IPPF - GUIAS PRÁTICOS

AVALIANDO A ADEQUAÇÃO DO GERENCIAMENTO DE RISCOS USANDO A ISO 31000

Instituto dos Auditores Internos do Brasil

Índice

Sumário Executivo

Muitas organizações estão engajadas na adoção de abordagens consistentes e holísticas para o gerenciamento de riscos e reconhecem que o gerenciamento de riscos é um processo de gestão que deve ser totalmente integrado à gestão da organização. Isso se aplica em todos os níveis da organização – nível da entidade, nível da função e nível da unidade de negócio.

A estrutura de gerenciamento de riscos deve ser desenvolvida sob medida para a organização: para seu ambiente interno e externo. Para que o gerenciamento de riscos seja eficaz, a estrutura em qualquer organização, independentemente de tamanho ou propósito, deve ter certos elementos essenciais. Este guia detalha três abordagens para a avaliação do processo de gerenciamento de riscos: uma abordagem de Elementos do Processo; uma abordagem baseada nos Princípios do Gerenciamento de Riscos; e uma abordagem de Modelo de Maturidade. O processo de avaliação usado deve ser personalizado, para atender as necessidades específicas da organização.

Os auditores internos devem ter meios para medir a eficácia do gerenciamento de riscos em sua organização. Isso pode ser obtido através do exame dos critérios que refletem aspectos do processo de gerenciamento de riscos. Os critérios usados devem ser relevantes, confiáveis, compreensíveis e completos. O conjunto das observações deve permitir que o auditor forme uma opinião acerca do nível de maturidade de gerenciamento de riscos da organização.

A qualidade do processo de gerenciamento de riscos da organização deve melhorar com o tempo. Implementar um gerenciamento de riscos eficaz – o verdadeiro ERM – demora, frequentemente, muitos anos. Um dos critérios chave que os auditores internos devem considerar é se há uma estrutura adequada implementada para promover uma abordagem corporativa e sistemática para o gerenciamento de riscos.

Este guia prático usa a ISO 31000 como base para a estrutura de gerenciamento de riscos. Outras estruturas podem ser usadas para conduzir a avaliação de riscos. Esta orientação não implica ou explicita apoio a esta ou qualquer outra estrutura.

Introdução

Durante os últimos anos, a importância de gerir riscos como parte de uma governança corporativa forte tem sido crescentemente reconhecida. As organizações estão sofrendo pressões para identificar os riscos significativos de negócios que elas encaram – sociais, éticos e ambientais, assim como estratégicos, financeiros e operacionais – e para explicar como eles são gerenciados por elas. O uso de estruturas de gerenciamento de riscos dentro da organização se expandiu conforme as empresas passaram a reconhecer as vantagens de abordagens coordenadas para o gerenciamento de riscos.

O gerenciamento de riscos é definido no Glossário das Normas Internacionais para Prática Profissional de Auditoria Interna (Normas) como “um processo para identificar, avaliar, gerenciar e controlar eventos ou situações em potencial para fornecer uma avaliação razoável do alcance dos objetivos da organização”.[1] Uma estrutura abrangente de gerenciamento de riscos fornece uma ligação de ponta a ponta entre os objetivos, estratégia, execução da estratégia, riscos, controles e avaliação em todos os níveis da organização.

O gerenciamento de riscos corporativos (*Enterprise Risk Management* – ERM) – ou melhor, o gerenciamento de riscos dentro da organização – é um termo de uso comum. O Comitê das Organizações Patrocinadoras da Comissão Treadway

[1] Isso é consistente com a definição da *International Organization for Standardization* (ISO) de gerenciamento de riscos: “atividades coordenadas para dirigir e controlar uma organização com relação ao risco”. (Guia ISO 73:2009, Definição 2.1)

(COSO) define como "um processo, efetuado pelo conselho de administração, administração ou outro pessoal de uma entidade, aplicado na determinação de estratégias e em toda a organização, desenvolvido para identificar eventos potenciais que possam afetar a entidade e gerenciar riscos para que se limitem a seu apetite, para fornecer uma avaliação razoável do alcance dos objetivos da entidade".

A ISO 31000 (Seção 4.1) declara que o sucesso do gerenciamento de riscos "irá depender da eficácia da estrutura de gestão que fornece os fundamentos e arranjos que irão incorporá-la através de toda a organização, em todos os níveis".[2] Uma estrutura de gerenciamento de riscos se refere aos componentes e à organização do gerenciamento de riscos dentro de uma entidade.

A Norma 2120 declara que "a atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos". Ela prossegue, com a seguinte interpretação:

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

- *Os objetivos da organização dão suporte e estão alinhados com a missão da organização;*
- *Os riscos significativos são identificados e avaliados;*
- *Respostas apropriadas aos riscos são selecionadas de forma a alinhar os riscos com o apetite de risco da organização; e*
- *Informações de riscos relevantes são capturadas e comunicadas de forma oportuna por toda a organização, permitindo que colaboradores, administração e conselho cumpram com suas responsabilidades.*

A atividade de auditoria interna pode coletar informações para dar suporte a essa avaliação durante múltiplos trabalhos. Os resultados desses trabalhos, quando examinados em conjunto, apresentam um entendimento dos processos de gerenciamento de riscos da organização e de sua eficácia.

Os processos de gerenciamento de riscos são monitorados através de atividades contínuas de gerenciamento, avaliações separadas ou ambos."

O ponto inicial para melhorar a abordagem de uma organização em relação ao gerenciamento de riscos deveria ser uma análise dos gaps que faça um balanço da situação e avalie quais processos e sistemas estão presentes no momento. Se qualquer parte essencial estiver faltando, é altamente improvável que o gerenciamento de riscos seja eficaz. Os auditores internos têm um papel importante a desempenhar na avaliação e melhoria do gerenciamento de riscos em suas organizações e avaliar as atividades de gerenciamento de riscos da organização é um componente crítico desse esforço.

Esse guia prático usa a estrutura e parte da terminologia da ISO 31000. Embora a ISO 31000 não tenha sido desenvolvida como base para certificação, seus conceitos e estruturas formam uma base para avaliar qualquer processo de gerenciamento de riscos. A estrutura ISO 31000 não é a única estrutura de gerenciamento de riscos de uso comum e essa orientação não significa qualquer apoio a essa estrutura em particular.

[2] © ISO. Esse material é reproduzido da ISO 31000:2009 ou do Guia ISO 73:2009, com permissão do *American National Standards Institute* (ANSI) em nome da *International Organization for Standardization* (ISO). Nenhuma parte deste material da ISO pode ser copiado ou reproduzido de qualquer forma, por sistema de restauração eletrônica ou disponibilizado de qualquer outra forma na Internet, em rede pública, por satélite ou outro meio sem a permissão prévia por escrito do ANSI. Cópias desta norma podem ser adquiridas no ANSI, 25 West 43rd 10036, (212) 642-4900, http://webstore.ansi.org.

Gerenciamento de Riscos na Organização

Governança

A Norma de Gestão de Riscos ISO 31000 fornece orientações para a estrutura de gerenciamento de riscos aplicável a organizações de qualquer tamanho. A ISO 31000 define uma estrutura de gerenciamento de riscos como um "conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização".[3] A estrutura de gerenciamento de riscos, independentemente do nível de formalidade, está inerentemente incorporada na estratégia geral da organização e em sua política e práticas operacionais. Arranjos organizacionais incluem planos, relacionamentos, prestações de contas, recursos, processos e atividades. O diagrama desta página (Figura 1) mostra um modelo conceitual que pode ser usado para análise desses arranjos.

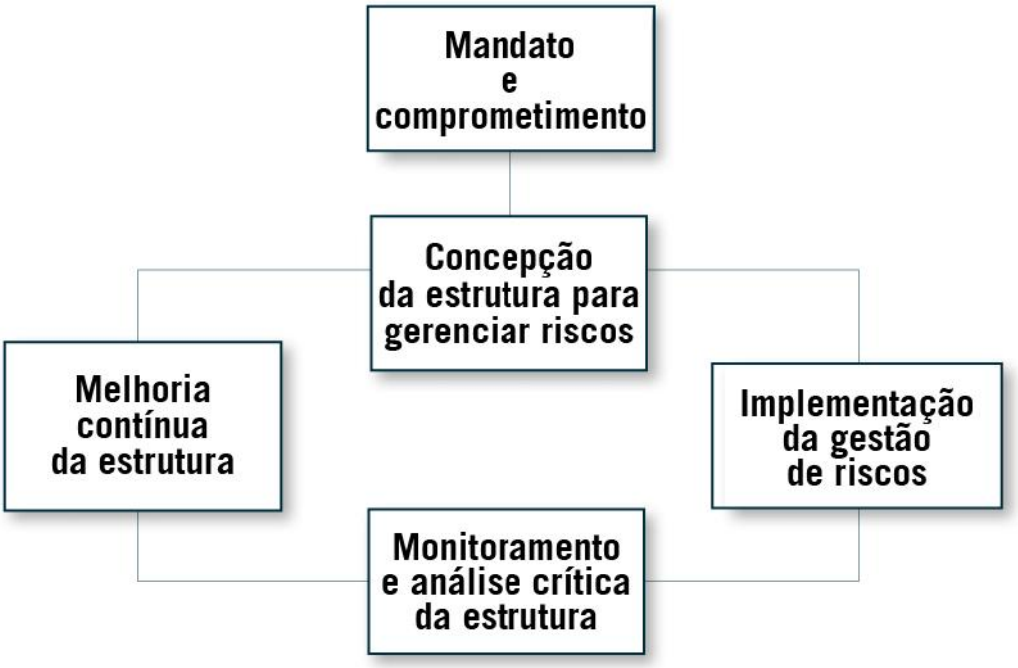

Figura 1 – Estrutura para Gerenciamento de Riscos (ISO 31000)

Responsabilidades pelo Gerenciamento de Riscos

A *International Organization for Standardization* (ISO) define atitude perante o risco como uma "abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do risco".[4] A administração é responsável por determinar a atitude da organização perante o risco e o conselho é responsável por determinar se a atitude perante o risco está alinhada com os interesses dos acionistas.

[3] © ISO. Esse material é reproduzido da ISO 31000:2009 ou do Guia ISO 73:2009, com permissão do *American National Standards Institute* (ANSI) em nome da *International Organization for Standardization* (ISO). Nenhuma parte deste material da ISO pode ser copiado ou reproduzido de qualquer forma, por sistema de restauração eletrônica ou disponibilizado de qualquer outra forma na Internet, em rede pública, por satélite ou outro meio sem a permissão prévia por escrito do ANSI. Cópias desta norma podem ser adquiridas no ANSI, 25 West 43rd 10036, (212) 642-4900, http://webstore.ansi.org.[4] Ibid.

O conselho realiza a supervisão da governança do ERM e deve entender os elementos chave de ERM, perguntar à gerência acerca dos riscos e concordar com certas decisões da gestão. As partes interessadas devem receber informações suficientes para entender a atitude da administração e do conselho perante o risco, de forma a investir de acordo com suas tolerâncias pela variação potencial do desempenho. As organizações comunicam os níveis de riscos em relatórios bimestrais e anuais, comunicados à imprensa, conferências com investidores, etc.

O conselho tem a responsabilidade geral de garantir que os riscos sejam gerenciados e que haja um sistema eficaz de gerenciamento de riscos aplicado. Na prática, o conselho delegará a operação da estrutura de gerenciamento de riscos para a equipe de gerenciamento. É possível que haja uma função separada com habilidades e conhecimento especializados que coordene e gerencie essas atividades, mas todos na organização têm um papel a desempenhar na garantia do gerenciamento eficaz dos riscos corporativos e a responsabilidade primária por identificar e gerenciar os riscos é da administração.

Monitoramento e Avaliação

A aplicação do ERM muda com o tempo. A atitude perante o risco pode mudar por conta de fatores internos ou externos, respostas ao risco que eram eficazes antes podem se tornar irrelevantes e atividades de controle podem ser tornar menos eficazes ou não mais realizadas. As mudanças podem ocorrer por conta da chegada de novos funcionários, modificações na estrutura da entidade ou pela apresentação de novos processos. Além disso, os objetivos da entidade, assim como a natureza de eventos ou condições em potencial que podem afetar o alcance desses objetivos, mudarão. Da mesma forma, a administração precisa determinar se os componentes de ERM continuam relevantes e capazes de lidar com novos riscos.

Um elemento crítico de um sistema sensato de gerenciamento de riscos é o monitoramento, para garantir que o desempenho seja o desejado. O monitoramento pode ser feito de duas formas: por meio de atividades contínuas ou avaliações separadas. Essa combinação de monitoramento contínuo com avaliações separadas garantirá que o ERM mantenha sua eficácia com o passar do tempo.

Os processos de ERM incorporam avaliações periódicas de riscos e classificações de riscos. Quanto maior o grau e a eficácia do monitoramento contínuo, menor a necessidade que pode existir de realizar avaliações separadas. A frequência das avaliações separadas necessárias para que a administração tenha uma avaliação razoável acerca da eficácia do ERM é uma questão de julgamento da própria administração. Ao fazer essa determinação, são considerados a natureza e o grau das mudanças, a competência e a experiência das pessoas que estão implementando as respostas ao risco e controles relacionados, a natureza e importância para o negócio dos riscos sendo gerenciados e os resultados do monitoramento contínuo.

O monitoramento contínuo é incorporado às atividades operacionais normais e recorrentes de uma empresa. Ele pode ser mais eficaz do que avaliações separadas, porque é conduzido em tempo real, reagindo dinamicamente a condições em constante mudança e está enraizado na organização. Os problemas serão frequentemente identificados mais rapidamente pelos processos de monitoramento contínuo, já que avaliações separadas ocorrem após a ocorrência do fato. Algumas entidades com atividades sensatas de monitoramento contínuo irão, contudo, conduzir uma avaliação separada de ERM ou de porções do mesmo. O nível percebido de objetividade é maior para avaliações separadas do que para automonitoramento.

Uma entidade que percebe uma necessidade de avaliações separadas frequentes deve focar em formas de melhorar suas atividades de monitoramento contínuo e, dessa forma, enfatizar atividades de monitoramento “incorporadas”, em vez de “acrescentadas”.

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 suas partes interessadas. Essa relação posiciona o conselho para estabelecer processos para delegar e limitar o poder de perseguir a estratégia e a direção da organização, de forma a melhorar as perspectivas para o sucesso a longo prazo da organização. Os processos de avaliação permitem que o conselho monitore o exercício desse poder.

A atividade de auditoria interna irá, normalmente, fornecer uma avaliação de todo o processo de gerenciamento de riscos, incluindo as atividades de gerenciamento de riscos (a eficácia de seu desenvolvimento e operação), o gerenciamento dos riscos classificados como "chave" (incluindo a eficácia dos controles e outras respostas a eles), a verificação do rigor e confiabilidade das avaliações de riscos e o reporte dos riscos e status de controle.

Com a responsabilidade pelo monitoramento e as atividades de avaliação tradicionalmente compartilhadas entre várias partes, incluindo a gestão de linha, auditoria interna, especialistas em gerenciamento de riscos e a função de conformidade, é importante que as atividades de avaliação sejam coordenadas para garantir que os recursos sejam usados da forma mais eficiente e eficaz. É comum que organizações tenham um certo número de grupos separados conduzindo funções de aconselhamento para gerenciamento de riscos, conformidade e avaliação diferentes independentemente umas das outras. Sem a coordenação e reporte eficazes, o trabalho pode ser duplicado ou os riscos chave podem passar despercebidos ou podem ser julgados mal.

O diretor executivo de auditoria (DEA) é orientado pela Norma 2050 a coordenar sua atividade com outros prestadores de avaliação. O uso de um mapa de avaliação pode ajudar a atingir essa meta, oferecendo uma ferramenta eficaz para gerenciar e comunicar essa coordenação. A Prática Recomendada 2050-2 dá mais informações acerca dos Mapas de Avaliação.

A Auditoria Interna e o Gerenciamento de Riscos

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 frequentemente tem o papel de fornecer avaliações independentes e objetivas para o conselho da organização acerca da eficácia das atividades de ERM da organização. Isso ajuda a garantir que os riscos chave do negócio estão sendo gerenciados apropriadamente e que o sistema de controles internos da organização esteja funcionando com eficácia e eficiência.

O gerenciamento de riscos é um processo de gerenciamento que promove a conquista rentável dos objetivos organizacionais, a avaliação fornece informações confiáveis sobre as conquistas da atividade de gerenciamento de riscos. O processo de avaliação e de gerenciamento de riscos são processos complementares.

Em apoio ao processo de gerenciamento de riscos, a auditoria interna e outros prestadores independentes de avaliação avaliariam se:

- O processo de gerenciamento de riscos foi aplicado apropriadamente e se todos os elementos do processo são adequados e suficientes.
- O processo de gerenciamento de riscos está de acordo com as necessidades estratégicas e de acordo com o objetivo da organização.
- Todos os riscos significativos foram identificados e estão sendo tratados.
- Os controles estão sendo desenvolvidos corretamente, de acordo com os objetivos do processo de gerenciamento de riscos.

- Os controles críticos são adequados e eficazes.
- A revisão pela gerência de linha e outras atividades de avaliação que não sejam de auditoria são eficazes na manutenção e melhoria dos controles.
- Os planos de tratamento de riscos estão sendo executados.
- Há um progresso apropriado e compatível com o reportado no plano de gerenciamento de riscos.

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

- Estabelecer uma estrutura de gerenciamento de riscos documentada e específica para a organização.
- Fornecer uma análise estruturada dos riscos da organização, registrando:
    - Objetivo(s) da organização e seus riscos associados.
    - Exposições e avaliações potenciais de riscos atuais.
    - A posição organizacional responsável por gerenciar cada risco.
    - Os sistemas chave de controle estabelecidos para gerenciar cada risco.

Não é incomum para a atividade de auditoria interna de uma organização trabalhar em cooperação com a função de gerenciamento de riscos. Algumas organizações não têm uma função formal de gerenciamento de riscos e, nesses casos, a auditoria interna frequentemente fornece à organização serviços mais extensos de consultoria em gerenciamento de riscos. A auditoria interna pode prestar consultoria em gerenciamento de riscos, considerando certas condições:

- Deve ficar claro que a administração continua responsável pelo gerenciamento de riscos. Quando a auditoria interna prestar consultoria à equipe de gerenciamento para estabelecer ou melhorar processos de gerenciamento de riscos, seu plano de trabalho deve incluir uma estratégia clara e um cronograma para migrar a responsabilidade por essas atividades para os membros da administração.
- A auditoria interna não pode dar avaliações objetivas acerca de nenhuma parte da estrutura de gerenciamento de riscos pela qual ela é responsável. Tal avaliação deve ser fornecida por outras partes qualificadas adequadas.
- A natureza de tais serviços prestados à organização deve ser documentada no estatuto de auditoria interna e deve ser consistente com outras responsabilidades de auditoria interna.
- Qualquer orientação de consultoria ou desafios (ou apoio) à tomada de decisões da gerência não coloca a auditoria interna em uma posição de tomar decisões de gerenciamento de riscos por si própria.

A Declaração de Posicionamento “O Papel da Auditoria Interna no Gerenciamento dos Riscos Corporativos” inclui o seguinte diagrama que ilustra uma variedade de atividades de ERM e indica quais papéis uma função profissional de auditoria interna eficaz deve e não deve desempenhar.

Revisão do Gerenciamento de Riscos por Parte da Auditoria Interna

Para as áreas de maior risco, nas quais a gerência reconheceu a necessidade de melhorar os controles, pode haver uma oportunidade para a auditoria interna agregar valor à organização através das atividades de

consultoria. O segmento de atividades de auditoria no meio da Figura 2 a seguir representa atividades de aconselhamento e consultoria, realizadas no nível da entidade ou da unidade de negócio/departamento, de uma maneira que deve manter a independência e a objetividade da auditoria interna.

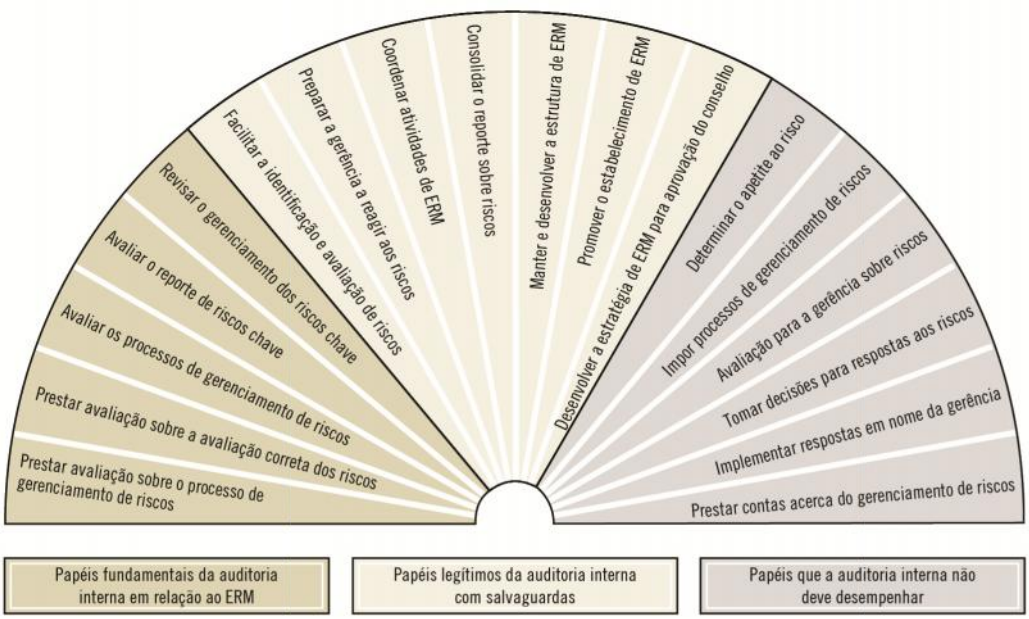

Figura 2 – O Papel da Auditoria Interna no ERM

Embora tais atividades de aconselhamento e de consultoria possam ser uma parte valiosa de um plano de auditoria, o escopo deste Guia Prático tem como foco as atividades de avaliação descritas ao lado esquerdo do leque. Tais atividades podem ser categorizadas em três tipos principais:

- Avaliação do processo de gerenciamento de riscos em si.
- Avaliação dos riscos significativos e das declarações da gerência.
- Acompanhamento do status do plano de tratamento de riscos.

Avaliação do Processo de Gerenciamento de Riscos

As avaliações do processo de gerenciamento de riscos em si podem ser realizadas para fornecer uma avaliação razoável para a alta administração e para o conselho de que um programa de gerenciamento de riscos de uma organização é desenvolvido, documentado e operacionalizado com eficácia, para atingir seus objetivos. A avaliação deve ser projetada para responder questões potenciais, as quais podem incluir:

- O programa de gerenciamento de riscos tem o comprometimento adequado da gerência da organização, incluindo status e recursos adequados em relação aos riscos e é uma parte apropriada dos processos e da tomada de decisões da organização?
- O desenvolvimento da estrutura de gerenciamento de riscos e os critérios de avaliação de riscos são apropriados para o contexto interno e externo (ambiente) da organização?
- Existe uma definição adequada e uma comunicação de requisitos, critérios de avaliação de riscos e prestação de contas acerca do desenvolvimento, implementação e manutenção da estrutura de gerenciamento de

riscos e avaliações de áreas específicas de risco?

- A atitude perante o risco foi estabelecida no nível adequado da estrutura de governança da organização?
- A comunicação interna e os mecanismos de reporte são adequados para garantir que os resultados essenciais das atividades de gerenciamento de riscos sejam comunicados de forma adequada dentro da organização (combinando transparência e sensibilidade)?
- Os relatórios às partes interessadas refletem adequadamente a atitude e o tratamento de riscos da organização?
- A comunicação externa e os mecanismos de reporte são adequados para cumprir com requisitos relevantes jurídicos, regulatórios, de governança corporativa e divulgação?
- A mensuração de desempenho e o reporte adequados existem para monitorar o desenvolvimento e a eficácia da estrutura de gerenciamento de riscos?
- Os critérios de avaliação de riscos, apetites, respostas e requisitos de escalação/relatórios são colocados em prática de forma consistente em toda a organização? As pessoas com o conhecimento adequado são as responsáveis pela identificação de riscos? O estado atual da identificação de riscos está adequado?
- A estrutura de riscos e os processos e controles relacionados são modificados conforme as condições do negócio e da organização precisam de mudanças?
- As pessoas com o conhecimento adequado são responsáveis pela análise, avaliação e tratamento/resposta ao risco? Essas atividades são revisadas e aprovadas adequadamente?
- Os planos e status do tratamento de riscos são monitorados e comunicados de forma adequada a todos os níveis apropriados da gerência e do conselho?

Avaliação sobre Riscos Significativos e Declarações da Administração

Durante todos os outros trabalhos de avaliação em que o escopo se relaciona a exposições potenciais maiores identificadas em um processo de gerenciamento de riscos de uma organização, os procedimentos e comunicações de auditoria devem ser desenvolvidos para avaliar as declarações da administração sobre a eficácia dos controles em trazer os riscos para dentro do limite de tolerância de risco da organização.

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

O efeito cumulativo de tais atividades de avaliação, ao longo do tempo, sobre áreas específicas de riscos em um plano de auditoria com base em riscos fornecerá uma avaliação não apenas acerca das áreas específicas de riscos, mas servirá como uma avaliação da eficácia do processo geral de gerenciamento de riscos.

Acompanhamento do Status do Plano de Tratamento de Riscos

Para planos de tratamento de riscos ou de remediação de controles com relação a maiores exposições potenciais, especialmente nos casos em que os planos têm duração relativamente maior, pode ser apropriado monitorar o desempenho em comparação com o plano. No mínimo, tal monitoramento deve ser

desenvolvido para fornecer à administração uma avaliação do progresso em comparação com marcos e validar os relatórios de status de planos de tratamento de riscos para o conselho.

Além disso, tal acompanhamento pode avaliar a estrutura do plano, os recursos, a prestação de contas, o gerenciamento de projetos, etc., e fornecer recomendações e considerações para aumentar a probabilidade de sucesso do plano.

Obtendo Evidências de Auditoria

Em auditorias do processo de gerenciamento de riscos de uma organização, a Prática Recomendada 2120-1, Avaliando a Adequação dos Processos de Gerenciamento de Riscos, parágrafo 8, afirma:

"Os auditores internos precisam obter evidências suficientes e apropriadas para determinar que os principais objetivos dos processos de gerenciamento de riscos estão sendo cumpridos, para formar uma opinião sobre a adequação dos processos de gerenciamento de riscos. Na coleta de tais evidências, o auditor interno pode considerar os seguintes procedimentos de auditoria:

- Pesquisar e revisar acontecimentos atuais, tendências, informações da indústria relacionada ao negócio conduzido pela organização e outras fontes apropriadas de informações, para determinar os riscos e exposições que podem afetar a organização e os procedimentos de controle relacionados utilizados para tratar, monitorar e reavaliar esses riscos.
- Revisar as políticas corporativas e as minutas do conselho para determinar as estratégias de negócio, a filosofia e a metodologia de gerenciamento de riscos, o apetite para o risco e a aceitação de riscos da organização.
- Revisar relatórios anteriores de avaliação de riscos emitidos pela administração, por auditores internos, auditores externos e quaisquer outras fontes.
- Conduzir entrevistas com a gerência de operações e a alta administração para determinar os objetivos das unidades de negócios, riscos relacionados e a mitigação de riscos e atividades de monitoramento de controle da administração.
- Assimilar informações para avaliar de forma independente a eficácia da mitigação de riscos, do monitoramento e da comunicação de riscos e atividades de controle associadas.
- Avaliar a adequação das linhas de reporte para atividades de monitoramento de riscos.
- Revisar a adequação e a oportunidade do reporte dos resultados do gerenciamento de riscos.
- Revisar a integralidade da análise de riscos da administração e as ações tomadas para remediar questões levantadas por processos de gerenciamento de riscos.
- Determinar a eficácia dos processos de autoavaliação da gerência através de observações, testes diretos dos procedimentos de controle e monitoramento, teste da precisão das informações usadas em atividades de monitoramento e outras técnicas apropriadas.
- Revisar as questões relacionadas a riscos que possam indicar fragilidades nas práticas de gerenciamento de riscos e, conforme for apropriado, discutir com a alta administração e o conselho. Se o auditor acredita que a administração aceitou um nível de riscos inconsistente com a estratégia e políticas de gerenciamento de riscos da organização, ou um nível considerado inaceitável para a organização, deve usar a Norma 2600 e orientações relacionadas para orientação adicional."

Técnicas diferentes podem ser usadas para a obtenção de evidências, incluindo:

- Observações – por exemplo, ao estar presente quando o gerenciamento de riscos é realizado nos diferentes níveis da organização, do conselho até os departamentos individuais, programas, projetos e os funcionários.
- Entrevistas.
- Revisões de Documentação – por exemplo, agendas, documentos de apoio e atas do comitê, do conselho executivo ou de outros comitês da alta administração, planos estratégicos e documentos de apoio para decisões de alocação de recursos.
- Os resultados de auditorias anteriores.
- A confiabilidade do trabalho dos outros.
- Técnicas analíticas – por exemplo, análise da causa raiz de falhas detectadas.
- Mapeamento de Processos.
- Análise estatística – por exemplo, a análise dos tipos de incidentes ou "quase acidentes".
- Revisão e avaliação do modelo de riscos.
- Pesquisas.
- Análise da autoavaliação de controle.

Frequentemente, uma combinação de técnicas diferentes de auditoria é usada para reunir informações e evidências suficientes para se chegar a uma conclusão. O auditor escolhe o procedimento mais adequado para o objetivo de auditoria da área. O auditor também avalia se os recursos e habilidades suficientes estão disponíveis para realizar todo o trabalho necessário para servir de suporte suficiente para uma opinião. O auditor considera se seria prudente se recusar a expressar a opinião ou qualificar a opinião, excluindo determinadas áreas ou riscos do escopo da opinião, caso os recursos ou habilidades suficientes não estejam disponíveis.

A exigência de prova varia de acordo com o tipo de opinião que o auditor deseja expressar. Avaliações positivas fornecem o mais alto nível de segurança e, normalmente, também exigem mais evidências para apoiar a opinião. Tal opinião não sugere apenas, por exemplo, se os controles/processos de mitigação de riscos são adequados e eficazes, mas também que evidências suficientes foram obtidas para se estar razoavelmente certo de que evidências do contrário, se é que existem, teriam sido identificadas.

Avaliações negativas não fornecem tanta avaliação e, portanto, normalmente não exigem tantas evidências de auditoria. Ao prestar uma avaliação negativa, o auditor, por exemplo, afirma que, com base no trabalho realizado, nada chamou a atenção do auditor. Por expressar essa opinião, o auditor não se responsabiliza pela suficiência do escopo e dos procedimentos da auditoria para encontrar todas as preocupações ou questões significativas. Tal opinião é geralmente considerada menos valiosa do que a avaliação positiva.

Orientações mais detalhadas sobre opiniões podem ser encontradas no Guia de Práticas "Formulando e Expressando Opiniões de Auditoria Interna".

Conclusões da auditoria devem ser factuais e objetivas e apoiadas por evidências suficientes de auditoria. A suficiência sugere que a evidência de auditoria é factual, adequada e convincente, de forma que uma pessoa prudente e informada chegaria às mesmas conclusões do auditor. A evidência de auditoria deve ser devidamente documentada e organizada.

A atividade de auditoria não deve fornecer inadvertidamente qualquer nível de avaliação falsa (use como referência a PA 2120-2: Gerenciando o Risco da Atividade de Auditoria Interna, parágrafo 8). "Avaliação falsa" é um nível de confiança ou de avaliação com base em percepções ou suposições, em vez de fatos. Em muitos casos, o simples fato de que a atividade de auditoria interna está envolvida em um assunto já pode criar algum nível de falsa avaliação. O escopo do envolvimento da atividade de auditoria

interna pode ser mal interpretado e, consequentemente, pode resultar em falsa avaliação.

Avaliação do Processo de Gerenciamento de Riscos

Um órgão de governança deve ser capaz de determinar até que ponto o processo de gerenciamento de riscos em sua organização atende as necessidades da organização e adotou boas práticas, geralmente aceitas. O gerenciamento de riscos é um componente crítico do sistema de controle interno, de forma que os processos deficientes de gerenciamento de riscos são um indicador de que o sistema de controle interno da organização pode ser deficiente.

É importante que uma organização obtenha uma avaliação de seu processo de gerenciamento de riscos. Esta avaliação deve cogitar a possibilidade de que o auditor interno pode não ser funcionalmente independente da função de gerenciamento de riscos. Neste caso, a avaliação pode ser solicitada a uma parte externa.

Três formas de processos de avaliação que podem ser utilizados na avaliação de um processo de gerenciamento de riscos são descritas abaixo:[5]

- Abordagem dos elementos do processo
- Abordagem dos princípios chave
- Abordagem do modelo de maturidade

Embora cada formulário seja autossuficiente, cada um deles oferece uma perspectiva diferente sobre a eficácia de um processo de gerenciamento de riscos em uma organização. Muitas vezes, a adoção de mais de uma abordagem pode produzir resultados mais informativos e úteis. O processo de gerenciamento de riscos deve ser adaptado adequadamente à organização, seu tamanho, objetivos, cultura e perfil de riscos. Portanto, o processo de avaliação também precisa ser adaptado as necessidades da organização.

Os resultados de qualquer revisão com base em documentos devem ser validados, examinando se a estrutura de gerenciamento de riscos está operando com eficácia na prática. Isto significa que este tipo de atividade de avaliação não deverá ser realizado de forma isolada e deve sempre acompanhar ou envolver uma avaliação normal, com base em controles, que determine se:

- Os riscos estão sendo identificados com eficácia e sendo analisados apropriadamente.
- Há tratamento e controle de riscos adequados e apropriados.
- Há monitoramento e revisão eficazes, conduzidos pela administração, para detectar mudanças nos riscos e controles.

Abordagem dos elementos do processo

Esta abordagem verifica se cada elemento do processo de gerenciamento de riscos está no lugar. É essencial validar as declarações de intenção da administração por meio de evidências de auditoria suficientes para comprovar que o elemento está sendo satisfeito na prática. A representação da administração, apenas, raramente seria suficiente. A ISO 31000 identifica sete componentes do processo de gerenciamento de riscos:

• Elemento 1 – Comunicação: o gerenciamento razoável dos riscos requer uma comunicação estruturada e contínua e consulta com os afetados pelas operações da organização ou atividade.

• Elemento 2 – Estabelecer o Contexto: O ambiente externo (político, social, etc) e interno (objetivos, estratégias, estruturas, ética, disciplina, etc) da organização ou atividade devem ser entendidos antes que toda a gama de riscos possa ser identificada.

[5] Essas abordagens são citadas a partir de *HB158:2010 Delivering assurance based on ISO 31000:2009 Risk management — Principles and guidelines*, uma publicação conjunta da Standards Australia, IIA-Australia e da Fundação de Pesquisa do IIA. A HB158 apresenta uma discussão mais extensa sobre essas e outras questões.

• Elemento 3 – Identificação de Riscos: Identificar riscos deve ser um processo formal e estruturado que considere fontes de risco, áreas de impacto e eventos potenciais, além de suas causas e consequências.

• Elemento 4 – Análise de Riscos: A organização deve utilizar uma técnica formal para considerar a consequência e a probabilidade de cada risco.

• Elemento 5 – Avaliação de Riscos: A organização deve ter um mecanismo para classificar a importância relativa de cada risco, de modo que uma prioridade de tratamento possa ser estabelecida.

• Elemento 6 – Tratamento de Riscos: o gerenciamento razoável dos riscos exige decisões racionais acerca do tratamento dos riscos. Este tratamento consiste, classicamente, em evitar a atividade a partir da qual o risco surge, compartilhar o risco, gerenciar o risco através da aplicação de controles ou aceitar o risco e não realizar nenhuma outra ação.

• Elemento 7 – Monitorar e Revisar: Monitorar inclui verificar o andamento dos planos de tratamento, monitorar controles e sua eficácia, garantir que atividades proscritas sejam evitadas e verificar que o meio ambiente não mudou de uma forma que afetaria os riscos.

Abordagem dos princípios chave

Esta abordagem é baseada no conceito de que, para ser totalmente eficaz, qualquer processo de gerenciamento de riscos deve satisfazer um conjunto mínimo de princípios ou características. A ISO 31000 inclui uma seção (Cláusula 4) sobre esses princípios.

Uma auditoria com base nesses princípios avalia até que ponto eles são verdadeiros para o processo de gerenciamento de riscos em uma organização:

- **O gerenciamento de riscos cria e protege o valor.**[6] Isto sugere a aplicação do gerenciamento de riscos mais rigoroso quando o valor em jogo é o mais alto. Também sugere que uma série de técnicas aplicáveis a diversos níveis de exposição deve estar disponível na organização.
- **O gerenciamento de riscos é uma parte integrante dos processos organizacionais.**[7] O gerenciamento de riscos não deve ser visto como uma tarefa complementar.
- **O gerenciamento de riscos faz parte da tomada de decisões.**[8] Quanto mais importante a decisão, mais explícita deve ser essa associação.
- **O gerenciamento de riscos aborda a incerteza de forma explícita.**[9] As avaliações de riscos seriam encarregadas de documentar áreas de incerteza e considerar qual a melhor forma de resolver a incerteza identificada.
- **O gerenciamento de riscos é sistemático, estruturado e oportuno.**[10]
- **O gerenciamento de riscos é baseado nas melhores informações disponíveis.**[11] Obter informações pode ser caro e o processo deve fornecer orientações sobre o que constitui informação suficiente.

[6] © ISO. Esse material é reproduzido da ISO 31000:2009 ou do Guia ISO 73:2009, com permissão do *American National Standards Institute* (ANSI) em nome da *International Organization for Standardization* (ISO). Nenhuma parte deste material da ISO pode ser copiado ou reproduzido de qualquer forma, por sistema de restauração eletrônica ou disponibilizado de qualquer outra forma na Internet, em rede pública, por satélite ou outro meio sem a permissão prévia por escrito do ANSI. Cópias desta norma podem ser adquiridas no ANSI, 25 West 43rd 10036, (212) 642-4900, http://webstore.ansi.org.[7] Ibid.[8] Ibid.[9] Ibid.[10] Ibid.[11] Ibid.

- **O gerenciamento de riscos é feito sob medida.**[12] Não é um processo "fora da caixa" e deve ser compatível com as operações da organização.
- **O gerenciamento de riscos considera fatores humanos e culturais.**[13] Os processos devem ser apropriados às competências e à cultura dos que devem usá-los.
- **O gerenciamento de riscos é transparente e inclusivo.**[14] Deve haver um envolvimento adequado e oportuno das partes interessadas.
- **O gerenciamento de riscos é dinâmico, interativo e receptivo a mudanças.**[15] O processo deve ser revisado regularmente e deve reagir a mudanças na organização e em seu ambiente, para que continue relevante.
- **O gerenciamento de riscos facilita a melhoria contínua e o aperfeiçoamento da organização.**[16] O gerenciamento de riscos deve amadurecer junto com outros processos organizacionais.

Abordagem do Modelo de Maturidade

A abordagem do modelo de maturidade tem como base a afirmação de que a qualidade do processo de gerenciamento de riscos de uma organização deve melhorar com o tempo. Sistemas imaturos de gerenciamento de riscos trazem muito pouco retorno para o investimento que foi feito e, muitas vezes, operam como uma despesa geral de conformidade ou como uma imposição, mais preocupados com o reporte dos riscos do que com seu tratamento eficaz. Processos eficazes de gerenciamento de riscos se desenvolvem ao longo do tempo, com valor adicional a ser agregado a cada passo do processo de maturação. Esta abordagem fornece uma avaliação do ponto em que o processo de gerenciamento de riscos da organização está na curva de maturidade, de modo que o conselho e a administração possam avaliar se ele atende as necessidades atuais da organização e se está amadurecendo como esperado.

Um aspecto fundamental da abordagem do modelo de maturidade é a ligação do desempenho e progresso do gerenciamento de riscos na execução de um plano de gerenciamento de riscos a um sistema de mensuração e gestão de desempenho. Os dados que resultarem de tal sistema podem ser apresentados à alta administração e ao conselho como evidências de melhoria do gerenciamento de riscos. Os componentes de um sistema deste tipo normalmente são:

- Um protocolo de padrões de desempenho, considerando abordagens de gerenciamento de riscos e prevendo futuras necessidades estratégicas. Os padrões de desempenho são normalmente apoiados por uma lista mais detalhada de requisitos de desempenho que permitem a mensuração de qualquer melhoria no desempenho.
- Um guia de como os padrões e subrequisitos podem ser satisfeitos na prática.
- Um meio de medir o desempenho real em comparação com cada padrão e subrequisito.
- Um meio de registro e de reporte do desempenho e de melhorias no desempenho.
- A verificação periódica independente da avaliação da administração.

[12] © ISO. Esse material é reproduzido da ISO 31000:2009 ou do Guia ISO 73:2009, com permissão do American National Standards Institute (ANSI) em nome da International Organization for Standardization (ISO). Nenhuma parte deste material da ISO pode ser copiado ou reproduzido de qualquer forma, por sistema de restauração eletrônica ou disponibilizado de qualquer outra forma na Internet, em rede pública, por satélite ou outro meio sem a permissão prévia por escrito do ANSI. Cópias desta norma podem ser adquiridas no ANSI, 25 West 43rd 10036, (212) 642-4900, http://webstore.ansi.org.[13] Ibid.[14] Ibid.[15] Ibid.[16] Ibid.

A cláusula 4 da ISO 31000 contém uma lista de práticas e "princípios" importantes que devem ser o ponto de partida para qualquer avaliação de maturidade. Estes princípios não resolvem apenas se "*o elemento do processo ou sistema existe*", mas também se "*é eficaz e relevante para sua organização*" e "*agrega valor*". Na verdade, o primeiro princípio é que o gerenciamento de riscos deve agregar valor.

O desempenho real, em comparação com o padrão de desempenho, é avaliado usando algum sistema de mensuração de maturidade que dá crédito para a intenção, mas a nota máxima só pode ser obtida pela implementação completa e aplicação prática do padrão. Um possível sistema de mensuração de maturidade (com base na ideia original de *Capability Maturity Models*, desenvolvidos pela *Carnegie Mellon University*) é mostrado abaixo.

MEDIDA	NENHUMA	MUITO POUCA	ALGUMA	BOA	COMPLETA
Significado	Muito pouca ou nenhuma conformidade com o requisito de qualquer forma.	Conformidade apenas limitada com o requisito. A administração apoia a intenção, mas a conformidade, na prática, é pouca.	Conformidade limitada com a declaração do elemento. Concordam certamente com a intenção, mas a conformidade é limitada na prática.	A administração apoia completamente a intenção, mas há conformidade parcial na prática.	Conformidade absoluta com a declaração do elemento – na intenção e na prática – em todos os momentos e locais.

Figura 3 – Modelo de Maturidade – fonte HB158

Avaliando a Qualidade da Documentação do Gerenciamento de Riscos

A extensão da documentação do ERM de uma entidade varia de acordo com o tamanho e a complexidade da entidade. Organizações maiores geralmente têm manuais de políticas, organogramas formais, descrições dos cargos já elaboradas, instruções de operação, fluxogramas do sistema de informação e assim por diante. Organizações menores e menos complexas normalmente têm consideravelmente menos documentação.

Muitos aspectos do ERM podem ser informais e não documentados e, ainda assim, podem ser realizados periodicamente e altamente eficazes. Estas atividades podem ser testadas da mesma maneira que as atividades documentadas. O fato de que os elementos do ERM não são documentados não significa necessariamente que o ERM não é eficaz ou não pode ser avaliado. Um nível apropriado de documentação, no entanto, geralmente torna o monitoramento mais eficiente. É útil em outros aspectos também. Facilita o entendimento dos funcionários de como o processo funciona e de suas respectivas funções e facilita fazer modificações, quando necessário.

Ao decidir documentar o processo de avaliação em si, o auditor interno normalmente vai trabalhar com a documentação existente dos processos de ERM da entidade. A documentação existente será tipicamente complementada com outros documentos preparados pelo auditor, incluindo as evidências dos testes e as análises realizadas no processo de avaliação. A

natureza e a extensão da documentação são normalmente mais substanciais quando declarações sobre o ERM são feitas a outras partes.

Quando a administração pretende fazer uma declaração a partes externas sobre a eficácia do ERM, ela deve considerar desenvolver e reter documentos que apoiem a declaração. O auditor interno deve considerar se:

- Uma estratégia para gerenciar informações de riscos vindas de todas as fontes está em prática.
- A infraestrutura necessária para a comunicação das informações de riscos está em prática.
- Existem definições comuns.
- Existem diretrizes para a criação, exclusão e o compartilhamento de informações de riscos.
- Existem recursos adequados atribuídos.
- A tecnologia é rentável e usada onde for apropriado.
- Uma abordagem proativa é usada no monitoramento.
- As informações de riscos fazem parte do processo de planejamento.
- As informações de riscos são integradas às informações de desempenho.

Estas considerações e quaisquer decisões tomadas documentadas. Tal documentação pode ser útil, caso a afirmação seja contestada posteriormente.

Autores:

Andrew MacLeod, CIA

Patricia A. MacDonald

Benito Ybarra, CIA

Trygve Sorlie, CIA, CCSA

Brian Foster, CIA

Teis Stokka, CIA

Revisores e Colaboradores:

Douglas J. Anderson, CIA

Steven E. Jameson, CIA, CCSA, CFSA

James A. Rose, III, CIA

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.

Disclaimer

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