TRADUZIDO POR • INSTITUTO DOS AUDITORES INTERNOS DO BRASIL •

IIA Brasil

GLOBAL PERSPECTIVES & INSIGHTS

Governança, Riscos e Controle

PARTE I: Repensando o Apetite a Risco da Perspectiva do Risco Não Financeiro

PARTE II: Quantificando o Risco Não Financeiro

PARTE III: Como a Transformação Digital Está Transformando o GRC

The Institute of Internal Auditors

Conteúdos

Parte 1: Repensando o Apetite a Risco da Perspectiva do Risco Não Financeiro

Sobre o Especialista

W. Scott Page, CIA, CCSA, CRMA, CPA, CA

Scott é diretor de auditoria interna da MDA, Ltd. Com sede em Brampton, Ontário, Canadá, a MDA fornece geointeligência, robótica, e operações e sistemas de satélite espaciais. Scott tem mais de 20 anos de experiência nas indústrias de fabricação espacial e de defesa, serviços profissionais, saúde, serviços de distribuição e manufatura.

Introdução

O conceito de apetite a risco — a quantidade de risco que uma organização está preparada para aceitar para atingir seus objetivos — é fundamental para uma governança eficaz em todas as organizações. Historicamente, as decisões sobre o apetite a risco de uma empresa eram regidas principalmente por considerações de risco financeiro. Isso está mudando, no entanto, em meio a um foco crescente em riscos não financeiros, incluindo riscos ambientais, sociais e de governança (ESG) e considerações regulatórias e de reporte relacionadas. Cada vez mais, mais atenção está sendo dada aos riscos associados à forma como as organizações operam em relação ao mundo ao seu redor.

Avaliar esses riscos como parte do apetite a risco é uma área em que os auditores internos podem fazer contribuições significativas. Este *Brief* de Conhecimento Global, o primeiro de uma série de três partes sobre governança, riscos e controle (GRC) do The IIA, examina em detalhes este tópico, os desafios de repensar o apetite a risco tendo em mente o risco não financeiro e o importante papel da auditoria interna no processo.

O Apetite a Risco

Equilibrando Ameaças e Oportunidades

Perfis de risco afetam o apetite

O *International Professional Practice Framework* do The IIA define o apetite a risco simplesmente como "o nível de risco que uma organização está disposta a aceitar". Na prática, o apetite a risco, também conhecido como tolerância a risco, representa um equilíbrio entre os potenciais benefícios da inovação e as ameaças que a mudança inevitavelmente traz. Como tal, os apetites a risco são únicos para cada organização e variam dependendo de vários fatores, como:

Cultura — Com base em diretrizes, atitudes ou outros fatores de longa data, a organização pode ser mais ou menos agressiva em sua abordagem ao risco.

Indústria — A quantidade de regulamentação ou outras preocupações de conformidade, por exemplo, podem ter impacto sobre o quanto a organização é aversa ao risco.

Mercado — O nível de competição que uma empresa enfrenta ou a estabilidade de seu mercado são fatores que podem afetar a tomada de decisão sobre riscos.

Solidez financeira — Uma empresa menos confiante em sua posição financeira pode ser mais avessa ao risco[1].

O Que é o Risco Não Financeiro?

Incorporar o risco não financeiro nas discussões sobre o apetite a risco começa com a compreensão do que ele pode abranger. De fato, o grande número de riscos que se enquadram nessa categoria (consulte a lista ao lado) aumenta as chances de que alguns sejam negligenciados ou mal interpretados, o que ressalta a importância de incorporar riscos não financeiros em qualquer discussão sobre o apetite a risco. Além da simples incorporação, no entanto, as organizações também devem estar preparadas para agir quanto a esses elementos não financeiros, identificando as informações necessárias para lidar com o risco em diferentes processos de negócios no nível corporativo.

RISCOS NÃO FINANCEIROS
(lista parcial)

- Operacional
- Conformidade
- Estratégico
- de Terceiros
- Cibersegurança
- Responsabilidade social
- Reputacional
- Privacidade dos Dados
- Integridade dos Dados
- Proteção da propriedade intelectual
- Compensação
- Conduta do funcionário
- Gestão do trabalho
- Cultura ética e corporativa
- Saúde pública
- Diversidade, equidade e inclusão
- Direitos humanos
- Recursos humanos
- Ambiental:
  - Emissões de gás de efeito estufa
  - Gestão de resíduos
  - Provisionamento de matéria-prima
  - Acesso/gestão de recursos naturais
  - Mudanças climáticas

[1] Jean-Gregoire Manoukian, "Risk Appetite and Risk Tolerance: What's the Difference?", Wolters Kluwer, 29 de setembro de 2016, https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference#:~:text=Risk%20Appetite%20Is%20the%20General%20Level%20of%20Risk%20You%20Accept&text=Because%20determining%20risk%20appetite%20will,risk%20you%20need%20to%20manage.

Desafios relacionados ao reporte do risco não financeiro

Reporte

Mais de 60% dos CAEs em organizações de capital aberto consideraram os níveis de risco do reporte não financeiros/de sustentabilidade como moderados, altos ou muito altos, de acordo com o *North American Pulse of Internal Audit*[2] De 2023 do The IIA. De fato, muitas empresas estão trabalhando para mensurar e reportar questões de sustentabilidade/não financeiras. Por exemplo, um total de 96% das empresas listadas no S&P 500 e 81% listadas no Russell 1000 publicam relatórios de sustentabilidade.[3]

Um desafio para as organizações nesta área é que muitos riscos não financeiros são difíceis de mensurar. Exemplos incluem inclusão, comportamento ético, cultura corporativa e impacto ambiental das ações da empresa e de seus fornecedores e parceiros de negócios.[4] Uma preocupação relacionada envolve consequências potenciais caso as organizações confiem em indicadores ou frameworks incorretos ou enganosos ao agregar ou reportar informações não financeiras.

Atualmente, não há normas definitivos e globalmente adotadas sobre reportes e divulgações não financeiros, o que pode levar à falta de um reporte consistente e comparável. Em vez disso, as organizações geralmente têm a oportunidade de escolher um conjunto de diretrizes, reunir diferentes diretrizes ou optar por não reportar com base em suas necessidades. Inclusive, o *Center for Sustainable Organizations* compilou uma lista de 23 normas e frameworks de mensuração e reporte não financeiros que abordam uma variedade de diferentes circunscrições, conceitos de desempenho e formatos primários de mensuração.[5]

No entanto, um conjunto de normas de reporte mais geralmente aceitas está no horizonte. Um avanço importante foi a criação do *International Sustainability Standards Board* (ISSB) pela *International Financial Reporting Standards Foundation* (IFRS). Ele consolida a *Value Reporting Foundation* e o *Climate Disclosure Standards Board* existentes e assume a responsabilidade pelo Framework de Reporte Integrado, tudo parte de um esforço para criar uma linha de base global abrangente de divulgação de sustentabilidade para os mercados de capitais. Seu objetivo é atender às demandas por reporte de alta qualidade, transparente, confiável e comparável por parte das empresas, sobre o clima e outros assuntos de ESG. O ISSB anunciou que suas normas iniciais sobre os reportes climático e de sustentabilidade serão emitidos no fim do segundo trimestre de 2023.

Regulatório

De acordo com o *World Business Council for Sustainable Development* (WBCSD), existem atualmente mais de 2.000 requisitos e recursos de reporte de ESG obrigatórios e voluntários em mais de 70 países. Isso por si só cria um desafio assustador para as organizações que tentam entender o reporte não financeiro obrigatório e voluntário e seus riscos relacionados.

A União Europeia (UE) assumiu a liderança na divulgação obrigatória de riscos não financeiros. Desde 2014, a *Non-Financial Reporting Directive* (NFRD) exigia que grandes empresas de interesse público sediadas na UE com mais de 500 funcionários (aproximadamente 11.700) publicassem informações relacionadas a questões ambientais, questões sociais, tratamento de funcionários, respeito pelos direitos humanos, anticorrupção e suborno, e diversidade nos conselhos das empresas (em termos de idade, gênero, escolaridade e experiência profissional), entre outros assuntos.

Em janeiro de 2023, a *Corporate Sustainability Reporting Directive* (CSRD) da UE entrou em vigor. Ela atualiza as regras de reporte social e ambiental da NFRD e amplia o número de empresas obrigadas a reportar (aproximadamente 50.000). As empresas terão de

---

2. *2023 North American Pulse of Internal Audit*, The IIA, 2023, https://www.theiia.org/globalassets/site/content/research/pulse/2023/2023-Pulse-of-Internal-Audit.pdf.
3. *2022 S&P 500 and Russell 1000 Sustainability Reporting in Focus*, Governance & Accountability Institute Inc., 2022, https://www.ga-institute.com/research/ga-research-directory/sustainability-reporting-trends/2022-sustainability-reporting-in-focus.html#:~:text=All%2DTime%20High%20of%20Sustainability,and%2081%25%20of%20Russell%201000.
4. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA, maio de 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.
5. "Non-Financial Measurement & Reporting Standards & Frameworks," Center for Sustainable Organizations, 2023, https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf.

aplicar as novas regras pela primeira vez no exercício de 2024, para a publicação dos relatórios em 2025. Até lá, aplicam-se as regras de reporte da NFRD.[6]

Nos EUA, a *Securities and Exchange Commission* (SEC) propôs exigir que os registrantes incluam divulgações específicas relacionadas ao clima e à cibersegurança em suas declarações de registro e reporte periódico. Espera-se que a SEC anuncie as regras finais dessas duas áreas em 2023. Embora isentas de quaisquer exigências da SEC, as empresas privadas também podem sentir pressão por parte dos stakeholders para fazer divulgações semelhantes.

Greenwashing

Além da falta de comparabilidade e transparência no reporte, a confiabilidade pode se tornar um problema quando as empresas usam suposições excessivamente otimistas ao estabelecer metas ou quando deturpam os dados para apresentar uma imagem mais positiva. Na Europa, as autoridades nacionais de proteção ao consumidor encontraram motivos para acreditar que 42% das alegações de negócios que se posicionavam como ecofriendly eram exageradas, falsas ou enganosas. Essas práticas, conhecidas como greenwashing, podem prejudicar a reputação das organizações. O impacto resultante na satisfação do cliente com uma empresa e seus produtos ou serviços pode influenciar o lucro por ação e o retorno sobre o investimento.[7]

42

PORCENTAGEM DAS ALEGAÇÕES *ECOFRIENDLY* QUE SE ACREDITA SEREM EXAGERADAS, FALSAS OU ENGANOSAS.

Fonte: Harvard Business Review, *"How Greenwashing Affects the Bottom Line"*

Além disso, de acordo com o The IIA, "sem uma estratégia ponderada de gerenciamento de riscos de ESG, construída com base em uma compreensão clara dos problemas, o reporte mal executado de sustentabilidade pode rapidamente entrar em conflito com a conformidade regulatória e desviar-se das expectativas dos investidores".[8]

As empresas que estão lidando com dados não financeiros pela primeira vez terão que desenvolver novos indicadores principais de desempenho e outras métricas, juntamente com políticas, processos e medidas de controle interno apropriados para gerar informações confiáveis para a tomada de decisões e garantir a qualidade dos dados produzidos e reportados.

6. "Corporate Sustainability Reporting," European Commission, acessado em março de 2023, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.
7. Ioannis Ioannou, George Kassinis, and Giorgos Papagiannakis, "How Greenwashing Affects the Bottom Line," 21 de julho de 2022, Harvard Business Review, https://hbr.org/2022/07/how-greenwashing-affects-the-bottom-line.
8. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA, maio de 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

O Papel da Auditoria Interna

Serviços de avaliação e assessoria

Considerando riscos não financeiros no planejamento da auditoria

Os auditores internos planejam suas auditorias com base nos apetites a risco da organização como um todo e das áreas sendo auditadas. A auditoria interna geralmente recebe a responsabilidade de prestar avaliação independente sobre a eficácia do framework de apetite a risco de uma organização. O crescente foco regulatório e dos stakeholders sobre a sustentabilidade e outras questões não financeiras exige que os líderes de auditoria interna considerem os riscos relacionados que podem representar uma ameaça à organização, incluindo entender como se encaixam nas atividades e estratégias da empresa e saber quais departamentos supervisionam as práticas relacionadas. Os líderes de auditoria interna também devem aumentar a conscientização sobre os riscos não financeiros junto aos conselhos e à gestão executiva.

Um papel fundamental para a auditoria interna será determinar um ambiente de controle apropriado para os riscos não financeiros, que permita monitorar métricas relevantes e evitar que a organização reporte informações inválidas e enganosas por conta de controles e sistemas mal projetados. Funções competentes de auditoria interna têm as habilidades e a experiência necessárias para oferecer suporte a ambientes eficazes de controle não financeiro, incluindo treinamento e serviços de assessoria. A auditoria interna pode assessorar sobre frameworks ou normas que a organização pode usar para gerenciar, mitigar e possivelmente reportar riscos não financeiros. A auditoria interna também pode oferecer conselhos sobre as métricas de reporte mais úteis, incluindo novos indicadores criados para capturar dados quantitativos e qualitativos que representem com precisão os riscos não financeiros.

Os dados sugerem que as considerações de sustentabilidade e não financeiras estão lentamente entrando na rotina da auditoria interna. De acordo com o relatório Pulse, 22% dos entrevistados disseram que incorporam considerações de sustentabilidade em suas auditorias em geral. No entanto, auditorias específicas de reporte de sustentabilidade/não financeiro representaram apenas 2% da alocação do plano de auditoria.[9]

O valor de um foco centralizado: a experiência de uma empresa

Definir a base adequada é um fator importante na incorporação de riscos não financeiros ao apetite a risco.

Quando Scott Page ingressou na MDA, Ltd. como diretor de auditoria interna, cada área de negócios tinha seu próprio processo de gerenciamento de riscos, mas a empresa estava interessada em centralizar seu foco. Para alcançar essa centralização, uma abordagem holística e integrada foi fundamental. Para agregar informações, a empresa pública com sede no Canadá, que presta serviços nas áreas de robótica, sistemas de satélites e geointeligência, adotou uma ferramenta de software versátil para o processo de avaliação. A mesma ferramenta pode ser usada por outras equipes, incluindo auditoria interna em testes de controle e TI na avaliação de riscos cibernéticos e de terceiros.

As informações e controles de riscos são, portanto, compartilhados por toda a empresa. A ferramenta reúne detalhes sobre todos os riscos que podem impactar a estratégia ou os objetivos, para ver como podem afetar a capacidade da empresa de cumprir com seus objetivos de curto prazo, bem como seu plano estratégico de longo prazo. “Queríamos reunir todas as considerações de risco em uma única fonte da verdade”, disse Page. “Isso nos ajuda a entender como o que fazemos se relaciona com o que todos os outros fazem.”

9. *2023 North American Pulse of Internal Audit*, The IIA.

Os riscos relacionados a controles internos, demonstrações financeiras, operações, TI e terceiros já foram bem capturados com as abordagens atuais. No entanto, a organização também começou a considerar riscos de ESG e outros riscos não financeiros. Usar a mesma ferramenta para consolidar esses riscos adicionais significa que "você está sempre informado sobre o que está acontecendo em outras áreas", disse Page.

Embora identificar, contabilizar e auditar riscos não financeiros possa ser complicado, o foco centralizado da MDA deu a ela um sólido ponto de partida. Entre outras preocupações, a empresa não quer separar o ESG em um silo, porque os riscos não financeiros relacionados afetam tantas áreas.

A centralização permite o uso de uma linguagem comum, que pode ser compreendida por toda a empresa e pelos stakeholders, disse Page. Ele, junto com os líderes do grupo de gerenciamento de riscos corporativos (ERM), define os riscos e como devem ser avaliados em uma escala de 1 a 5. As informações sobre riscos podem ser coletadas uma vez e aproveitadas por toda a organização, aumentando a eficiência da auditoria interna e de outros departamentos, além de garantir o controle de versão. Usando essa linguagem comum, a gestão executiva e o conselho podem entender facilmente quando a auditoria interna ou outras equipes definem um risco como prioridade máxima — Categoria 5 — em oposição a uma prioridade menos urgente — Categoria 1.

Uma consideração contínua é a auditabilidade de informações não financeiras, porque não há, conforme discutido anteriormente, normas de reporte geralmente adotadas. Até que isso mude, a auditoria interna pode oferecer assessoria sobre para quais controles, processos e informações uma organização precisará estar preparada.

Quantificar os números é outro desafio, porque os dados podem não estar disponíveis e pode ser difícil obter dados comparáveis. A MDA, por exemplo, não tem tanto envolvimento nas emissões de gases de efeito estufa, uma preocupação comum de ESG. No entanto, ela trabalha com muitos fornecedores e consultores externos, e esses terceiros podem estar gerando emissões ou tomando outras medidas que a MDA precisará considerar. Ao desenvolver os pilares de seu programa de riscos não financeiros, a MDA está identificando esses terceiros, considerando como mensurar quaisquer riscos relacionados, decidindo a melhor forma de auditá-los e, em seguida, desenvolvendo uma compreensão mais ampla do que riscos de terceiros e outros riscos não financeiros significam para a empresa.

De acordo com a pesquisa Pulse do The IIA, os relacionamentos com terceiros são a terceira área de maior risco (depois da cibersegurança e TI), e a frequência de auditoria de relacionamentos com terceiros é relativamente baixa em comparação com o nível de risco.

Embora a MDA esteja nos estágios iniciais de identificação das áreas de possíveis riscos não financeiros, o processo até agora destacou o impacto que elas poderiam ter na capacidade da empresa de atingir suas estratégias, bem como na percepção do público sobre a empresa. O processo também fornecerá mais informações para a tomada de decisões da gestão executiva e do público, disse Page. "Temos uma compreensão mais ampla dos riscos financeiros e não financeiros, e de como precisamos controlá-los", afirmou.

Envolvimento desde o início

Os auditores internos devem alertar a gestão e os conselhos sobre o valor de envolver a auditoria interna desde o início, especialmente ao lidar com um novo conceito, como o risco não financeiro. "Se a auditoria interna estiver envolvida desde o início, há uma chance maior de sucesso no futuro", disse Page. "Por que uma empresa deveria lançar seus planos ou processos de ESG ou não financeiros, e a auditoria interna vir mais tarde e apontar todos os problemas quando já estiverem em vigor?"

Para manter a independência, a auditoria interna não pode tomar decisões para uma empresa, mas pode oferecer insights sobre a melhor forma de começar a considerar os riscos não financeiros e quais abordagens podem ou não funcionar. "Podemos ser um parceiro de negócios de valor agregado", disse ele.

Page descobriu que fazer contatos em toda a organização é uma boa maneira de entender melhor as áreas que sua equipe auditará. Page entra em contato regularmente com pessoas envolvidas em importantes funções de negócios e pede uma reunião de 15 minutos

durante um café – e ele incentiva sua equipe a fazer o mesmo. “Nunca alguém disse 'não'”, disse ele. “Todos são apaixonados e amam o que fazem.”

“O que me preocupa como chefe de auditoria é: o que eu não sei?” acrescentou Page. “A única forma de descobrir é conversando com as pessoas.” As auditorias de sua equipe incluem conversas com funcionários da área que está sendo auditada. Ele também se mantém atualizado sobre o trabalho da equipe corporativa de ERM, embora a auditoria interna tenha seu próprio processo independente de avaliação de riscos.

O networking com seus colegas da indústria ou comitês profissionais também ajuda a determinar se sua abordagem de gerenciamento de riscos está atualizada e se é tão completa quanto possível. Esse conhecimento prévio será especialmente importante para informações não financeiras ou de ESG, conforme esses riscos continuam evoluindo.

Page e sua equipe obtêm com maior compreensão de suas conversas e, portanto, estão mais bem-posicionados na hora de auditar uma área, algo que será especialmente útil para entender a nova fronteira de dados não financeiros. A MDA abrange três áreas de negócios separadas, de modo que a auditoria interna também pode compartilhar práticas bem-sucedidas usadas por outras equipes e detectar qualquer duplicação desnecessária de esforços. “O tino comercial leva a um sucesso muito maior”, disse Page. Os auditores internos também podem agregar valor questionando o status quo, questionando as práticas existentes e desenvolvendo diretrizes para permitir uma melhor compreensão e identificação das informações não financeiras.

Orientação Prática do *Risk in Focus* de 2023

O *Risk in Focus* de 2023, o mais recente relatório anual sobre riscos produzido pelos membros da *European Confederation of Institutes of Internal Auditing* (ECIIA), abordou diversas áreas de risco não financeiro, incluindo riscos macroeconômicos e geopolíticos. Os participantes de uma mesa redonda de líderes de auditoria interna abordaram a reavaliação do risco global, especialmente porque o conflito na Ucrânia impactou os riscos em várias áreas, incluindo a estabilidade dos sistemas globais de energia. Um participante da mesa redonda, Ken Marnoch, vice-presidente executivo de auditoria interna e investigações da Shell International, disse que ele e sua equipe estão envolvidos em “conversas mais fortes sobre o apetite a risco”.

Segundo o *Risk in Focus* de 2023:

> “[Marnoch] diz que ter uma compreensão clara de quanto risco cada negócio pode assumir em áreas específicas é mais útil durante um dilema – onde todas as escolhas podem ter vantagens e desvantagens potenciais. Então, a clareza sobre o apetite aos riscos associados às diferentes escolhas pode atuar como um farol na resolução de um problema.
>
> Historicamente, a auditoria interna da Shell concentrou-se em riscos operacionais, culturais e baseados em conduta. O grupo de auditoria interna já constituiu uma equipe específica para enfocar os riscos e o framework de controle associados ao atingimento dos objetivos estratégicos.
>
> ‘Se você dividir os objetivos estratégicos em metas mensuráveis, os riscos relacionados, os controles explícitos e uma compreensão de como os líderes de negócios sabem que os controles estão funcionando, você terá o escopo de uma auditoria interna’, diz ele. ‘Parte do papel da nova equipe é ajudar as pessoas a se afastarem da mentalidade engessada sobre a exatidão das suposições que fizeram no início de um projeto ou estratégia, quando tanto no mundo está mudando dramaticamente. Ser ativamente questionador, encontrar informações que testem as crenças e ter feedback rápido sobre a realidade atual são requisitos para navegar um futuro incerto.’

> ‘Se você abrir mão da necessidade de estar certo e reconhecer que foi uma decisão tomada com as melhores informações do momento, estará mais aberto a buscar informações que desafiem sua mentalidade. Isso abre muito mais poder no gerenciamento de um risco importante para o atingimento de seus objetivos estratégicos.’”[10]

O *Risk in Focus* de 2023 inclui uma lista de perguntas que a auditoria interna pode usar na avaliação do risco organizacional:

1. Em termos de tempo e esforço dedicados a atribuições de auditoria interna, como a auditoria interna está alinhada aos objetivos estratégicos da organização — incluindo aqueles que envolvem riscos geopolíticos e mudanças climáticas?
2. Quão forte é o suporte a atividades de auditoria interna em áreas como estratégia e gestão de crises, e o que pode ser feito para melhorar esse suporte onde ele estiver faltando?
3. Até que ponto a auditoria interna é capaz de alavancar recursos de outras linhas para fornecer cobertura adequada e minimizar a duplicação de esforços?
4. Como você sabe se as suposições que a organização (e a função de auditoria interna) fizeram sobre a natureza das principais áreas de risco ainda são válidas hoje e se encaixam nas circunstâncias que provavelmente surgirão em 2023?
5. A organização tem avaliações de riscos atualizadas do risco de sanções, e tem controles robustos para a triagem de propriedade de terceiros e acionistas da empresa?
6. Até que ponto a organização aproveita ferramentas digitais para modelar principais riscos e executar cenários “e se”?
7. Você reavaliou o relacionamento entre as equipes de continuidade de negócios, gestão de crises e gerenciamento de riscos da organização, para garantir que sejam adequadas ao propósito?
8. A organização considera seriamente vozes críticas e de especialistas externos em sua avaliação de riscos?

[10] *Risk in Focus 2023: More Risky, Uncertain, and Volatile Times Ahead,* European Confederation of Institutes of Internal Auditing, 2022, https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/.

Conclusão

Um Entendimento Abrangente

É importante entender que os riscos não financeiros podem ter um impacto financeiro significativo em uma organização, inclusive sobre seus esforços de ERM. Para ajudar a liderança a entender e lidar com os riscos não financeiros, os líderes de auditoria interna podem usar seu entendimento abrangente das diversas facetas da entidade — e ameaças a ela — para fornecer informações valiosas sobre esses riscos, bem como para contabilizá-los e abordá-los devidamente ao ajudar a determinar o apetite a risco da organização.

Parte 2: Quantificando o Risco Não Financeiro

Sobre os Especialistas

Anishka Collie, CIA, CPA

Anishka Collie, CIA, CPA, é CEO e principal consultora da ATC Financial Advisors & Consultants, em Nassau, nas Bahamas. Ela tem mais de 20 anos de experiência em auditoria externa, auditoria interna e governança corporativa, gerenciamento de riscos corporativos e controles internos, bem como em planejamento financeiro, consultoria, remediação de processos financeiros e revisões de processos de negócios. Tem foco em clientes da indústria de serviços financeiros e já palestrou em diversos seminários de treinamento em contabilidade e auditoria.

Hassan NK Khayal, CIA, MBA, CRMA, CFE

Hassan NK Khayal, CIA, MBA, CRMA, CFE, é gerente de auditoria interna da Scope Investment em Dubai. Foi apresentado como um dos 15 melhores líderes globais emergentes com menos de 30 anos como uma estrela promissora da profissão de auditoria interna na Internal Auditor, uma publicação global do The Institute of Internal Auditors. Está concluindo seu doutorado em administração de empresas na Universidade Católica de Murcia, Espanha. Além de seus diplomas e certificações profissionais, também possui certificações profissionais em automação robótica de processos, gestão da qualidade, saúde e segurança, gestão ambiental e gerenciamento de riscos.

Jason Minard, CIA, CISA, CPA (inativo)

Jason Minard, CIA, CISA, CPA (inativo), é vice-presidente sênior e gerente sênior de controles e análises de supervisão da Wells Fargo Advisors, em St. Louis, Missouri, EUA. Com mais de 25 anos de experiência na indústria de valores mobiliários e auditoria, executou e gerenciou auditorias em áreas como vendas de investimentos, conformidade regulatória, operações com valores mobiliários, investment banking, gestão de ativos, administração fiduciária e finanças. É bacharel em administração de empresas pela St. Louis University e possui licenças de representante geral de valores mobiliários e supervisor geral de vendas.

Introdução

O guru da administração, Peter Drucker, é frequentemente citado como tendo dito: "[apenas] o que é mensurado é gerenciado". De fato, as empresas há muito entenderam a importância de quantificar e mensurar os riscos financeiros. A novidade nos últimos anos tem sido o crescente interesse nos riscos não financeiros, incluindo ambiental, social e governança (ESG) e considerações regulatórias e de reporte relacionadas. O desafio tem sido como mensurar algo que muitas vezes não tem valor monetário facilmente identificado. É algo que as organizações devem superar, porque os riscos não financeiros podem definitivamente ter impacto financeiro.

Este *Brief* de Conhecimento Global, o segundo de uma série de três partes sobre governança, riscos e controle (GRC), examina os desafios de quantificar riscos não financeiros e como as empresas os estão abordando, bem como o importante papel que a auditoria interna pode desempenhar no avanço da compreensão nesta área.

Entendendo os Riscos Não Financeiros

Uma miríade de potenciais ameaças

Aprendendo a reconhecer e mensurar

Como regra geral, os riscos não financeiros são aqueles que surgem do impacto de uma organização no mundo e, inversamente, do impacto do mundo na organização. Uma lista parcial (veja a caixa ao lado) reflete muitos, mas não toda a ampla gama de riscos não financeiros que as organizações podem enfrentar. As definições desses riscos geralmente são inconsistentes ou pouco claras, tornando o reconhecimento e a mensuração mais desafiadores.

No entanto, riscos não financeiros também existem em transações financeiras simples. Por exemplo, ao considerar o risco de crédito em um empréstimo de US$ 50.000, o valor do empréstimo e a perda inicial potencial são claros. Por outro lado, o risco não financeiro desta transação inclui considerações como o tempo e o esforço gastos para lidar com uma possível inadimplência do empréstimo, observou Anishka Collie, CIA, CPA, CEO e principal consultora da ATC Financial Advisors & Consultants, Nassau, nas Bahamas, que presta serviços terceirizados de assessoria em riscos e auditoria interna. Se o empréstimo for significativo ou fizer parte de um padrão de créditos malparados, a organização também pode ter que se aprofundar para entender se a cultura corporativa, a documentação e os controles internos disponíveis ou o nível de treinamento atual são adequados para mitigar o risco de crédito e garantir boas decisões de empréstimo.

Como os riscos não financeiros podem ser difíceis de quantificar, um risco relacionado é a possibilidade de que o reporte e a divulgação de riscos não financeiros de uma organização não sejam confiáveis. Por exemplo, o atingimento de certas metas de sustentabilidade pode ser visto como intencionalmente inflado ou os problemas para atingir essas metas podem ser subestimados, uma prática conhecida como *greenwashing* quando relacionada a questões de ESG. O *greenwashing* pode ser intencional ou simplesmente ocorrer devido aos níveis relativamente baixos de maturidade atualmente disponíveis nas normas de reporte não financeiro, observou um chefe executivo de auditoria em uma mesa redonda realizada pela *European Confederation of Institutes of Internal Auditing* (ECIIA).[11] No momento, o reporte pode ser inconsistente ou difícil de comparar, porque não há normas adotadas globalmente sobre reporte e divulgação não financeiros. Existem também vários frameworks ou normas disponíveis, tornando potencialmente difícil que as empresas determinem quais diretrizes seguir e como aplicá-las, especialmente porque muitas vezes podem ser usadas em parte ou em combinação com regras de outra norma ou framework. O *Center for Sustainable Organizations* compilou uma lista de 23 normas e frameworks de mensuração e reporte não financeiro baseados em diversas métricas de desempenho diferentes e destinadas a diferentes tipos de organizações.[12]

RISCOS NÃO FINANCEIROS
(lista parcial)

- Operacional
- Conformidade
- Estratégico
- de Terceiros
- Cibersegurança
- Responsabilidade social
- Reputacional
- Privacidade dos Dados
- Integridade dos Dados
- Proteção da propriedade intelectual
- Compensação
- Conduta do funcionário
- Gestão do trabalho
- Cultura ética e corporativa
- Saúde pública
- Diversidade, equidade e inclusão
- Direitos humanos
- Recursos humanos
- Ambiental:
  - Emissões de gás de efeito estufa
  - Gestão de resíduos
  - Provisionamento de matéria-prima
  - Acesso/gestão de recursos naturais
  - Mudanças climáticas

[11] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.
[12] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf

Preparando o Palco

As organizações devem ser proativas ao considerar como quantificar o risco não financeiro, mas muitas não são. Lidar com o risco financeiro está relacionado ao principal objetivo de uma organização – maximizar a riqueza dos acionistas e aumentar as receitas. Ao lidar com riscos não financeiros, as organizações são solicitadas a gastar dinheiro com esforços cujo valor pode ser difícil de entender e que não aumentam imediatamente a receita. "Até que você possa quantificar e colocar um valor financeiro no impacto do risco, é improvável que você garanta o apoio necessário da gestão para lidar com isso", de acordo com a PwC.[13]

Outro obstáculo é que as funções de controle para riscos não financeiros podem ser isoladas pela organização afora. Como esses riscos são tão diversos, muitas vezes estão sob a supervisão de uma ampla gama de equipes. Cada equipe pode ter seu próprio processo de identificação de riscos, estrutura de reporte e até sistemas de TI diferentes relacionados a riscos não financeiros. "Os mesmos indivíduos, seja auditoria interna, conformidade ou alguma outra área, recebem pedidos para realizar o mesmo procedimento repetidamente", disse Hassan NK Khayal, CIA, MBA, CRMA, CFE, gerente de auditoria interna da Scope Investment em Dubai. A despesa adicional dessa duplicação de esforços torna mais provável que a gestão adie os investimentos na coleta de informações e nos esforços de quantificação.

No entanto, tomar medidas preventivas reduz os custos de remediação e protege a marca da empresa e suas relações comerciais. Na maioria das organizações, os métodos de reporte de risco ainda não são sofisticados ou precisos o suficiente para apresentar um argumento convincente à gestão, disse Khayal. Mas, se escolhidos devidamente, os indicadores certos podem capturar e quantificar com precisão os riscos não financeiros e fornecer o contexto adequado para que a gestão compreenda seus possíveis impactos.

A identificação proativa de possíveis ameaças não financeiras antes que elas aconteçam torna mais fácil entendê-las e quantificá-las. Por exemplo, na indústria de alimentos e bebidas, é fácil quantificar o risco financeiro quando uma certa quantidade de comida estraga. No entanto, calcular os custos e riscos relacionados à saúde e segurança é mais difícil, observou Khayal. Ao considerar esses riscos, uma organização pode tomar medidas proativas e preparatórias, como melhorar a limpeza para tornar um restaurante mais atraente e menos propenso a causar doenças ao cliente. Da mesma forma, na indústria da construção, quando os engenheiros de segurança são mais rigorosos no monitoramento e na aplicação das regras de saúde e segurança, o número de acidentes normalmente cai.

"Cada incidente vem com seu próprio custo associado", disse Khayal, seja o custo direto de lidar com o evento e com quaisquer lesões relacionadas, ou a despesa de atrasos associados. "No momento em que o risco ocorreu, já é tarde demais", observou ele, e o dano à reputação e aos relacionamentos da organização já foi feito, talvez com impacto duradouro ou significativo. Mas, quando as organizações avaliam os custos de eventos de risco potenciais, é mais provável que vejam o valor de tomar medidas preventivas.

Khayal acredita que os riscos não financeiros podem ter efeitos maiores do que os financeiros. Seu impacto pode levar stakeholders, como acionistas, funcionários e clientes, a questionar o modelo de negócios ou as práticas de uma empresa quando ocorrem danos à reputação. "Tudo isso coloca uma pressão considerável sobre as organizações para gerenciar riscos não financeiros", disse ele.

Trabalhando em Busca da Quantificação

Embora os riscos não financeiros não tenham valores monetários diretos, é possível atribuir-lhes valores numéricos. A chave é definir os riscos e o que eles abrangem e, em seguida, encontrar considerações tangíveis para mensurar. Ao abordar o risco do cliente, por

[13] "Taking Control: How to Get on top of Non-Financial Risks," Christopher Eaton e David O'Brien, PwC Channel Islands, 9 de março de 2021.

exemplo, é possível determinar fatores como o número de reclamações de clientes, os locais ou situações relacionadas, perdas de clientes associadas, declínios no número de novos clientes e quais tendências esses dados revelam ao longo do tempo.

Quando não há critérios tangíveis para mensurar, uma opção é categorizar os riscos da forma mais descritiva e significativa possível, como se estão em níveis alto, médio ou baixo. Por exemplo, quando há um risco regulatório e de conformidade, as organizações podem tentar quantificar o risco, determinando a gama de possíveis constatações de um regulador em cada categoria de risco. Categorizar as constatações dessa forma dá às empresas um framework para avaliar melhor cada risco e definir prioridades.

Um framework organizado de classificação é outra opção que permite capturar constatações sobre uma variedade de riscos não financeiros. As equipes de auditoria interna podem usar um framework de classificação que classifique as observações feitas pela auditoria interna e quaisquer outras equipes, como conformidade, riscos, segurança da informação ou jurídico, que identifique riscos não mitigados e os rastreie, reporte ou corrija. O framework pode ser usado para avaliar o impacto de riscos não financeiros e apoiar sua quantificação. Um exemplo do tipo de framework que as empresas podem usar para entender e comunicar melhor o impacto financeiro de suas medidas de sustentabilidade é o Pacto Global das Nações Unidas e o *Value Driver Model* dos Princípios para Investimento Responsável.

O Papel da Auditoria Interna

“Pioneiros” do Risco Não Financeiro

Mantendo o Foco no Futuro e Monitorando os Controles

Conforme as empresas trabalham para abordar a quantificação, o papel da auditoria interna é ser estratégico e focar nas melhores formas de agregar valor, conforme descrito no Modelo das Três Linhas do The IIA (consulte a Figura 1). Para atingir esse objetivo, os auditores internos não devem se limitar a analisar declarações e riscos financeiros, mas devem ser os pioneiros na abordagem de riscos não financeiros, seguindo uma abordagem baseada em riscos e sempre considerando o futuro, disse Khayal. “Idealmente, deveríamos ser um dos departamentos da organização mais voltados para o futuro”, disse. “Devemos nos concentrar nos riscos futuros antes que a gestão, de olho nos impactos do dia a dia, esteja ciente deles.” Para manter a independência, a auditoria interna não define as categorias ou definições de riscos que a organização usa, mas questiona as políticas de risco não financeiro e como elas são implantadas de acordo com o processo geral de avaliação de riscos.

Figura 1: Modelo das Três Linhas

Como consultora, o papel de Collie é muito parecido com o de um auditor interno e é aquele que os auditores podem seguir quando se trata de riscos não financeiros. No início, ela fala com os líderes da organização, incluindo não apenas o CEO e o CFO, mas também os chefes de *compliance*, risco e auditoria interna. O objetivo é entender as definições de riscos da organização, como eles identificam os riscos, em que nível de detalhe e quais controles estão em vigor. Durante essas discussões, os participantes geralmente chegam a uma nova compreensão do risco e de seu impacto, disse Collie.

Essas conversas iniciais são de alto nível, para entender o que é necessário para que a organização opere de forma eficaz. O próximo passo é conversar com gerentes ou chefes de departamentos, para saber mais sobre o dia a dia das operações e onde podem ocorrer riscos. Com esse entendimento, o auditor pode fazer um brainstorming com os funcionários desse nível, para saber quais etapas de gerenciamento de riscos já foram bem-sucedidas ou falharam, e onde existem deficiências de gerenciamento de riscos. Assim como

os consultores podem oferecer experiência em diversas organizações, os auditores internos têm um conhecimento holístico de muitas áreas da organização. "Você pode trazer coisas à tona nas quais essas equipes podem não ter pensado", disse Collie.

Os auditores precisarão de novas habilidades para facilitar o processo. As abordagens tradicionais de auditoria interna envolvem a identificação de riscos relacionados a controles, dados e documentos. Trabalhar com clientes para identificar e compreender os riscos não financeiros requer habilidades adicionais e treinamento contínuo relacionado a entrevistas ou requer facilitar uma sessão de brainstorming, disse Collie. "Na verdade, ajudar os clientes a percorrerem o processo de identificação de riscos é um exercício completamente diferente", disse ela. A liderança terá que investir nessa educação, para garantir que a organização esteja atuando de forma eficaz e eficiente.

A auditoria interna também pode avaliar o valor e a confiabilidade dos principais indicadores e métricas de desempenho existentes quando aplicados a riscos não financeiros, bem como novas métricas desenvolvidas especificamente para riscos não financeiros e controles relacionados e processos de gerenciamento de riscos. Para evitar acusações de *greenwashing*, podem garantir que os dados compartilhados com os stakeholders mostrem uma imagem justa e precisa dos esforços corporativos, de acordo com o ECIIA.[14]

Khayal constrói seu plano de auditoria e avaliação de riscos em torno dos muitos elementos de riscos que podem afetar a capacidade de uma organização de alcançar a estratégia, tanto financeira quanto não financeira. Por exemplo, se a estratégia organizacional e a criação de valor dependerem de práticas rigorosas da cadeia de suprimentos, a aquisição sempre será uma preocupação fundamental, disse ele. O mapeamento de riscos, principalmente riscos não financeiros, pode revelar ameaças como problemas de credibilidade do cliente, problemas na cadeia de suprimentos e desafios de cibersegurança.

Conforme as organizações desenvolvem seus frameworks e refinam as definições que usam, elas criam uma linguagem comum sobre os riscos não financeiros. Isso melhora a comunicação sobre riscos entre a primeira, segunda e terceira linhas; esclarece as responsabilidades de cada linha; e permite que cada uma adicione seus próprios refinamentos às definições compartilhadas.

Responsabilidades Voltadas para o Futuro

Na organização de Khayal, qualquer pessoa envolvida em controles e autoavaliação de riscos deve fazer um curso detalhado de treinamento de riscos que inclua riscos não financeiros. Ele também incentiva sua equipe a se concentrar em três tarefas principais:

- **Mantenha-se atualizado**. Os auditores internos devem se manter informados sobre os últimos eventos mundiais e locais, para obter uma melhor compreensão dos incidentes que podem ter impacto sobre o risco agora ou no curto ou longo prazo.
- **Mantenha-se atualizado sobre as tecnologias emergentes.** Khayal acredita que os auditores do futuro e as organizações para as quais trabalham devem ser experientes em TI. Os auditores não podem mais confiar apenas nos métodos tradicionais, mas devem incorporar ferramentas tecnológicas. "O mundo está mudando em um ritmo mais rápido", disse. Sem uma tecnologia robusta, "as organizações não conseguirão acompanhar, especialmente porque, cada vez mais, os fatores macroeconômicos que enfrentamos não são financeiros".
- **Permanecer em sintonia com a estratégia, missão e visão da organização.** Os planos de auditoria devem considerar quais riscos são mais importantes e qual a melhor forma de quantificá-los. Como as organizações geralmente não conseguem lidar com todos os tipos de riscos que podem enfrentar, os auditores devem considerar vários fatores, para identificar e tentar quantificar os riscos que provavelmente terão maior importância e impacto.

[14] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

Conclusão

Como conselheiros de confiança da organização, os auditores internos estão em uma posição única para promover maior compreensão e reconhecimento dos riscos não financeiros. Eles podem fazê-lo alavancando seu conhecimento abrangente do negócio, acrescentando novas competências e defendendo uma mudança na perspectiva organizacional que determina a melhor forma de quantificar o risco não financeiro.

Parte 3: Como a Transformação Digital Está Transformando o GRC

Sobre as Especialistas

Sarah Kuhn, CIA, CCSA, CRMA

Sarah Kuhn é uma profissional altamente experiente na área de auditoria interna. Com mais de 20 anos como membro do The Institute of Internal Auditors (IIA) e uma presidência anterior da filial de Tulsa, demonstrou seu compromisso com a indústria, com experiência em treinamento de departamento, reporte e conformidade com normas, além de liderar uma auditoria equipe focada em análise de dados e automação. Sarah também faz parte da equipe atual da filial de Houston do IIA.

Audra Nariunaite, CIA, CISA, CFE, CHC, CHPC

Audra Nariunaite é uma profissional de conformidade e auditoria, com experiência em múltiplas indústrias e com capacidade comprovada de impulsionar o crescimento e a excelência, por meio de iniciativas estratégicas e reengenharia de processos. Atualmente, faz parte do conselho de administração da filial do Nordeste da Flórida do IIA e é membro do IIA–Lituânia. Audra é atualmente diretora de *compliance* na plataforma global de empregos Oyster HR.

Introdução

Indiscutivelmente, nenhuma tendência está afetando o cenário de governança, riscos e conformidade (GRC) de forma mais significativa do que o surgimento das tecnologias nas operações comerciais diárias — e é fácil entender por quê. Os benefícios da transformação digital não podem ser subestimados, e as ferramentas que surgem a partir dessa tendência agora são usadas em quase todas as principais indústrias para automatizar e acelerar processos, permitindo que as operações de GRC e de segurança identifiquem e respondam rapidamente a possíveis riscos e problemas.

Por exemplo, com sua capacidade de analisar fontes de dados não estruturadas, desde e-mails a feeds de redes sociais, o processamento de linguagem natural auxiliado pela IA pode ser combinado com as habilidades e a experiência de equipes humanas de GRC, para fornecer recursos de gerenciamento de riscos e conformidade em um nível de sofisticação e complexidade que não poderia ter sido compreendido na geração passada.

Embora a necessidade de passar por uma transformação digital tão radical poderia ter sido considerada um luxo, o cenário de risco atual oferece às organizações pouco espaço para adiar essa adoção. As ameaças cibernéticas estão se intensificando em volume e sofisticação a cada dia; o volume bruto de dados sendo produzidos, coletados e processados continua a crescer em um ritmo impressionante, criando riscos cada vez maiores à privacidade dos dados; e o cenário regulatório continua evoluindo rapidamente, para acompanhar a velocidade dos riscos atuais. De fato, sem as vantagens que a transformação digital oferece, as funções de GRC no mundo de hoje poderiam estar perdidas.

Como Parte 3 da série do *Brief* de Conhecimento Global do The IIA sobre GRC, esta parte final aborda como os sistemas de GRC estão evoluindo a partir da incorporação de novas tecnologias, bem como quais riscos inerentes estão envolvidos na adoção da transformação digital. Este resumo também aborda onde a auditoria interna se encaixa nessa conversa e como ela pode ajudar melhor as organizações, conforme continuam nessa jornada crítica.

A Conversa sobre a Transformação Digital de 2023

Entendendo um risco carregado

O alcance da transformação digital

A explosão da transformação digital observada durante a pandemia do COVID-19 continua forte e, de certa forma, sua evolução está ganhando velocidade. Isso ocorreu não apenas por causa de um desejo básico de aumentar lucros e eficiências para obter uma vantagem competitiva no mercado, mas também por causa de um esforço para manter o ritmo (ou, idealmente, ficar à frente) da extensa lista de riscos emergentes que se materializaram nos últimos anos. Inflação, tensões geopolíticas como o conflito na Ucrânia, a disputa China-Taiwan, incerteza econômica generalizada resultante de eventos como o fechamento repentino de várias instituições bancárias de grande porte, discussões em andamento relacionadas a riscos de ESG e mudanças relacionadas no cenário regulatório, disrupções e escassez na cadeia de suprimentos — essas são apenas algumas das formas que o risco assumiu em 2023. Da perspectiva das organizações encarregadas de manter alguma forma de avaliação contra eles, uma adoção em larga escala da transformação digital é vista como uma solução eficaz. De fato, de acordo com um relatório recente da Gartner, 89% dos diretores do conselho dizem que os negócios digitais agora estão incorporados em todas as estratégias de crescimento de negócios, mesmo que apenas 35% digam que alcançaram ou estão no caminho certo para alcançar as metas de transformação digital.

"Os conselhos de administração chegaram a um ponto em que a estratégia de negócios digitais e a estratégia geral de negócios são a mesma coisa", disse Jorge Lopez, vice-presidente e analista distinto da Gartner, no relatório. "Embora os CIOs tenham feito progressos significativos ao alavancar a tecnologia para a excelência operacional, isso não é suficiente para obter os benefícios estratégicos de negócios que [os conselhos de administração] buscam nos investimentos digitais".[15]

A aparência da transformação digital varia entre diferentes locais, indústrias e organizações. O que é eficaz, ou mesmo alcançável, para uma organização pode não ser ideal para outra. Apesar disso, há algumas semelhanças fundamentais entre as organizações que adotam alguma forma de transformação digital. "[A transformação digital] é mais do que apenas tecnologia", disse Chintan Shah, CEO e fundador da Brainvire, escrevendo para a Forbes. "[É] sobre a mudança de mentalidade que permite que as organizações reinventem seus modelos e processos de negócios para aproveitar as oportunidades criadas pelas tecnologias emergentes."[16]

Lopez expressou um sentimento semelhante. "Conforme as empresas operam cada vez mais em um mundo de disrupção constante, os conselhos mais experientes estão considerando como as reviravoltas e riscos podem servir como fonte de oportunidades. Os CEOs e CIOs precisarão adotar essa mentalidade, pois a tecnologia desempenha um papel cada vez maior em promover o sucesso dos negócios".

Essa reimaginação pode assumir várias formas, incluindo, mas não se limitando a:

- Inteligência artificial (IA), aprendizado de máquina e adoção de processamento de linguagem natural.

15. "Gartner Says 89% of Board Directors Say Digital Is Embedded in All Business Growth Strategies," *release* de imprensa, Gartner, 29 de outubro de 2022, https://www.gartner.com/en/newsroom/press-releases/2022-10-19-gartner-says-89-percent-of-board-directors-say-digital-is-embedded-in-all-business-growth-strategies.

16. Chintan Shah, "Businesses Need to Watch these Digital Transformation Trends in 2023," Forbes, 27 de janeiro de 2023, https://www.forbes.com/sites/forbestechcouncil/2023/01/27/businesses-need-to-watch-these-digital-transformation-trends-in-2023/?sh=7147b04a185d.

- Automação robótica de processos *(robotic process automation* – RPA).
- Foco em cibersegurança e privacidade de dados.
- Migração para a nuvem.
- Análise de dados.
- Adoção do 5G e otimização digital.
- *Blockchain.*
- Colaboração comercial virtual.
- Plataformas de dados do consumidor.

O efeito da transformação digital sobre o GRC

Claramente, com tantas conotações e aplicações, a transformação digital teve um efeito profundo nas funções de GRC e, em muitos casos, as organizações têm lutado para manter níveis adequados de cobertura de GRC, conforme as mudanças no cenário tecnológico mantêm um ritmo acelerado. Uma pesquisa recente da Risk.net em colaboração com a IBM, com profissionais de GRC no setor de serviços financeiros, revelou algumas tendências alarmantes, incluindo:

- 62% acreditam que sua transformação digital expôs lacunas nos processos existentes de GRC, e quase metade dos entrevistados (45%) acha que suas organizações agora estão "tentando recuperar o atraso". Apenas 37% disseram ter investido tempo e recursos em sua transformação digital antes da mudança.
- 77% acreditam que os riscos de suas empresas aumentaram, conforme ficaram mais dependentes de canais digitais.[17]

Além disso, no mesmo estudo, quando questionados sobre quais riscos assumiram maior destaque em sua organização como resultado das tendências de transformação digital, 56% identificaram a segurança da informação/dados, 48% disseram violações de cibersegurança, 32% disseram risco de terceiros/cadeia de suprimentos, e 31% disseram risco de conformidade.

Para permanecerem eficazes, as funções de GRC tiveram que se modernizar, aplicando medidas definitivas para adotar a transformação digital, ou arriscariam sujeitar suas organizações a riscos significativos. Tais etapas incluem:

- Alocar ou recrutar novos recursos.
- Adotar alguma forma de modelo de armazenamento de dados em nuvem híbrida, para usos aprimorados de análise de dados.
- Upgrade das ferramentas e capacidades atuais de GRC.
- Implantação de tecnologia avançada, incluindo ferramentas relacionadas à IA e sistemas de automação.

Embora algumas dessas ações possam parecer um tanto óbvias, a velocidade com que o atual cenário de risco está evoluindo as torna tudo menos óbvias. Por exemplo, historicamente, as organizações confiaram na conformidade com uma orientação específica ou um framework de normas, certificações e/ou regulamentos para estabelecer uma base de controles e processos comprovados que preparam uma função de GRC para o sucesso.

Hoje, no entanto, tal abordagem pode se tornar complexa rapidamente. Isso pode ser devido a:

- O rápido desenvolvimento de frameworks novos ou atualizados, que exigem pronta conformidade. Os exemplos incluem a rápida criação de uma variedade de iniciativas regulatórias propostas na UE relacionadas à estratégia digital, incluindo as leis *Data*

[17] "Digital Transformation and the Future of GRC," Risk.net, IBM, fevereiro de 2022, https://www.ibm.com/downloads/cas/WWQXRPLG.

Conformance Act, Digital Markets Act, Digital Services Act, Data Act e *AI Act*, cujas aprovações são esperadas até o fim de 2023; ou

- A falta de clareza ou orientação dos frameworks atuais, que faz com que as organizações — pelo menos por um tempo — encontrem seu rumo por conta própria.

"Com sistemas como ChatGPT e Bing Chat sendo lançados e a preparação atual para o lançamento do CoPilot, muitas organizações precisam agir rapidamente, porque os funcionários já estão usando algumas dessas tecnologias para concluir tarefas", disse Sarah Kuhn, líder de auditoria interna com mais de duas décadas de experiência e serviço na profissão. "Há algumas organizações que irão bloqueá-los totalmente, enquanto outras, com equipes mais equipadas para entender as tecnologias, criarão internamente diretrizes mais detalhadas sobre como e quando devem ser usadas."

As equipes encarregadas de desenvolver estratégias para criar essas diretrizes variam em composição com base na organização, mas podem incluir partes como os diretores digital e de informação, equipes de TI e gerenciamento de riscos, grupos jurídicos e financeiros. Uma vez criadas, no entanto, as estratégias para comunicar e fazer cumprir as diretrizes são igualmente críticas. "As empresas podem operar com base na honestidade até certo ponto", disse Kuhn, "mas também são necessárias medidas mais formais para comunicar as diretrizes em evolução. Por exemplo, quando um funcionário digita um determinado endereço, existe um programa que pode ser implantado que fará com que um banner apareça em seu navegador, lembrando-o das diretrizes da empresa."

Para realizar isso de forma tão perfeita, Kuhn observou que uma função ágil e adaptável de GRC precisaria estar em vigor antes que tecnologias emergentes, como o ChatGPT, entrassem no cenário de riscos da organização. Nem toda organização terá a bênção de tal visão de futuro, seja devido a recursos restritos, dados disponíveis limitados ou de baixa qualidade, priorização de outras questões ou simples negligência. Independentemente das razões, a auditoria interna precisa estar preparada para tomar a iniciativa de colocar rapidamente as funções de GRC em uma posição adequada para ter sucesso nesta nova era.

Auditoria Interna na Discussão de GRC

Melhorando o GRC no contexto da transformação digital

Mantendo um lugar à mesa

A auditoria interna pode apoiar o GRC eficaz de várias maneiras importantes, especialmente em organizações que são consideradas atrasadas em seus objetivos de atualizar as funções de GRC.

Primeiramente, poucas mudanças que valem a pena buscar podem ser realizadas sem um certo grau de investimento. Esses investimentos, no entanto, podem ser difíceis sem o apoio de todos os níveis — desde o topo da organização até cada stakeholder da função de GRC. Se não houver aceitação em relação à transformação digital, há uma boa chance de que seus benefícios não estão sendo comunicados devidamente. A esse respeito, a auditoria interna está em uma posição única para retransmitir essas informações simplesmente ao manter seu lugar à mesa.

"A partir de nosso lugar à mesa, podemos garantir, por meio de cada tendência emergente, que a gestão e o conselho tomem decisões informadas", disse Kuhn.

De fato, um lugar à mesa deve ser sempre fundamental para que um auditor interno desempenhe as suas funções de acordo com o seu mandato. Por meio da comunicação regular e informada com os stakeholders, a auditoria interna desempenha um papel inestimável na promoção de uma forte cultura organizacional em torno da avaliação de riscos e conformidade. Quando os canais de comunicação de auditoria interna são alavancados em todo o seu potencial, o GRC sempre deve ser lembrado.

O risco de proliferação das ferramentas de GRC

Nem todos os controles disponíveis para implantação conduzirão a uma cultura bem-sucedida focada em GRC. Por exemplo, com a digitalização dos processos organizacionais, agora há muitas ferramentas de análise de dados disponíveis que apresentam módulos de GRC como complementos. A auditoria interna pode se encontrar significativamente prejudicada na comunicação de uma visão abrangente do GRC para os stakeholders, se todas as funções individuais de GRC se comprometerem com o uso de ferramentas separadas para auxiliá-las.

"Adoro as ferramentas de análise de dados e as habilidades de teste 100% que fornecem, mas agora há muitas outras ferramentas que agregam o GRC como oferta de valor", diz Audra Nariunaite, diretora de conformidade do provedor de plataforma automatizada de empregos Oyster. "Uma ferramenta que eu estava olhando recentemente agrega outras ferramentas SaaS para destacar quais contratos estão próximos da renovação e possíveis economias em impostos, mas também fornece uma versão de um painel de risco com base nas informações que as ferramentas SaaS processam. Se a intenção de comprar tal ferramenta fosse para algo diferente de GRC, eu nem saberia disso."

"De repente, eu poderia estar em uma situação em que teria uma dúzia de ferramentas SaaS aleatórias com componentes, todas elas representando um risco de alto nível, porque os fornecedores estão processando nossas informações privadas", continuou Nariunaite. "Atualmente, há mais de 100 ferramentas SaaS em nosso ecossistema. Mesmo que uma pequena porcentagem dessas ferramentas ofereça uma versão de GRC para processos muito específicos, torna-se difícil de gerenciar. Isso cria bolsos individuais onde as pessoas pensam que estão fazendo avaliações de riscos, mas não estão fazendo de forma integrada, holística e reportável."

Para combater esse risco, uma estratégia é que os stakeholders de GRC atribuam proprietários de processos individuais para simplificar a abordagem de GRC e criar um rastro de comunicação claro para a auditoria interna. "Todo mundo quer fazer o que é certo", disse

Nariunaite. “Há um esforço para gerenciar o risco geral agora, e isso é ótimo. No entanto, é preciso haver discussões sobre a divisão de funções e como devem ocorrer para alinhar prioridades e escopos.”

Kuhn expressou um sentimento semelhante ao enfatizar o equilíbrio que as organizações devem ter entre responsabilidade compartilhada e controle *top-down*. “A auditoria interna deve tentar permitir que os stakeholders conduzam os objetivos e processos de GRC tanto quanto possível e, em seguida, abordá-los a partir de um contexto de promover a colaboração e a transparência. A auditoria interna deve fazer parte dessa conversa, para que possamos estar lá para soar o alerta vermelho quando virmos algo. A maioria das pessoas entende o risco e o controle no que se refere às suas próprias funções. Eles realmente não precisam de nossa interferência, mas precisamos entender os objetivos mais amplos e quem são os responsáveis por realizar uma supervisão adequada.”

Estratégias para liderar e promover a discussão

Sempre que possível, a auditoria interna deve liderar pelo exemplo, projetando e promovendo os benefícios da transformação digital por meio da eficácia de sua função. Embora alguns aspectos da transformação digital dentro da auditoria interna obviamente exijam uma margem orçamentária significativa, outros aspectos, como a automação básica, podem ser realizados por meio de programas como Excel, Power BI e outras ferramentas de produtividade da Microsoft que provavelmente já existem internamente ou, pelo menos, podem ser adquiridas a um custo mínimo.

Liderar pelo exemplo também se aplica ao compartilhamento de conhecimento, incluindo destacar onde faltam competências críticas nas funções de GRC. Tanto na função de auditoria interna quanto em outros departamentos, a auditoria interna pode desempenhar um papel construtivo ao destacar lacunas no conhecimento, treinamento ou experiência da força de trabalho relacionada ao trabalho com tecnologias emergentes, ao mesmo tempo em que promove medidas corretivas apropriadas. Tais medidas podem incluir treinamento em grupo em conferências, contratação de terceiros para treinamento e qualificação, ou simplesmente incorporar treinamento baseado em habilidades em funções de trabalho, por meio de recursos on-line gratuitos ou com preços razoáveis.

Em alguns casos, as organizações podem trabalhar para promover a qualificação interna por meio de interações e colaborações com outros departamentos. “Uma estratégia que vi é construir um site onde todos na organização possam inserir suas próprias ideias de inovação e, então, votar ou comentar sobre o que gostariam de ver na empresa”, disse Kuhn. “Seria uma forma de compartilhar conhecimentos e ideias de forma controlada, para que todos não saíssem e fizessem mil coisas diferentes para desenvolver competências.”

Essa discussão nem sempre precisa ser formal; mesmo algo tão simples como um bate-papo comunitário pode produzir um resultado semelhante. “Em nossa organização, existem vários canais do Slack nos quais qualquer um pode participar”, disse Nariunaite. “Ultimamente, por exemplo, tenho frequentado o canal de humor da engenharia. Eles entendem que sou o chefe de *compliance*, mas me tratam como uma parceira. Adoro que todos possamos ter conexões informais com equipes que estão realmente na vanguarda do movimento de transformação digital.”

No entanto, para que a auditoria interna contribua com a discussão, deve haver um ímpeto adicional para que ela se torne bem-informada sobre essas tecnologias.

De fato, a aquisição de tal conhecimento pode ser uma oportunidade valiosa para a auditoria interna agregar ao valor organizacional que fornece. “Acho que não podemos nos envolver significativamente na discussão com os stakeholders quando pedimos para nos reunir com elas sobre, digamos, IA ou análise de dados, se nós mesmos não tivermos um grau significativo de conhecimento”, disse Nariunaite. “Muitos aspectos da transformação digital no GRC ainda estão em aberto sobre quem vai se apropriar deles. Por que não a auditoria interna? Somos curiosos; temos uma mente aberta; e estamos sempre aprendendo junto com nossos clientes, para termos lugar nas discussões. E se fôssemos nós a prestar assessoria sobre algo como a implantação da IA na conformidade?”

Conclusão

Seja uma Parte Ativa da Comunidade de Auditoria Interna

Não há como voltar atrás em uma transformação digital, e as escolhas para uma organização são simples: aceitar ou ficar para trás. Esse sentimento realmente flui por todos os elementos da organização, desde a alta administração e o conselho, até o GRC, operações e auditoria interna.

Além disso, especialmente em um mundo cada vez mais interconectado e globalizado, ele deve mesmo fluir entre indústrias e fronteiras geográficas. Isso significa não apenas executar tarefas dentro dos limites de uma organização, mas também ir além, para se tornar um participante ativo nas discussões globais de auditoria. As filiais locais do IIA podem ser um ótimo lugar para forjar tais conexões, assim como a participação regular em webinários e conferências do IIA.

"O melhor aprendizado de auditoria interna que você pode ter é ouvir em primeira mão as experiências de outras funções", disse Nariunaite. "Aprendo tanto só por 'nerdar' sobre tópicos atuais de auditoria e tendências tecnológicas com outros profissionais no Twitter. A profissão mudou muito desde quando comecei; é muito importante manter essas conexões da indústria e acompanhar como os outros estão enfrentando com sucesso os desafios que você enfrenta."

Embora a tecnologia tenha avançado tanto – e continuará avançando –, há um certo grau de conforto em saber que, quando se trata de aprender e crescer em uma função profissional, ainda não há substituto para a conexão humana genuína. Diante de mudanças implacáveis, será importante lembrar disso.

Sobre o The IIA

The Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos que atende a mais de 235.000 membros globais, tendo concedido mais de 190.000 certificações *Certified Internal Auditor* (CIA) no mundo todo. Fundado 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.

Isenção de Responsabilidade

The IIA publica este documento para fins informativos e educacionais. Este material não se destina a fornecer respostas definitivas a circunstâncias individuais específicas e, como tal, destina-se apenas a ser usado como guia. The IIA recomenda buscar assessoria especializada independente relacionada diretamente a qualquer situação específica. The IIA não aceita qualquer responsabilidade por qualquer pessoa que confie exclusivamente neste material.

Copyright

Junho de 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101