IPPF - GUIAS PRÁTICOS

# COORDENANDO O GERENCIAMENTO E A AVALIAÇÃO DE RISCOS

Instituto dos Auditores Internos do Brasil

# Índice

# Sumário Executivo

O gerenciamento de riscos é fundamental para o controle organizacional e uma parte crítica para a condução de uma boa governança corporativa. Ele impacta todas as atividades da organização. O estabelecimento de um sistema de gerenciamento de riscos eficaz em toda a organização é uma responsabilidade chave da gerência e do conselho, que são responsáveis pela adoção de uma abordagem holística em relação à identificação de riscos organizacionais, criação de controles para mitigar esses riscos e monitorar e revisar os riscos e controles identificados. Eles devem garantir que o gerenciamento de riscos esteja integrado à organização, tanto no nível estratégico quanto operacional.

Com a responsabilidade por atividades de avaliação tradicionalmente compartilhada entre a gerência, a auditoria interna, o gerenciamento de riscos e o setor de *compliance*, é importante que as atividades de avaliação sejam coordenadas, para garantir que os recursos sejam usados de forma eficaz e eficiente. Muitas organizações operam com atividades tradicionais (e separadas) de auditoria interna, riscos e conformidade. É comum que as organizações tenham um certo número de grupos separados, conduzindo funções diferentes de gerenciamento de riscos, conformidade e avaliação, e independemente umas das outras. Sem coordenação e reporte eficazes, o trabalho pode ser duplicado ou riscos importantes podem passar despercebidos ou ser mal avaliados.

Muitas funções de auditoria interna trabalham em cooperação com o gerenciamento de riscos. Algumas organizações não têm uma função formal de gerenciamento de riscos e, nesse caso, a atividade de auditoria interna frequentemente presta serviços de consultoria em gerenciamento de riscos para a organização. A auditoria interna não deve dar sua avaliação independente com relação a qualquer parte da estrutura de gerenciamento de riscos pela qual ela seja responsável. Outras partes adequadamente qualificadas devem prestar tal avaliação.

# Introdução

A Norma 2050: Coordenação declara que "o Diretor Executivo de Auditoria (DEA) deve compartilhar informações e coordenar atividades com outros prestadores internos e externos de serviços de avaliação e consultoria, para assegurar a cobertura apropriada e a minimização da duplicação de esforços". Esta responsabilidade requer a inclusão e a participação do DEA na estrutura do fornecedor de avaliação da organização. Esta estrutura consiste da auditoria interna, auditoria externa, governança, gerenciamento de riscos ou outras funções/ divulgações de controle do negócio conduzidas pela equipe de gestão da organização. A inclusão e participação nesta estrutura ajudam a garantir que o DEA esteja ciente dos riscos e controles da organização com relação às metas e objetivos organizacionais.

Os conselhos contam com diversas fontes para obter avaliações confiáveis, incluindo a gerência, a auditoria interna e terceiros. Conforme discutido na Prática Recomendada 2050-2: Mapas de Avaliação, um mapa de avaliação é uma ferramenta valiosa para a coordenação das atividades de gerenciamento de riscos e avaliação, para aumentar a eficácia e a eficiência dos investimentos da organização na avaliação do gerenciamento de riscos.

# Gerenciamento de Riscos e Avaliação (Serviços de Avaliação)

O Glossário das *Normas Internacionais para a Prática Profissional de Auditoria Interna* (Normas) define o gerenciamento de riscos como um "processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer uma razoável certeza em relação ao cumprimento dos objetivos da organização". Isso é consistente com a definição de gerenciamento de riscos da *International Stardards Organization*: "atividades coordenadas para dirigir e controlar uma organização com relação a riscos".

O gerenciamento de riscos corporativos (*enterprise risk management* – ERM), também conhecido como gerenciamento de riscos da organização – é um termo comumente usado. O *Committee of Sponsoring Organizations of the Treadway Commission* o define como "um processo, aplicado pelo conselho de administração, gerência ou outro pessoal de uma organização, desenvolvido para identificar eventos potenciais que possam afetar a entidade e para gerenciar os riscos, de modo que fiquem dentro de seu apetite ao risco, para fornecer uma avaliação razoável com relação ao atingimento dos objetivos da entidade".

Serviços de avaliação devem ser objetivos e profissionais e podem ser obtidos de uma gama de prestadores de avaliação. Tais prestadores podem ser internos – tais como a auditoria interna, segurança do trabalho, *compliance* e segurança -, assim como externos, como a auditoria estatutária.

O Glossário das Normas define serviços de avaliação como um "exame objetivo da evidência, com o propósito de fornecer para a organização uma avaliação independente dos processos de governança, gerenciamento de riscos e controles".

Geralmente, há três partes envolvidas nos serviços de avaliação:

- A pessoa ou grupo diretamente envolvido com a entidade, operação, função, processo, sistema ou outros; e as funções de supervisão como gerenciamento de riscos, *compliance* e financeiro.
- A pessoa ou grupo conduzindo a avaliação (o prestador da avaliação).
- O usuário da avaliação, como o gerente executivo e o conselho.

# Estrutura de Avaliação

A necessidade de uma avaliação surge dos processos de governança de uma organização. Sua origem é a relação de administração entre o conselho de uma organização e seus acionistas. Este relacionamento exige que os conselhos estabeleçam processos para delegar e limitar o poder de buscar a estratégia e a direção da organização, de forma a melhorar suas possibilidades de sucesso a longo prazo.

O gerenciamento de riscos é um processo de gestão que promove o atingimento eficiente e eficaz dos objetivos organizacionais. Avaliação e gerenciamento de riscos são processos complementares. Em apoio ao processo de gerenciamento de riscos, o papel principal da auditoria interna e outros prestadores independentes de avaliação é de avaliar que:

- O processo de gerenciamento de riscos foi aplicado apropriadamente e que os elementos do processo são adequados e suficientes.
- O processo de gerenciamento de riscos está de acordo com as necessidades estratégicas e com as intenções da organização.
- Há processos e sistemas em prática, para garantir que todos os riscos materiais tenham sido identificados e estejam sendo tratados.

- Todos os riscos intoleráveis priorizados têm planos de tratamento rentáveis em prática.
- Os controles estão sendo desenvolvidos corretamente, de acordo com os destinos do processo de gerenciamento de riscos.
- Os controles principais são adequados e eficazes.
- Os riscos não são supercontrolados ou controlados ineficazmente.
- A revisão da gerência de linha e outras atividades de avaliação de não-auditoria são eficazes para a manutenção e melhoria dos controles.
- Os planos de tratamento de riscos estão sendo executados.
- Há progresso apropriado e conforme reportado no plano de gerenciamento de riscos.

Em apoio ao processo de avaliação, o processo de gerenciamento de riscos deve:

- Estabelecer uma política e estrutura documentada de gerenciamento de riscos.
- Atribuir responsabilidade pela identificação e gerenciamento eficazes dos riscos significantes.
- Fazer uma análise estruturada dos riscos à organização, registrando:
    - Riscos, suas exposições associadas e classificações atuais de riscos.
    - O(s) objetivo(s) organizacional(is) a que o risco se aplica.
    - O cargo organizacional responsável pela identificação e gestão de cada risco.
    - Os sistemas principais de controle estabelecidos para identificar e gerir cada risco.

A estratégia de avaliação é alinhada diretamente ao plano corporativo ou outros planos estratégicos da organização. Os ambientes jurídico, legislativo, cultural e econômico nos quais a organização opera, assim como a natureza das atividades da organização e seus planos de longo prazo, guiam as necessidades de avaliação.

Identificar quem serão os usuários da avaliação organizacional é um primeiro passo importante. Claramente, o conselho e a gerência são os usuários primários. Outros usuários podem incluir proprietários, reguladores, o governo ou consumidores para os quais a organização seja um componente crítico de fornecimento. Na economia atual, altamente interconectada, entidades externas podem precisar de avaliações da organização como parte de seu próprio processo de gerenciamento de riscos.

A avaliação necessária pode variar entre dar conforto ao conselho quando precisarem aprovar as demonstrações financeiras formais ou conteúdos do relatório anual, e a provisão de uma declaração formal de conformidade ou conforto para um órgão externo.

Os objetivos de avaliação ditarão a estratégia de avaliação e o nível de rigor aplicado, mas os requisitos básicos incluem avaliar que:

- Todos os riscos materiais tenham sido identificados.
- Os riscos tenham sido analisados e avaliados precisamente.
- Os principais controles sejam adequados e eficazes.
- A gerência está abordando apropriadamente os riscos intoleráveis.

Há três classes fundamentais de prestadores de avaliação, diferenciadas pelas partes interessadas que atendem, seu nível de independência das atividades às quais prestam avaliação e a robustez dessa avaliação. Elas são:

- Aqueles que reportam à gerência ou que fazem parte da gerência (avaliação da gerência), incluindo indivíduos que conduzem autoavaliações de controle,

auditores de qualidade, auditores ambientais e outros gerentes (designados como pessoal de avaliação).

- Aqueles que reportam ao conselho, incluindo a auditoria interna.
- Aqueles que reportam às partes interessadas externas (avaliação de demonstrações financeiras), um papel tradicionalmente desempenhado pelo auditor independente/ estatutário.

O nível de avaliação desejado varia de acordo com o risco e outros fatores, tais como regulamentos. Quem deverá prestar a avaliação varia de acordo com a habilidade do prestador da avaliação de entregar o nível necessário de independência e objetividade, assim como a estrutura organizacional histórica da entidade e conjuntos de habilidades disponíveis dentro do grupo de avaliação.

# Os Papéis Respectivos do Gerenciamento de Riscos, Auditoria Interna, Compliance e Outros Prestadores de Avaliação

Os prestadores de avaliação de uma organização podem incluir:

- A gerência de linha e funcionários (a gerência presta avaliação como a primeira linha de defesa dos riscos e controles pelos quais são responsáveis).
- A alta administração.
- Auditores internos e externos.
- *Compliance*.
- Certificação de Qualidade.
- Gerenciamento de Riscos.
- Auditores ambientais.
- Auditores de saúde e segurança do trabalho.
- Auditores de desempenho governamental.
- Equipes de revisão de reporte financeiro.
- Subcomitês do conselho (como de auditoria, atuarial, crédito, governança).
- Prestadores externos de avaliação, incluindo de pesquisas, revisões especializadas (saúde e segurança), etc.

Consulte o Guia Prático do IIA, *Reliance on Internal Audit by Other Assurance Providers* (Dezembro de 2011), para mais informações sobre a variedade de prestadores internos e externos de avaliação. Além disso, consulte a Declaração de Posicionamento do IIA, *The Role of Internal Auditing in Enterprise-wide Risk Management* (Janeiro de 2009), com relação aos papéis apropriados para a auditoria interna no gerenciamento de riscos.

A atividade de auditoria interna normalmente proverá a cobertura de avaliação sobre partes da organização aprovadas no estatuto de auditoria interna ou no termo de compromisso. Esta cobertura deve incluir os processos de gerenciamento de riscos (tanto seu desenvolvimento quanto eficácia operacional), o gerenciamento dos riscos classificados como altos (incluindo a eficácia dos controles e outras respostas a eles), verificação da confiabilidade e adequação da avaliação de riscos e o reporte do status do risco e controle.

Com a responsabilidade por atividades de avaliação tradicionalmente compartilhada entre a gerência, a auditoria interna, o gerenciamento de riscos e o setor de *compliance*, é importante que as atividades de avaliação sejam coordenadas, para garantir que os recursos sejam usados de forma eficaz e eficiente. Muitas organizações operam com atividades separadas de auditoria interna, riscos e conformidade. A conformidade é definida no Glossário das *Normas* como a "aderência aos requisitos da lei, indústria e normas e códigos

organizacionais, princípios de boa governança e normas éticas e aceitas pela comunidade". Um programa de conformidade é uma série de atividades que, quando combinadas, têm o propósito de atingir a conformidade. Sem coordenação e reporte eficazes, o trabalho pode ser duplicado ou riscos principais podem passar despercebidos ou ser mal avaliados.

O gerenciamento de riscos é fundamental para o controle organizacional e uma parte crítica do desempenho de uma boa governança corporativa. Ele envolve todas as atividades da organização. Por esse motivo, muitas organizações estão se mobilizando para adotar um processo mais formal de ERM.

# O Papel de Coordenação do DEA

A Norma do IIA 2050: Coordenação declara que o DEA deve compartilhar informações e coordenar atividades com outros prestadores internos e externos de serviços de avaliação e consultoria, para garantir a cobertura apropriada e minimizar a duplicação de esforços. Essa responsabilidade requer a inclusão e participação do DEA na estrutura de prestação de avaliação da organização. Esta estrutura pode consistir da auditoria interna, auditoria externa, governança, gerenciamento de riscos e outras funções/divulgações de controle do negócio, conduzidas pela equipe de gestão da organização. A inclusão e participação nesta estrutura ajuda a garantir que o DEA esteja ciente dos riscos e controles da organização com relação às metas e objetivos.

A maioria das funções de auditoria interna conduzem atividades de avaliação de riscos anuais e com base nos trabalhos, para ajudar a priorizar os riscos de acordo com seu impacto potencial sobre o atingimento das metas e objetivos da organização. No nível macro, essas atividades ajudam a atividade de auditoria interna a desenvolver uma proposta de plano de auditoria para apresentar ao conselho. No nível micro, essas atividades ajudam a priorizar o escopo do trabalho de auditoria e avaliação produzido pelas atividades de auditoria interna.

É importante que o trabalho desenvolvido pelos prestadores de avaliação seja compreendido e avaliado pelo DEA de forma contínua. Isso ajuda a garantir que o zelo profissional devido apropriado seja dedicado ao desempenho do trabalho de auditoria interna, incluindo as atividades de avaliação de riscos conduzidas para produzir as propostas de planos de auditoria apresentadas ao conselho. Isso também ajuda o conselho a entender a cobertura oferecida pelos prestadores de avaliação da organização, para melhor avaliar a distribuição apropriada dos recursos e exposições potenciais devidas à não-cobertura.

A coordenação entre os prestadores de avaliação inclui o compartilhamento regular de relatórios e resultados das atividades de avaliação. Esta coordenação formal deve ocorrer regularmente e deve incluir tempo para discussão e revisão de técnicas e métodos usados para chegar às conclusões. Isso inclui as respostas da gerência e um entendimento das atividades conduzidas para mitigar quaisquer riscos ou deficiências de controle identificadas.

O DEA pode desenvolver um relatório anual para compartilhar com o conselho e com a gerência executiva da organização. Este relatório deve delinear a estrutura de prestação de avaliação da organização, a cobertura da avaliação prestada, áreas de alto risco e áreas de risco residual/não-mitigado dentro da organização. Outra alternativa seria que o DEA coordenasse o desenvolvimento e a distribuição desse relatório na função de governança ou gerenciamento de riscos. Independentemente da origem do relatório, é importante que o DEA possa confiar nas técnicas e métodos usados pelos prestadores de avaliação.

Um processo contínuo, minucioso e documentado de gerenciamento de riscos faz parte da boa governança e é uma ferramenta importante de gestão, para avaliar que os controles apropriados

estejam em prática para alcançar os objetivos de uma organização.

O estabelecimento de um sistema de gerenciamento dos riscos de toda a empresa é uma responsabilidade chave da gerência. Os conselhos e a gerência são responsáveis pela adoção de uma abordagem holística à identificação dos riscos organizacionais, pela criação de controles para mitigar esses riscos, pelo monitoramento e revisão dos riscos e controles identificados e pela garantia de que o gerenciamento de riscos esteja integrado à organização – nos níveis estratégico e operacional. Algumas organizações delegam funções independentes de gerenciamento de riscos, mas outras não têm uma função independente de gerenciamento de riscos e precisam da auditoria interna para prestar serviços de consultoria nessa área. A auditoria interna pode auxiliar na identificação, avaliação e facilitação das metodologias de gerenciamento de riscos. A auditoria interna também é responsável por avaliar a eficácia e contribuir para a melhoria do processo de gerenciamento de riscos.

A identificação de riscos de forma sistemática atua em favor da tomada de decisões. Ela gira em torno da realização de uma análise minuciosa da organização em diversos níveis, descrevendo eventos que podem ocorrer, decidindo a importância desses riscos e desenvolvendo as medidas adequadas para lidar com eles.

# Usando o Processo de Gerenciamento de Riscos no Planejamento de Auditoria Interna

A documentação do gerenciamento de riscos em uma organização pode ser feita muitos níveis abaixo do processo estratégico de gerenciamento de riscos. Muitas organizações desenvolveram registros de riscos que documentam os riscos abaixo do nível estratégico, fornecendo documentação dos riscos significantes para uma área e as classificações de riscos inerentes e residuais relacionadas, principais controles e fatores mitigantes. Um exercício de alinhamento pode, então, ser realizado para identificar ligações entre os itens incluídos no universo de auditoria, documentado pela atividade de auditoria interna, e as categorias de riscos e aspectos descritos nos registros de riscos.

Algumas organizações podem identificar diversas áreas de (exposição potencial a) riscos inerentes altos (ou mais altos). Embora esses riscos possam certamente atrair a atenção da auditoria interna, não é sempre possível revisar todos eles. Nos casos em que o registro de riscos mostrar uma classificação alta, ou mais alta, para um risco inerente (ou para uma exposição potencial de grande importância) em uma área específica, e se o risco atual permanecer igualmente alto sem atitudes da gerência ou da auditoria interna planejada, o DEA deve reportar essas áreas ao conselho, com detalhes sobre a análise de riscos e motivos para a falta, ou ineficácia, dos controles internos.

Além de avaliar a eficácia do processo de gerenciamento de riscos da organização e de contribuir para sua melhoria, a auditoria interna também usa os resultados do processo de gerenciamento de riscos para desenvolver planos de auditoria anuais e trabalhos individuais de auditoria.

Frequentemente, pede-se à auditoria interna que entregue resultados melhores com recursos já "esticados". Isso pode ser feito por meio da colocação estratégica do trabalho de auditoria interna onde ele possa ser mais eficaz na entrega dos melhores resultados e onde terá o melhor efeito sobre os resultados das metas operacionais e estratégicas da entidade de negócios. Uma das ferramentas para alcançar isso é basear os planos de auditoria interna e trabalhos individuais de auditoria nos principais riscos identificados e controles.

A auditoria interna deve preparar planos de auditoria de curto e longo prazo, para garantir que suas atividades estejam cobrindo as principais áreas de risco e os controles internos da organização. Conforme as circunstâncias de negócio mudarem substancialmente, o monitoramento contínuo e a revisão periódica dos planos anuais – com, pelo menos, revisões anuais dos planos de longo prazo – são necessários para garantir que os planos de auditoria sejam flexíveis, com base em informações atualizadas e que cubram as novas prioridades e áreas de risco.

**A Norma 2010: Planejamento** declara que "o DEA deve estabelecer um plano baseado em riscos para determinar as prioridades da atividade de auditoria interna, de forma consistente com as metas da organização". Além disso, a Norma 2010.A1 declara que "o planejamento dos trabalhos da atividade de auditoria interna deve ser baseado em uma avaliação de riscos documentada, realizada pelo menos anualmente. As informações fornecidas pela alta administração e pelo conselho devem ser consideradas nesse processo".

**A Norma 2120: Gerenciamento de Riscos** declara que "a atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos".

Os itens a seguir são passos a considerar na preparação dos planos de auditoria interna, para determinar os riscos e exposições que possam afetar o atingimento das metas e objetivos da organização:

- Pesquisa e revisão dos documentos corporativos, tais como planos de negócios da organização, planos estratégicos, avaliações de riscos corporativos, relatórios anuais, minutas das reuniões do conselho, minutas das reuniões da gerência, relatórios externos, relatórios de auditoria externa e outras fontes apropriadas.
- Revisão de planos anteriores de auditoria interna, dos relatórios de progresso e dos trabalhos em andamento.
- Consultar a alta administração da organização e solicitar informações com relação às preocupações ou áreas de risco.
- Conduzir uma avaliação de riscos dos problemas e determinar as prioridades para o plano anual de auditoria.
- Preparar um rascunho do plano de auditoria.
- Comunicar a proposta do plano de auditoria para as partes interessadas.
- Enviar feedback e validação das principais áreas de risco a revisar.
- Finalizar os planos de auditoria.
- Apresentar à gerência e ao conselho para aprovação.
- Monitorar, revisar e reavaliar regularmente os planos, em relação às novas circunstâncias.

Embora o raciocínio mais amplo e o objetivo de uma auditoria interna sejam desenvolvidos na fase de planejamento anual, é necessário realizar uma pesquisa e trabalho detalhados no início da auditoria, para definir o objetivo e escopo detalhados e desenvolver critérios e metodologia.

A **Norma 2201: Considerações sobre o Planejamento** declara que, "no planejamento dos trabalhos de auditoria, os auditores internos devem considerar:

- Os riscos significantes para a atividade, seus objetivos, recursos e operações e os meios pelos quais o impacto potencial dos riscos é mantido em um nível aceitável.
- A adequação e a eficácia dos sistemas de gerenciamento de riscos e controle da atividade, em comparação com uma estrutura ou modelo de controle compatível.
- As oportunidades para melhorias significantes nos processos de gerenciamento de riscos e controle da atividade.

Além disso, a **Norma 2210: Objetivos do Trabalho de Auditoria** 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 desta avaliação". Com relação aos trabalhos de consultoria, a Norma 2120.C1 declara que, "durante os trabalhos de consultoria, os auditores internos devem abordar os riscos de forma consistente com os objetivos do trabalho e estar alertas à existência de outros riscos significantes".

O planejamento minucioso de uma auditoria interna é crucial para seu sucesso. Ele traz uma oportunidade de se familiarizar com a entidade sendo auditada; de coletar questões, preocupações e riscos relevantes; de completar uma avaliação de riscos; e determinar os objetivos e escopo da auditoria.

No desenvolvimento de um plano de trabalho de auditoria, a equipe de auditoria interna conduz uma avaliação de riscos formal, abrangente e documentada, para identificar os problemas de auditoria e eventos de risco. Isso envolve uma pesquisa significante, consultas junto à gerência da entidade ou da área sob revisão e a familiarização com a entidade ou área.

Os métodos de avaliação de riscos podem variar; no entanto, todas as avaliações de riscos devem cobrir os seguintes pontos:

- Descrição do evento de risco (ocorrência negativa, evento indesejável).

- Probabilidade de ocorrência do evento (forte, moderada, fraca).
- O impacto da ocorrência negativa sobre o atingimento das metas e objetivos (alto, moderado, baixo).
- Os controles atuais (sistemas, políticas, procedimentos, etc) em prática e sua eficácia (eficaz/ineficaz).
- Classificação dos eventos de risco.

Toda auditoria potencial enfatiza uma grande variedade de problemas a examinar. No entanto, não é necessário, razoável ou rentável examinar todos eles. A equipe de auditoria precisa estar ciente disso e concentrar seus esforços nos problemas mais importantes e de maior risco.

Ao classificar possíveis eventos de risco, este processo identificará os problemas de maior importância e classificação. Neste ponto, pode ser tomada uma decisão com relação aos problemas que são materiais e aos que serão auditados, considerando o objetivo da auditoria e levando em conta outros fatores, tais como auditabilidade, recursos e *timelines*. Os resultados da avaliação de riscos devem ser apresentados e discutidos com a gerência da entidade sob revisão, para garantir sua concordância e validação.

# Preparação de Mapas de Avaliação

Os conselhos usarão diversas fontes para obter uma avaliação confiável, incluindo a gerência, a auditoria interna e terceiros. Muitas organizações operam com funções separadas de auditoria interna, riscos e conformidade. Não é incomum que as organizações tenham um certo número de grupos separados, conduzindo funções diferentes de gerenciamento de riscos, conformidade e avaliação, e independemente umas das outras. Conforme discutido na Prática Recomendada 2050-2, um mapa de avaliação é uma ferramenta valiosa para coordenar essas atividades de gerenciamento e avaliação de riscos, de modo a aumentar a eficiência e eficácia dos investimentos feitos por uma organização em avaliações. Mapas de avaliação podem ajudar a:

- Identificar duplicação e sobreposição na cobertura da avaliação, permitindo que o conselho e a alta administração decidam se a sobreposição é necessária, intencional ou se deve ser eliminada.
- Definir limites de escopo, papéis e responsabilidades dos diversos prestadores de avaliação, para garantir que os recursos certos sejam concentrados nos riscos certos. Isso pode aprimorar a eficácia dos prestadores de avaliação, garantindo que eles se concentrem nas áreas que demandam sua atenção, articulando claramente as expectativas do conselho e da alta administração.
- Auxiliar na identificação de quaisquer lacunas, na cobertura da avaliação, que precisem ser abordadas.

São responsabilidades do DEA entender os requisitos de avaliação do conselho e da organização, esclarecer o papel que a atividade de auditoria interna desempenha e o nível de avaliação que ela fornece. No entanto, considerando seu ponto de vantagem único para atividades de avaliação na organização, o DEA pode ir além e ajudar na criação do mapa de avaliação para a organização. Isso não ajudará o conselho apenas a supervisionar a governança, mas também auxiliará o DEA a garantir que a atividade de auditoria esteja otimizando seus recursos para o máximo valor de avaliação, além de criar uma comunidade de avaliação mais conectada, por meio da coordenação eficaz.

# Feedback sobre Áreas de Risco Significantes em Relatórios de Auditoria Interna

Durante todos os trabalhos de avaliação, principalmente nos casos em que o escopo se relacione às exposições potenciais identificadas no processo de gerenciamento de riscos de uma organização, a abordagem, procedimentos e comunicações de auditoria devem ser desenvolvidas para avaliar as afirmações da gerência sobre a eficácia dos controles em trazer o risco para dentro da faixa de tolerância de riscos da organização.

Os relatórios para a gerência e o conselho podem descrever a exposição potencial e a avaliação dos riscos atuais da gerência (com o valor implícito dos controles em prática), em conjunto com a avaliação de auditoria das classificações dos riscos. Quaisquer diferenças devem ser incluídas no processo de gerenciamento de riscos da gerência, para consideração.

O efeito cumulativo, ao longo do tempo, de tais atividades de avaliação sobre as áreas de risco, usando um plano de auditoria com base em riscos, prestará uma avaliação não apenas dessas áreas, mas também da eficácia do processo geral de gerenciamento de riscos.

# Avaliação da Adequação do Gerenciamento de Riscos por Parte da Auditoria Interna

A auditoria interna deve prestar avaliação conforme exigido pela Norma 2100: Natureza do Trabalho, 2120: Gerenciamento de Riscos e 2400: Comunicação dos Resultados à alta administração e, finalmente, ao conselho, de que a organização está gerenciando seus riscos com eficácia. Conforme a auditoria interna precisar incluir a adequação do gerenciamento de riscos dentro desse escopo, há duas dimensões a considerar:

1. Se a função de gerenciamento de riscos inclui todas as áreas de risco apropriadas em seu escopo.
2. Se a função de gerenciamento de riscos está operando com eficácia.

Os principais elementos da avaliação que a auditoria interna precisará englobar são cobertos, em grande extensão, pela Prática Recomendada 2120-1: Avaliando a Adequação dos Processos de Gerenciamento de Riscos. As principais características são:

- Conselhos de gestão, como parte de seu papel de supervisão, podem orientar a auditoria interna a ajudar na revisão e reporte da adequação do gerenciamento de riscos.
- A gerência e o conselho são responsáveis pelo gerenciamento de riscos; no entanto, os auditores internos que atuam em um papel de consultoria podem auxiliar a gerência com essa responsabilidade.
- Nos casos em que a organização não tiver um processo formal de gerenciamento de riscos, o DEA deve discutir a situação formalmente com a gerência e o conselho.

O DEA deve estabelecer que:

- Haja uma cultura de gerenciamento de riscos eficaz.
- Haja um entendimento claro, em todos os níveis, das exposições potenciais ou riscos inerentes que a organização enfrenta (ex: um registro de riscos).
- Haja um entendimento claro do nível de risco atual dentro da organização.

- A quantidade de riscos aceitos em todos os níveis da organização seja claramente definida e entendida.
- Haja controles adequados e eficazes em prática, para mitigar os riscos.
- Haja um método apropriado de comunicação à alta administração e ao conselho do status da eficácia do sistema de gerenciamento de riscos.

O DEA tem três funções importantes na revisão do gerenciamento de riscos e em qualquer outro trabalho de auditoria:

- Testar os controles.
- Reportar quaisquer controles faltosos ou ineficazes.
- Recomendar melhorias.

# A Promoção do Gerenciamento de Riscos por Parte da Auditoria Interna

A Norma 2100 declara que "a atividade de auditoria interna deve avaliar e contribuir para a melhoria dos processos de governança, gerenciamento de riscos e controles, utilizando uma abordagem sistemática e disciplinada". A atividade de auditoria interna tem, frequentemente, um papel de fornecer avaliações independentes e objetivas para o conselho da organização, com relação à eficácia das atividades de ERM da organização. Isso ajuda a garantir que os principais riscos de negócio estejam sendo gerenciados apropriadamente e que o sistema de controles internos da organização esteja operando com eficácia e eficiência.

O gerenciamento de riscos é um processo de gestão que promove o atingimento rentável dos objetivos organizacionais. Por meio da revisão independente do processo de gerenciamento de riscos de uma organização, a auditoria interna pode promover o gerenciamento de riscos por toda a empresa e o processo de auditoria pode ser alinhado às estruturas de gerenciamento de riscos. O uso de uma linguagem consistente de riscos por toda a organização pode ser adotado pela auditoria interna.

A revisão, por parte da auditoria interna, da identificação de riscos, avaliação de riscos, identificação e avaliação de controle e tratamentos apropriados de riscos desafia e aprimora os registros de riscos e a estrutura de gerenciamento de riscos.

# Como a Auditoria Interna Facilita o Gerenciamento de Riscos

Algumas organizações não têm uma função formal de gerenciamento de riscos e, nesse caso, a atividade de auditoria interna pode prestar serviços de consultoria em gerenciamento de riscos para a organização. A auditoria interna pode prestar consultoria em gerenciamento de riscos, desde que certas condições sejam aplicáveis:

- Deve estar claro que a gerência continua responsável pelo gerenciamento de riscos, mesmo nas organizações em que a auditoria interna tenha sido chamada para facilitar o programa de gerenciamento de riscos. A auditoria interna não deve gerenciar quaisquer riscos em nome da gerência, tampouco tomar decisões finais com relação ao apetite de riscos da organização ou ao nível de alocação de recursos para controlar ou mitigar riscos. Em qualquer situação em que a auditoria interna atuar em apoio à equipe de gestão, para implementar ou melhorar processos de gerenciamento de riscos, o comitê de auditoria deve aprovar seu plano de trabalho.

- A natureza das responsabilidades da auditoria interna deve ser documentada no estatuto de auditoria interna e aprovada pelo conselho. Qualquer trabalho além das atividades de avaliação deve ser reconhecido como um trabalho de consultoria e as normas de implementação relacionadas a tais trabalhos devem ser seguidas.
- A auditoria interna deve aconselhar, desafiar e atuar em apoio à tomada de decisões da gerência, em vez de tomar decisões de gerenciamento de riscos. A auditoria interna não pode fazer uma avaliação objetiva de qualquer parte da estrutura de gerenciamento de riscos pela qual ela seja responsável. Outras partes adequadamente qualificadas devem prestar tal avaliação.

A Declaração de Posicionamento do IIA, *The Role of Internal Auditing in Enterprise-wide Risk Management* (Janeiro de 2009), descreve os papéis apropriados para a auditoria interna com relação ao gerenciamento de riscos.

# Impacto sobre a Auditoria Interna quando não há uma Função Formal de Gerenciamento de Riscos

Quando uma organização não tem uma função de gerenciamento de riscos, ela normalmente requer um esforço maior por parte do DEA para comunicar as atividades de gerenciamento de riscos e avaliação ao conselho. Uma maior importância é dada à qualidade da avaliação de riscos da auditoria interna, como o único ponto de vista a que o conselho poderá ser exposto.

O DEA deve promover a função de gerenciamento de riscos como uma atividade importante, que auxilia a organização no atingimento de seus objetivos e traz recomendações para o estabelecimento desse processo. Caso seja solicitado, o DEA pode desempenhar um papel proativo de consultoria, no auxílio do estabelecimento inicial de um processo de gerenciamento de riscos para a organização. No entanto, embora a função de auditoria interna possa facilitar ou permitir a criação de processos de gerenciamento de riscos, ela não deve ser responsável por processos ou pelo gerenciamento de riscos identificados. Inicialmente, a função de auditoria interna pode facilitar os processos de avaliação de riscos da gerência; no entanto, é recomendável que essas atividades de facilitação sejam separadas das atividades de avaliação na organização do DEA.

Se o papel da auditoria interna exceder as atividades normais de avaliação e consultoria, de modo que sua independência seja prejudicada, o DEA deve seguir os requisitos de divulgação das *Normas*.

# Autores:

Andrew MacLeod, CIA, CMIIA

Brian Foster, CIA

Patricia Macdonald

Andy Robertson

Teis Stokka, CIA

Benito Ybarra, CIA

# Revisores:

Doug Anderson, CIA, CRMA

Andy Dahle, CIA

Steve Jameson, CISA, CCSA, CFSA, CRMA

David Zechnich, CIA, CPA

## Sobre o Instituto

Fundado em 1941, *The Institute of Internal Auditors* (IIA) é uma associação profissional com sede global em Altamonte Springs, Fla., EUA. O IIA é a voz da profissão de auditoria interna em todo o mundo, autoridade reconhecida, líder valorizado, advogado chefe e principal educador.

## Sobre os Guias Práticos

Os Guias Práticos fornecem uma orientação detalhada para a condução de atividades de auditoria interna. Eles incluem processos e procedimentos detalhados, como ferramentas e técnicas, programas e abordagens passo-a-passo, assim como exemplos de *deliverables*. Os Guias Práticos são parte da Estrutura Internacional de Práticas Profissionais do IIA. Como parte da categoria de orientação Fortemente Recomendada, a conformidade não é obrigatória, mas é altamente recomendada, e a orientação é endossada pelo IIA por meio de processos formais de revisão e aprovação. Para mais materiais de orientação fidedignos fornecidos pelo IIA, por favor, visite nosso website: www.iiabrasil.org.br ou www.theiia.org

## Isenção de Responsabilidade

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

## Copyright