- Identificar onde e com que frequência as avaliações de riscos são conduzidas em toda a organização.
- Examinar se os processos de identificação, avaliação, tratamento, monitoramento e reporte de riscos são consistentes.
- Revisar as informações obtidas na avaliação preliminar de riscos, para avaliar o impacto e a probabilidade dos riscos relacionados aos processos de gerenciamento de riscos em toda a organização.

Anexo F. Referências e Leituras Adicionais

Referências

International Professional Practices Framework (IPPF), edição de 2017. Lake Mary, FL: The Institute of Internal Auditors, 2017.

Leituras Adicionais

Anderson, Richard J. e Mark L. Frigo. *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors.* Lake Mary, FL: Internal Audit Foundation, 2017. https://bookstore.theiia.org/assessing-and-managing-strategic-risks.

Anderson, Urton e Andrew J. Dahle. *Applying the International Professional Practices Framework, 4ª edição*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/applying-the-international-professional-practices-framework4th-edition-2.

Baker, Larry L. *Practical Enterprise Risk Management: Getting to the Truth*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/practical-enterprise-risk-managementgetting-to-the-truth.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *COSO Enterprise Risk Management – Integrating with Strategy and Performance*. COSO, 2017. https://bookstore.theiia.org/enterprise-risk-management-integrating-with-strategy-andperformance.

Committee of Sponsoring Organizations of the Treadway Commission. *COSO Enterprise Risk Management – Integrating with Strategy and Performance: Compendium of Examples*. PwC, 2018. https://bookstore.theiia.org/coso-enterprise-risk-management-integrating-withstrategy-and-performance-compendium-of-examples.

International Organization for Standardization (ISO). ISO 31000:2018, *Risk management – Guidelines*. ISO, 2018. https://www.iso.org/standard/65694.html.

Sobel, Paul J. *Auditor's Risk Management Guide: Integrating Auditing and ERM, edição de 2015.* Wolters Kluwer, 2015.

Sobel, Paul J. *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework.* Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/managing-risk-inuncertain-times-2.

Agradecimentos

Equipe de Desenvolvimento de Orientações

Glenn Ho, CIA, CRMA, África do Sul (Presidente)

Hans-Peter Lerchner, CIA, Áustria (Líder do Projeto)

Susan Haseley, CIA, Estados Unidos

Rune Johannessen, CIA, CCSA, CRMA, Noruega

Ian Lyall, CIA, CCSA, CGAP, CRMA, Austrália

Michael Lynn, CRMA, Estados Unidos

Denis Neukomm, CIA, CRMA, Suíça

Contribuintes das Orientações Globais

Mohamed Ahmed Abdulla, Egito

Lance Johnson, CIA, CRMA, Estados Unidos

Cornelis Klumper, CIA, Estados Unidos

Steven Nyakatuura, CFSA, África do Sul

Tejinder Bob Shahi, CIA, Canadá

Rita Thakkar, CIA, Estados Unidos

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

Jeanette York, CCSA, Diretora de FS

Shelli Browning, Editora Técnica

Lauressa Nelson, Editora Técnica

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 ao 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 190.000 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

Março de 2019

The Institute of Internal Auditors | Global

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