TONE at the TOP®

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

Edição 93 | Junho de 2019

A Auditoria Anda na Linha Entre a Auditoria e o Gerenciamento de Riscos

Executivos de auditoria interna reportam sobre vários tipos de coisa, e isso não vai mudar. A quem todas essas coisas devem ser reportadas, no entanto, está em aberto.

Por um lado, solicita-se que os executivos de auditoria façam cada vez mais. Espera-se que sejam conselheiros de confiança, aconselhando o conselho sobre riscos. Devem adotar novas tecnologias, que permitam melhores análises e um monitoramento mais perceptivo do risco em toda a empresa.

Ao mesmo tempo, os conselhos estão sob pressão. Os reguladores, acionistas, clientes, parceiros de negócios e outros querem que façam um trabalho melhor de governança dos riscos — não apenas revisando ou definindo tolerâncias de riscos. Os stakeholders querem uma maior prestação de contas para os conselhos, o tempo todo.

Pense no que isso significa. Se o executivo de auditoria e o conselho estiverem sendo desafiados a fazer um melhor trabalho nas mesmas tarefas — avaliar riscos e desenvolver a capacidade de intervir quando um risco vai além da zona de conforto —, um emaranhado de questões é levantado sobre governança corporativa, avaliação de riscos e o papel do *chief audit executive.*

Por exemplo, os conselhos corporativos devem estabelecer comitês de risco? Se sim, que problemas o executivo de auditoria deve reportar a eles? É sensato que o CAE discuta algumas questões com o comitê de risco, e outras questões com o comitê de auditoria? O papel do CAE deve ser dividido? Ou seria verdade o inverso: a tecnologia moderna está fundindo a auditoria interna e o gerenciamento de riscos em uma função maior de avaliação de riscos?

"Não tenho certeza de que nós, como disciplina, explicamos bem o suficiente os benefícios dos proprietários dos riscos para aqueles que não são tão apaixonados quanto somos", diz Tom McLeod, diretor de risco da Australian Broadcasting Corp. e ex-diretor do conselho do Institute of Internal Auditors–Austrália.

Como resultado, os executivos de auditoria podem estar à deriva em um papel que ninguém esperava, abrangendo deveres de auditoria e de gerenciamento de riscos. Eles sempre foram bons em auditoria e a tecnologia moderna está fazendo com que fiquem bons no gerenciamento de riscos também — e, bem, alguém tem que fazê-lo.

"É aquela lenta jornada", diz McLeod, "em que você não percebe que está mais envolvido no monitoramento de riscos, até que esteja mais envolvido no monitoramento de riscos".

Isso é verdade para os executivos de auditoria e para os conselhos corporativos. Então, como os dois grupos canalizam essa evolução de maneira produtiva?

Sobre o The IIA

The Institute of Internal Auditors Inc. (The IIA) é uma associação profissional internacional com mais de 190.000 membros em mais de 170 países e territórios. O The IIA serve como principal defensor da profissão de auditoria interna, criador global de tendências e maior pesquisador e educador.

The IIA

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

Assinaturas Gratuitas

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

Feedback do Leitor

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

Conselho Consultivo de Conteúdo

Com décadas de experiência na alta administração e em conselhos corporativos, os estimados profissionais a seguir oferecem orientação quanto ao conteúdo desta publicação:

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

Comece Com As Pressões Sobre o Conselho

De acordo com um estudo de 2018 do *EY Center for Board Matters*, divulgado no *Harvard Law School Forum on Corporate Governance and Financial Regulation*, apenas cerca de 11% dos conselhos do S&P 500 têm um comitê de risco. Mesmo assim, a concentração está no setor financeiro, no qual 74% das empresas têm comitês de risco. Fora desse setor, o percentual cai, com apenas 4% dos setores de consumo, industriais, técnicos e de serviços tendo comitês de risco.

Mas esses números não contam toda a história. Por exemplo, o Federal Reserve exige que bancos de capital aberto com ativos de US$ 10 bilhões ou mais tenham um comitê de risco, portanto, não é de surpreender que muitos o façam.

Enquanto isso, de acordo com o mesmo estudo da EY, 14% das empresas de consumo têm um comitê de política pública e 38% têm um comitê de responsabilidade corporativa. No setor de saúde, 21% têm um comitê de assuntos regulatórios e 18% têm um comitê de tecnologia.

Tudo isso faz sentido. Empresas de consumo preocupam-se em serem vistas como bons cidadãos corporativos; portanto, mais delas têm comitês de responsabilidade corporativa. Empresas de saúde são altamente regulamentadas, especialmente quanto a informações pessoais de saúde; como resultado, têm mais comitês de conformidade e tecnologia. Desde que a empresa tenha algum comitê do conselho que examine os riscos importantes para o negócio, quem liga para como ele se chama?

James Lam, presidente do comitê de risco da E*TRADE e consultor de gerenciamento de riscos de longa data, diz que qualquer negócio com mais de US$ 1 bilhão em receita anual deve considerar a criação de um comitê de risco dedicado.

Na perspectiva de Lam, esse comitê deve abordar "riscos técnicos e granulares", que poderiam ir de conformidade à cibersegurança, à prevenção da lavagem de dinheiro, ou qualquer outra coisa que demande atenção. O objetivo é eliminar essas questões da agenda do conselho, para que ele possa se concentrar nos riscos estratégicos.

"Se o conselho conseguir fazer tudo isso, tudo bem", diz Lam. "Mas é uma agenda bem cheia."

McLeod cita o exemplo da Rio Tinto, onde foi *chief audit executive* no início de 2010. O conselho tinha um comitê de sustentabilidade que analisava os direitos à terra, o uso da água e outras preocupações ambientais — "questões profundas e fundamentais de riscos, que raramente eram abordadas ou consideradas", diz ele.

McLeod reportava ao comitê de auditoria e ao comitê de risco da Rio Tinto, mas sabia o que precisava discutir com cada comitê. Quando os comitês de risco e auditoria são combinados, "não há um entendimento claro das delimitações", explica.

Tudo isso pode representar, mais do que qualquer outra coisa, um mau entendimento da governança de riscos. Os comitês de auditoria existem há décadas, e seus deveres relacionados ao forte reporte financeiro são claros desde a Lei Sarbanes-Oxley de 2002. Ou seja, as pessoas entendem o que os comitês de auditoria devem fazer.

A governança de riscos é vaga. Fora do setor bancário, são escassos os regulamentos específicos sobre o que um comitê de risco faz. Pensar sobre o risco exige criatividade e imaginação — características que geralmente não são exigidas dos membros do comitê de auditoria.

"O comitê de auditoria 'é pago para pensar dentro da caixa', em um mundo de divulgações corporativas, regras de reporte financeiro e testes de SOX", diz Lam. "Existem regras muito específicas, requisitos de controle interno e testes".

O comitê de risco, no entanto, "é pago para pensar fora da caixa". Então, verá as atividades de negócios da organização de forma diferente da perspectiva do comitê de auditoria. Um comitê de risco precisará de diferentes tipos de informação — mais tipos de informação — para orientar seu trabalho.

O Problema do Meio-Termo

Bem, calma. *Chief audit executives* fornecem informações ao conselho. Então, se o conselho estabelecer comitês separados de auditoria e risco, o CAE pode reportar a ambos?

McLeod acredita que sim. Foi o que fez na Rio Tinto. No outro extremo do espectro, no entanto, estão vozes como Richard Anderson, presidente do comitê de risco da Pay.UK em Londres e membro do comitê de auditoria da empresa. Ele vê o gerenciamento de riscos como "enfrentar os múltiplos futuros que nosso negócio pode encarar" e, portanto, algo bem diferente da função de auditoria.

O que torna essa questão tão delicada é a chegada da tecnologia moderna. Sim, a inteligência artificial, a automação robótica de processos e a visualização de dados ajudam o *chief audit executive* a identificar riscos e testar controles internos de formas nunca antes possíveis. Essa é a boa notícia.

Por outro lado, depois que a equipe de auditoria criar as ferramentas de análise de riscos da próxima geração, elas imediatamente se tornam ferramentas de gerenciamento de riscos, que as funções de negócios podem usar para orientar suas operações.

Itens de Ação

Revise os estatutos do comitê. Os comitês de auditoria têm uma preocupação atrás da outra, desde o risco de conformidade até a cibersegurança, cultura corporativa e muito mais — além de seus deveres regulares de supervisionar o reporte financeiro e os controles internos. Revisite os estatutos do comitê do conselho, para verificar se aqueles riscos de reporte não-financeiro seriam atendidos de melhor forma por um comitê de risco, que pudesse dar a essas questões a atenção que exigem.

Avalie os deveres de avaliação de riscos. Da mesma forma, revise todos os deveres de avaliação de riscos da organização, para verificar se seria justificada a criação do cargo de *chief risk officer*. Provavelmente, a maioria das funções da Primeira e Segunda Linhas de Defesa já executam algum gerenciamento de riscos, mesmo que não tenham uma abordagem uniforme e disciplinada. Se for esse o caso, um CRO ajudaria a trazer essa disciplina? Ou uma organização menor poderia adotar uma metodologia padrão para alcançar a mesma coisa?

Considere como a tecnologia ajudará no gerenciamento de riscos. A análise de dados, as ferramentas de visualização e a inteligência artificial podem ser facilmente tecnologias de "dupla utilização" — capazes de ajudar a função de auditoria a avaliar os controles e de ajudar outras funções a gerenciar os riscos. Sua organização tem uma estratégia de tecnologia para orientar isso, para ajudar a alta administração e o conselho a tomar melhores decisões?

Por exemplo, seria um exercício relativamente simples para a equipe de auditoria criar algoritmos que encontrassem dados pessoais coletados antes do consentimento ou contratos de revenda assinados antes que a *due diligence* de terceiros fosse feita. Depois, as equipes de marketing ou vendas poderiam usar esses algoritmos para gerenciar seus próprios riscos. Para negócios globais, com preocupações de privacidade ou suborno, essas são questões que um comitê de risco poderia querer supervisionar.

Neste mundo impulsionado pela análise de dados — que é, lembre-se, o mundo que todos dizem que a função de auditoria deve adotar —, onde termina a auditoria e começa o gerenciamento de riscos operacionais?

Anderson não poupa palavras sobre a ideia de a auditoria interna desenvolver algoritmos que a empresa possa usar no gerenciamento de riscos: “eles não devem desenvolver ou executá-los.” As empresas devem criar seus próprios modelos, cuja eficácia a auditoria, então, pode testar.

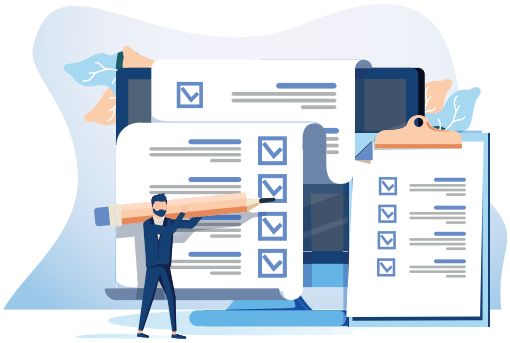
Feliz ou infelizmente, no entanto, muitas empresas não fazem isso. Em vez disso, engatinham no gerenciamento de riscos baseado em análise e convidam a auditoria interna a liderar o caminho, porque ela vem aprimorando suas habilidades de análise de dados há anos, enquanto estuda transações financeiras ou gastos de T&E.

Considere a ideia do início ao fim: o conselho começa com a urgência de um melhor gerenciamento de riscos, mas não define o que um comitê deveria fazer para resolvê-la. Em vez disso, o conselho diz, essencialmente, “você, função de auditoria — ajude-nos com isso”.

Esse impulso poderia levar a auditoria e o gerenciamento de riscos a se tornarem, combinadas, o que McLeod chama de “função chefe de avaliação. (...) O papel do futuro, uma fusão dos dois, já que nunca foram devidamente delineados.”

Mas McLeod acrescenta: "o que fica pelo caminho é o aspecto da independência."

E, por fim, os conselhos precisam entender a exclusividade que a auditoria interna traz e o valor derivado de se ter uma função independente.



Pesquisa Rápida

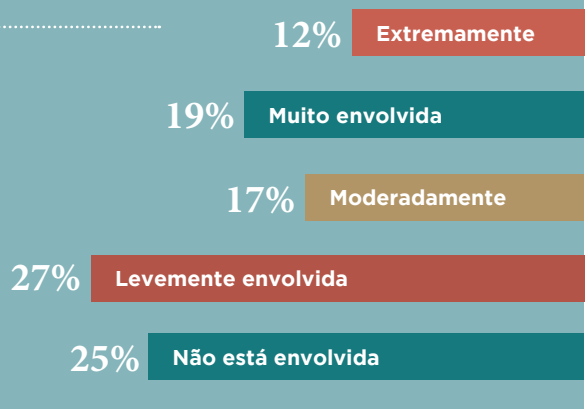
Com que frequência a auditoria interna fornece relatórios ao Comitê de Risco?

- ❑ Regularmente
- ❑ Periodicamente, sobre questões específicas de risco
- ❑ Mediante solicitação
- ❑ Não há Comitê de Risco separado

Visite **www.theiia.org/tone** para responder à pergunta e ver como outros estão respondendo.

RESULTADOS DA PESQUISA RÁPIDA:

Qual o nível de envolvimento da auditoria interna em garantir fluxos precisos e completos de informação para o Conselho?



Fonte: Pesquisa do Tone at the Top de Abril de 2019.