TONE at the TOP®

TRADUZIDO POR • INSTITUTO DOS AUDITORES INTERNOS DO BRASIL • IIA Brasil

Trazendo à alta administração, conselhos de administração e comitês de auditoria informações concisas sobre tópicos relacionados a governança.

Edição 134 | Abril de 2026

O que os Conselhos precisam saber sobre a supervisão de ERM

No atual ambiente empresarial incerto, os membros dos conselhos estão sendo chamados a aprimorar sua supervisão de riscos. Todos os tipos de stakeholders esperam, cada vez mais, que os conselhos assumam um papel proativo na supervisão de um cenário de riscos em constante mudança.

Os riscos enfrentados pelas organizações incluem perturbações geopolíticas, preocupações com a cibersegurança, o impacto das tecnologias emergentes, problemas na cadeia de suprimentos, escassez de mão de obra e condições climáticas severas, para citar apenas alguns. "O gerenciamento de riscos corporativos não é apenas uma responsabilidade comercial e operacional da equipe de gestão de uma empresa — é uma questão de governança e estratégia que se enquadra diretamente na responsabilidade de supervisão do conselho de administração", de acordo com o artigo *"Risk Management and the Board of Directors"*, do Harvard Law School Forum on Corporate Governance.

O artigo acrescenta que os tribunais e órgãos regulatórios estão se concentrando na supervisão do conselho e nas respostas do conselho quando ocorrem crises. Embora os conselheiros não devam se envolver no gerenciamento diário dos riscos, "o papel de supervisão de todo conselho deveria incluir o envolvimento ativo no monitoramento dos principais fatores de risco corporativo, inclusive por meio do uso devido dos comitês do conselho", observa o artigo.

Esta edição examina as considerações do conselho no gerenciamento de riscos corporativos *(enterprise risk management* - ERM) e o papel da auditoria interna em fornecer ao conselho avaliações e orientações valiosas.

Determinando a Maturidade do ERM

Uma avaliação realista do nível de maturidade do ERM da organização pode proporcionar aos conselhos uma compreensão mais ampla da situação atual e das mudanças que possam ser necessárias. De acordo com o *Director's Guide to ERM Fundamentals* da PwC, em um nível geral, as etapas de maturidade do ERM de uma organização incluem:

- **Inicial.** Há algumas práticas informais, mas não há políticas ou processos formais. A organização reage às questões.
- **Em desenvolvimento.** Há sistemas e processos que são eficazes em alguns aspectos de sua criação ou operação. As abordagens estão de certa forma alinhadas às operações de negócios.
- **Desenvolvido.** Há frameworks e sistemas formais incorporados e em operação para atender a Normas reconhecidas.
- **Integrado.** A organização possui sistemas e processos integrados, colaborativos e aprimorados, que permitem uma resposta coordenada, estratégica e eficiente aos riscos atuais e emergentes.
- **Otimizado.** Sistemas, processos e cultura estão bem integrados e alinhados às prioridades estratégicas. A tecnologia é utilizada para aprimorar a governança, o gerenciamento de riscos e o monitoramento/reporte.

"À medida que o programa de ERM amadurece, o conselho pode promover a melhoria contínua, questionando a gestão sobre o que está funcionando e o que não está", afirma o guia.

Aprofundando

O Sumário Executivo de *Enterprise Risk Management-Integrating With Strategy and Performance* do COSO sugere perguntas que os conselhos podem fazer à gestão sobre o ERM, incluindo:

- Toda a gestão — não apenas o diretor de riscos — é capaz de explicar como o risco é considerado na seleção de estratégias ou decisões de negócios?
- A gestão consegue explicar claramente o apetite a risco da entidade e como ele pode influenciar uma decisão específica? O COSO observa que a resposta pode revelar insights sobre a verdadeira mentalidade da organização em relação à tomada de riscos.
- A alta administração consegue discutir não apenas os processos de risco, mas também como a cultura da organização facilita ou inibe a tomada de riscos?
- Que perspectiva a gestão utiliza para monitorar a cultura de risco, e como isso mudou? Dadas as inevitáveis mudanças dentro e fora da organização, como o conselho pode ter certeza de que receberá uma resposta adequada e tempestiva da gestão?

O *Compendium of Examples* do COSO inclui observações específicas sobre governança. Um dos exemplos aborda como o ERM pode aprimorar a tomada de decisões para obter melhores resultados, ampliar oportunidades de melhoria e minimizar surpresas negativas.

No exemplo, uma empresa tomou medidas para compreender melhor as capacidades de ERM existentes e desejadas. Por exemplo, o CEO e o auditor interno participam de reuniões de avaliação de desempenho com as divisões operacionais, para acompanhar o progresso em relação às metas de desempenho e determinar como a compreensão dos riscos afeta a forma como buscam atingir essas metas. Graças a esse esforço, o CEO consegue entender melhor o desempenho dos negócios e o auditor interno tem conseguido elaborar com mais eficácia um plano de auditoria interna.

Orientações sobre as melhores práticas

As organizações que buscam aprimorar sua abordagem de gerenciamento de riscos corporativos podem escolher entre diversos frameworks de ERM, incluindo o *Enterprise Risk Management-Integrated Framework do COSO,* a *ISO 31000 Risk Management Standard* e o *U.S. National Institute of Standards and Technology's Risk Management Framework.* De acordo com o documento *"Enterprise Risk Management Fundamentals"* da Optro, esses frameworks tipicamente compartilham cinco componentes principais:

- Cultura, governança e valores da empresa.
- Planejamento estratégico, objetivos e definição de metas.
- Ciclo de gerenciamento de riscos.
- Monitoramento e melhoria contínua.
- Transparência, comunicação e reporte.

O Modelo das Três Linhas do The IIA é um modelo de melhores práticas para a supervisão do gerenciamento de riscos pelo conselho de administração, mostrando como os principais papéis atuam em conjunto para apoiar uma governança sólida. A ferramenta *Enterprise and Business Process Risks Tool,* alinhada ao Modelo, ajuda as organizações a implementar e gerenciar um programa estruturado de ERM, fornecendo uma abordagem prática e personalizável à identificação, avaliação, gerenciamento e monitoramento dos riscos nos níveis corporativo e de processos.

Parceria com a Auditoria Interna

A auditoria interna pode ser uma parceira valiosa para os conselhos em seus esforços para aprimorar a ERM. O The IIA relata que os papéis da auditoria interna relacionados ao ERM estão evoluindo e um número crescente de CAEs tem responsabilidade pelo ERM. De acordo com o estudo *North American Pulse of Internal Audit* do The IIA, a porcentagem de CAEs que relataram ser responsáveis por programas de ERM, além de seu papel como chefe de auditoria interna, subiu para 34% em 2025.

Um ponto importante para uma função de gerenciamento de riscos eficaz é a colaboração entre as três linhas. De acordo com o Modelo das Três Linhas do The IIA:

- **Primeira linha:** Gestão e líderes operacionais que gerenciam os riscos.
- **Segunda linha:** Funções de gerenciamento de riscos e conformidade que monitoram e supervisionam os riscos.
- **Terceira linha:** Terceira linha: Auditoria interna, que oferece avaliação e assessoria independentes para a concretização das metas da organização.

Sobre o The IIA

O Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos, que atende a mais de 265.000 membros e concedeu mais de 200.000 certificações *Certified Internal Auditor* (CIA) no mundo todo. Criado em 1941, o The IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, visite **theiia.org.**

The IIA

1035 Greenwood Blvd.
Suíte 401
Lake Mary, FL 32746 EUA

Assinaturas Gratuitas

Visite **theiia.org/Tone** para se cadastrar para uma assinatura gratuita.

Feedback do Leitor

Envie perguntas/comentários para **Tone@theiia.org.**

Expectativas para os Conselhos

As principais responsabilidades do conselho relacionadas a riscos incluem:

- Definir o apetite e a tolerância a risco da organização.
- Aprovar e monitorar o framework de ERM.
- Alinhar a estratégia e a exposição ao risco.
- Supervisionar a cultura de risco e os controles internos.
- Monitorar riscos emergentes e áreas críticas.
- Assegurar papéis e responsabilidades claros.

– Diligent, "*Understanding Board Oversight of Risk Management Now and for the Future*"

O Modelo "deixa claro que, embora a independência da auditoria interna em relação à gestão garanta que ela esteja livre de obstáculos e viés no planejamento e na execução de seu trabalho, a independência não implica isolamento completo", de acordo com *Collaboration Without Compromise: Practitioner Perspectives on Internal Audit, Risk Management, and Governance Practices,* um relatório da Baker Tilly, da Internal Audit Foundation e da Wolters Kluwer TeamMate. Como as responsabilidades da auditoria interna aumentam em diversas áreas, incluindo o gerenciamento de riscos empresariais (ERM), surgem oportunidades para elevar o papel dessa função como avaliadora independente da eficácia da governança e do gerenciamento de riscos.

O relatório destaca que 90% dos entrevistados veem benefícios na coordenação entre a segunda e a terceira linhas, incluindo:

- Maior cobertura de riscos.
- Redução da duplicação de esforços.
- Alinhamento organizacional fortalecido.
- Melhor comunicação com o conselho e reporte mais eficiente.

Trinta e nove por cento dos entrevistados afirmam ter observado uma maior integração entre as funções de auditoria interna e de gerenciamento de riscos nos últimos cinco anos e 60% acreditam que esse número aumentará nos próximos cinco anos. "Quando cuidadosamente criadas por meio do compartilhamento de informações, atividades coordenadas e prioridades alinhadas, tais abordagens ajudam a garantir que os conselhos recebam informações confiáveis para a tomada de decisões bem fundamentadas", afirma o relatório.

Uma Visão Clara

Acima de tudo, o ERM consiste em reconhecer ou antecipar mudanças e decidir o que elas significam para a organização. O COSO observa que uma visão clara das mudanças permite que as organizações tomem decisões acertadas sobre perguntas difíceis, como, por exemplo, se é melhor fazer novos investimentos ou recuar. Conforme afirma o COSO, "o gerenciamento de riscos corporativos fornece o framework adequado para que os conselhos avaliem riscos e adotem uma mentalidade de resiliência".

Tecnologia e ERM

Há um grande potencial para que a inteligência artificial (IA) desempenhe um papel mais significativo no ERM. Menos de um em cada dez entrevistados relata usar a IA com frequência para auxiliar na identificação de riscos (6%) ou afirma que a utiliza intensamente para a inserção de dados em atividades de gerenciamento de riscos (3%), de acordo com o relatório *Enhanced Enterprise Risk Management and Strategic Decision-Making*, da Baker Tilly e da Internal Audit Foundation.

Plataformas integradas de governança, risco e conformidade (GRC) podem apoiar os processos de ERM. Uma Pesquisa de Maturidade do ERM, realizada pela Baker Tilly e pela Internal Audit Foundation, revela que apenas 21% dos profissionais que responderam às perguntas as utilizam. Os programas de ERM de muitas organizações baseiam-se em ferramentas simples, como processadores de texto e planilhas (59%) ou ferramentas tecnológicas internas (20%).

"Em uma época em que a transformação digital acelerou a dependência da tecnologia em todos os aspectos das operações e redefiniu estratégias, é perigoso que o ERM não acompanhe esse ritmo", alerta o relatório *Enhanced Enterprise Risk Management.*

Com isso em mente:

- Softwares como serviço e ferramentas de GRC podem aprimorar os programas básicos de ERM e promover uma compreensão mais profunda dos riscos em toda a empresa. Eles podem centralizar dados, automatizar fluxos de trabalho e facilitar a identificação de riscos, o que pode permitir uma melhor tomada de decisão e minimizar a exposição a riscos.

- O relatório orienta as organizações a apoiar, facilitar e monitorar a exploração do uso seguro da IA dentro da organização e a identificar formas de aplicar a IA nos processos de ERM.

"Superar as abordagens tradicionais de ERM com a ajuda de ferramentas colaborativas, varredura externa de riscos, integração multifuncional e tecnologias de ponta deveria ser a meta de todos os programas de ERM", afirma o relatório.

Entre os experts globais entrevistados, 50% esperam um panorama de riscos globais turbulento ou tempestuoso nos próximos dois anos, número que crescerá para 57% nos próximos 10 anos. Apenas 1% prevê um panorama tranquilo.

– Relatório de Riscos Globais de 2026 do Fórum Econômico Mundial.