KPMG

Comitê de Auditoria: prioridades para a agenda de 2024

KPMG ACI Celebrando 20 anos

KPMG Board Leadership Center

Exploring issues. Delivering insights. Advancing governance

KPMG ACI Celebrando 20 anos | KPMG Board Leadership Center Exploring issues. Delivering insights. Advancing governance

Introdução

O ambiente de negócios e dos seus respectivos riscos emergentes mudou drasticamente ao longo do último ano, com uma maior instabilidade, destacando-se os aspectos geopolíticos, o aumento global da inflação, altas taxas de juros e níveis sem precedentes de disrupção, principalmente a tecnológica.

Nesse contexto, os comitês de auditoria devem esperar que as demonstrações financeiras e demais divulgações ao mercado, o *compliance*, o gerenciamento de riscos e os controles internos serão testados por uma série de desafios — desde a volatilidade econômica global e os conflitos bélicos internacionais, até os riscos de cibersegurança e os ataques de *ransomware*. Soma-se a esse cenário a preparação para atender às novas regulações para divulgações climáticas e relatórios de sustentabilidade, que exigirá o desenvolvimento de controles internos e procedimentos de divulgação adicionais e apropriados.

Com base em nossas interações com membros de comitês de auditoria e demais líderes corporativos, ao longo de discussões individuais e em nossas Mesas de Debate, o ACI Institute e o Board Leadership Center da KPMG destacou oito temas que devem ser considerados à medida que o comitê de auditoria (COAUD) elabora e executa a sua agenda para 2024:

- (Ainda a) Prioridade número um: mantenha o foco nas demonstrações financeiras e nos riscos relacionados aos controles internos.
- Estabeleça o papel do comitê de auditoria, alinhado com os demais comitês e o próprio conselho de administração, com relação às novas regras e regulações sobre divulgações climáticas, do relatório de sustentabilidade e relativas ao ESG, com o propósito do cumprimento, qualidade e confiança das informações publicadas.
- Mantenha o foco na cibersegurança e na privacidade de dados — incluindo o quanto a empresa está preparada para atender as regras regulatórias.
- Defina as responsabilidades do comitê de auditoria, com relação à Inteligência Artificial Generativa (GenAI).
- Esteja atento à estrutura financeira e contábil da Empresa, com relação à liderança e talentos.
- Monitore a qualidade do auditor independente e assegure uma comunicação efetiva.
- Certifique-se de que a auditoria interna esteja focada nos riscos críticos da empresa — para além dos trabalhos adicionais — e que ela seja um recurso valioso para o próprio comitê de auditoria.
- Auxilie a empresa a aprimorar o foco em ética, *compliance* e cultura corporativa.

(Ainda a) Prioridade número um: mantenha o foco nas demonstrações financeiras e nos riscos relacionados aos controles internos.

O foco nas demonstrações financeiras e nas demais divulgações ao mercado, impactado pelo atual cenário geopolítico, macroeconômico e de riscos emergentes, continuará sendo a prioridade número um e o maior desafio para os comitês de auditoria em 2024. Destaque para as novas exigências e obrigações do Formulário de Referência (FRE) do ano de 2023[1], complementadas pela Resolução CVM 59[2], além de outras regras contábeis e de divulgação estabelecidas ou em andamento, tais como as relacionadas às questões climáticas e de segurança cibernética.

Assuntos que merecem atenção:

Notas explicativas e estimativas ou projeções:

— Divulgações sobre o impacto dos conflitos na Ucrânia e no Oriente Médio e possíveis ações/sanções governamentais, disrupções nos canais de vendas e na cadeia de suprimentos, aumento dos riscos cibernéticos, inflação e taxas de juros, volatilidade do mercado e o risco de inadimplência;

— Processo de elaboração e premissas utilizadas para as estimativas e as projeções de caixa e dos negócios;

— Redução do valor recuperável dos ativos não financeiros (*impairment*), incluindo ágio por expectativa de rentabilidade futura (*goodwill*) e outros ativos intangíveis;

— Impacto de eventos e tendências sobre a liquidez e a contabilização de ativos financeiros *(fair value)*;

— Continuidade operacional *(going concern)*;

— Qualidade, consistência e suficiência/necessidade das divulgações financeiras e não-financeiras.

Com as empresas sendo exigidas a tomar decisões cada vez mais difíceis, os órgãos reguladores estão enfatizando a importância do melhor julgamento nas decisões e da transparência nas suas divulgações, incluindo documentações apropriadas e processos e controles de qualidade rigorosos que possam demonstrar a fundamentação das decisões, o seu registro e divulgação. Dada a natureza instável do ambiente de negócios, seja no curto ou no longo prazo, a divulgação de mudanças no julgamento, estimativas e controles pode ser requerida com mais frequência.

Ao realizar suas atividades, o COAUD deve considerar os aspectos críticos sob foco dos reguladores e as recomendações sobre o que deve ser divulgado e como fazê-lo. Considere realizar discussões mais amplas com a gestão para alinhar as informações a serem apresentadas pela empresa e as expectativas de divulgação ao mercado. Ao mesmo tempo, deve-se assegurar a qualidade de processos, pessoas e controles internos que geram essas informações.

Controles internos do processo contábil e de preparação das demonstrações financeiras.

Considerando o atual ambiente de riscos, bem como as mudanças no mercado — tais como M&A, novas linhas de negócios, transformações digitais, entre outras — a efetividade dos controles internos continuará a ser testadas. Discuta com a gestão como as tendências dos negócios e as exigências regulatórias, incluindo as novas regras

[1] Formulário de Referência CVM 2023 para companhias abertas. KPMG no Brasil, 2023.

[2] Resolução CVM 59. Comissão de Valores Mobiliários (CVM), 2021.

sobre segurança cibernética e proteção de dados, divulgações climáticas e de sustentabilidade, afetam os controles internos, que asseguram a efetividade do processo contábil e de preparação e divulgação das demonstrações financeiras e de outras informações ao mercado.

Quando deficiências nos controles internos forem identificadas, os órgãos de governança — seja o conselho de administração, o comitê de auditoria ou a gestão — devem avaliá-las sob uma perspectiva holística e não somente de forna pontual, a fim de avaliar o grau de severidade e a causa da deficiência. Na 18ª edição do estudo "A Governança Corporativa e o Mercado de Capitais"[3], elaborado pelo ACI Institute e o Board Leadership Center da KPMG no Brasil, 37% das empresas abertas analisadas informaram a existência de deficiências significativas nos controles internos reportadas pelos seus auditores independentes. Um plano de ação para endereçar uma deficiência identificada no nível do processo ou de uma transação pode não ser suficiente ou adequado para se remediar a causa raiz de um problema mais amplo no ambiente corporativo de controles internos, e dependendo da sua gravidade, pode trazer perdas ou prejuízos significativos no futuro.

O comitê de auditoria, juntamente da gestão, está analisando e avaliando regularmente a qualidade do atual ambiente de controles internos e dos processos de divulgação das demonstrações financeiras e das outras informações financeiras ao mercado? Os controles internos vêm acompanhando o ritmo das operações, do modelo de negócios e do perfil de riscos em constante transformação? Como os riscos emergentes são avaliados em termos de impactos nas demonstrações financeiras e quais as ações em prática para gerenciá-los, como otimização ou mitigação?

Veja também: Controles Internos e as deficiências reportadas pelas empresas abertas brasileiras[4]

Importância do gerenciamento de riscos corporativo (ERM- Enterprise Risk Management).

Cada vez mais, os comitês de auditoria têm sido exigidos a monitorar a estrutura de gerenciamento de riscos da empresa e a assegurar a sua efetividade. O conselho de administração, *stakeholders* e os próprios reguladores têm exigido ou esperam que os comitês de auditoria monitorem o gerenciamento dos riscos corporativos, além dos riscos relacionados às demonstrações financeiras e das demais informações ao mercado. É unânime entre os membros dos comitês de auditoria a preocupação do acúmulo de tarefas sob a sua responsabilidade.

Nesse contexto, é importante que o comitê de auditoria tenha a habilidade de assegurar que os resultados dos trabalhos da auditoria interna, área de gerenciamento de riscos, *compliance* e auditoria independente os auxilie nessa atividade de monitoramento do gerenciamento de riscos corporativos e respectivos controles internos, e a sua conexão com o processo contábil e de preparação das demonstrações financeiras e demais informações divulgadas ao mercado.

Agenda, composição e expertise do comitê de auditoria.

Como citado anteriormente, a agenda dos comitês de auditoria está gradativamente mais repleta de atividades e novas responsabilidades. O surgimento de regras regulatórias, atuação mais rigorosa dos reguladores, maior escrutínio dos *stakeholders*, riscos emergentes e disruptivos têm trazido dificuldades para os comitês de auditoria focarem nas suas atividades primárias, relacionadas às demonstrações financeiras e correspondentes controles internos, e no monitoramento e relacionamento com os auditores independentes. Isso, com certeza, aumenta as preocupações com relação à composição do comitê de auditoria e a sobrecarga da sua agenda.

Reavalie se o COAUD possui tempo suficiente e se os membros têm o conhecimento adequado e suficiente para supervisionar os riscos emergentes e de maior impacto para o negócio. Muitas vezes, esse conhecimento pode estar num outro comitê do conselho.

Riscos relacionados à segurança cibernética e proteção de dados, inteligência artificial, questões climáticas e ESG deveriam ser endereçadas diretamente pelo conselho de administração ou poderiam estar num outro comitê do conselho ou mesmo num comitê específico? Talvez, a adição de membros especialistas ou a contratação de consultores externos com outros conjuntos de habilidades possa ser suficiente para o COAUD?

Reavalie se o comitê de auditoria dispõe de tempo e conhecimento adequado/suficiente para as suas atividades, incluindo o monitoramento do gerenciamento dos principais riscos emergentes.

[3] A Governança Corporativa e o Mercado de Capitais – 18ª edição. ACI Institute e Board Leadership Center da KPMG no Brasil, 2023.

[4] Controles Internos e as deficiências reportadas pelas empresas abertas brasileiras. ACI Institute e Board Leadership Center da KPMG no Brasil, 2024.

Estabeleça o papel do comitê de auditoria, alinhado com os demais comitês e o próprio conselho de administração, com relação às novas regras e regulações sobre divulgações climáticas, do relatório de sustentabilidade e relativas ao ESG, com o propósito do cumprimento e a qualidade e confiança das informações publicadas.

ESG é um tema recorrente nas agendas dos comitês de auditoria, sobretudo na supervisão do cumprimento às exigências legais e de órgãos reguladores e as suas divulgações ao mercado[5], seja no aspecto da suficiência, consistência ou confiança das informações. O esforço da administração para atender o aumento das exigências de divulgação de informações sobre as questões climáticas e o ESG nos próximos anos deverá exigir um foco constante, tanto do COAUD, como do próprio conselho de administração (vide também a publicação "Conselho de Administração: Prioridades para a agenda de 2024") .

À medida que os órgãos reguladores, do Brasil ou do exterior, investidores e potenciais investidores, empresas de *rating*, funcionários, clientes e demais *stakeholders* buscam por informações úteis, precisas e comparáveis, estabelecer o papel e as responsabilidades do comitê de auditoria nesse tema deve ser uma prioridade. O COAUD deve estar preparado e contar com as competências adequadas para monitorar a qualidade das divulgações ao mercado — obrigatórias ou voluntárias — e o cumprimento das regras de divulgação que vêm se consolidando, sejam elas já estabelecidas pela CVM, pelo *IFRS Sustainability Disclosure Standards*, emitido pelo *ISSB-International Sustainability Standards Board*, e outras regras e regulações sobre questões climáticas e de sustentabilidade em desenvolvimento, ou já em vigência, tais como nos Estados Unidos (SEC) e na União Europeia (ESRS-*European Sustainability Reporting Standards, baseado no – CSRD - EU´s Corporate Sustainability Reporting Directive*), entre outras.

No Brasil, a Resolução CVM 193 colocou o país na posição do primeiro em que o órgão regulador determinou a adoção das normas do ISSB como padrão para as divulgações de sustentabilidade[6]. Em um primeiro momento, as companhias poderão optar por adotar, ou não, as normas do ISSB; a partir dos exercícios sociais iniciados em, ou após, 1º de janeiro de 2026, a adoção passará a ser obrigatória[7] . Outros países também anunciaram a adoção ou o compromisso de considerar a adoção das normas finais do ISSB, como Austrália (somente clima), Japão e Reino Unido.

Já no caso das diretrizes do *Corporate Sustainability Reporting Directive (CSRD),* da União Europeia, as regras entraram em vigor em janeiro de 2024, e chamam atenção pela sua abrangência internacional. Apesar de a CSRD ser uma diretiva da UE, existem implicações consideráveis nos relatórios ESG para empresas sediadas no exterior, com subsidiárias na UE, incluindo aquelas com títulos listados em uma bolsa regulamentada pela UE. Existem isenções, e dependendo do tamanho e da receita da empresa, a data do início da obrigatoriedade é diferente, assim como os requerimentos dos relatórios. Por isso, é fundamental avaliar se a organização está sujeita às regras do CSRD e a partir de quando.

[5] Desafios e Prioridades do Comitê de Auditoria. ACI Institute e Board Leadership Center da KPMG no Brasil, 2023.

[6] Resolução Nº 193 da CVM dispõe sobre adoção das normas ISSB. KPMG no Brasil, 2023.

[7] Normas de sustentabilidade no Brasil. KPMG no Brasil, 2023.

Posteriormente, a empresa deve se preparar para identificar os impactos, riscos e oportunidades e realizar uma avaliação de dupla materialidade que abrange não apenas a empresa relatora, mas também a sua cadeia de valor. Além disso, é importante garantir estruturas de governança adequadas logo no começo da obrigatoriedade[8]. Vale destacar que ainda que as diretrizes não sejam mandatórias para organizações fora do escopo, segui-las pode trazer vantagens competitivas na contratação de fornecedores terceirizados.

As regras regulatórias citadas anteriormente vêm se baseando, seja parcialmente ou substancialmente, nos padrões e no framework do *Task Force on Climate Related Financial Disclosures (TCFD)* e o *Greenhouse Gas (GHG) Protocol*, cujas diretrizes são orientativas e permitem expansão. Dessa forma, mais detalhes com relação à divulgação, tais como dados sobre a emissão de gás carbônico e outros gases (*GHG emission*) de Escopo 1 de Escopo 2 (em muitos casos, de escopo 3), asseguração sobre a emissão de terceiros (*third-party assurance*), bem como o impacto dos riscos relacionados ao clima sobre o negócio, o modelo de negócio, as condições financeiras e a própria estratégia das empresas, têm sido desenvolvidos dentro desse arcabouço regulatório. No Brasil, o Formulário de Referência, documento de divulgação obrigatória, estabelecido pela CVM, já exige que as empresas abertas divulguem se consideram as recomendações da TCFD nos relatórios de sustentabilidade, ou recomendações de outras entidades reconhecidas relacionadas a questões climáticas, se for o caso. As empresas precisarão acompanhar os desenvolvimentos e alterações nas regras regulatórias em andamento, vigência e a sua aplicabilidade na companhia.

Uma das principais áreas de foco do comitê de auditoria será acompanhar o grau de preparação da empresa para o atendimento a essas regras regulatórias, em linha com as expectativas dos *stakeholers*, realizando atualizações periódicas com a gestão, incluindo *gap analysis*, suficiência e habilidade dos recursos e talentos necessários para cumprir os prazos regulamentares. Além disso, as companhias também precisam assegurar se as divulgações são consistentes, precisas e suficientes ou detalhadas em excesso e se os potenciais riscos de divulgação e imagem foram mitigados ou endereçados. Essa tarefa exigirá uma interação multidisciplinar com os demais comitês do conselho de administração, executivos, gestores das área de sustentabilidade e demais gestores com relação ao ESG e o próprio conselho de administração. Um total alinhamento e uma comunicação clara e constante são fundamentais para definir os papéis e limites da atuação de cada um. Nesse contexto, o comitê de auditoria poderia considerar os seguintes aspectos para o seu foco:

— Dar o suporte ao conselho de administração para definir os responsáveis por atender as regras regulatórias relativas à definição dos papéis e responsabilidades na empresa com relação às divulgações climáticas, ao relatório de sustentabilidade e outras informações públicas referentes ao ESG, realizadas de forma obrigatória ou voluntária, por meio de *webcasts*, *site* da empresa ou na mídia. Essa definição deve incluir também os responsáveis pelas revisões, aprovações e monitoramento desse processo.

— Assegurar que a gestão tenha um processo estabelecido para garantir a qualidade, suficiência e consistência das divulgações, que potenciais riscos tenham sido mapeados, avaliados e que os controles internos tenham sido implementados para mitigá-los ou endereçá-los. O COAUD deverá monitorar a efetividade desse processo, incluindo assegurar a adequação das informações divulgadas, com o mesmo rigor aplicado às demonstrações financeiras.

— Ainda com relação a um processo estabelecido, assegurar que a empresa possui profissionais qualificados, com tempo e habilidade suficientes, e de sistemas apropriados e integrados com os demais sistemas operacionais, financeiros e contábeis para garantir a qualidade e a consistência das informações, inclusive na coleta de informações de terceiros, quando aplicável.

— Avaliar se a composição do COAUD é suficiente para atender essa demanda, ou se haveria a necessidade de novos membros, a contratação de especialistas para atuar com *advisors* e/ou a distribuição de atividades ou mesmo uma maior interação com os demais comitês do conselho de administração.

[8] HOT TOPIC ESG in Europe Global implications of EU sustainability reporting, KPMG nos EUA, dezembro 2023.

Mantenha o foco na cibersegurança e na privacidade de dados — incluindo o quanto a empresa está preparada para atender as regras regulatórias.

O risco de cibersegurança continua a crescer. A aceleração do desenvolvimento da Inteligência Artificial, a sofisticação cada vez maior dos ataques cibernéticos, os conflitos na Ucrânia e no Oriente Médio e os seus efeitos tecnológicos, e as linhas de responsabilidade pouco definidas — entre usuários, empresas, fornecedores e órgãos governamentais — vêm intensificando cada vez mais a sua abordagem nas agendas do comitê de auditoria e do conselho de administração.

No aspecto regulatório, as empresas são cada vez mais demandas por maior transparência sobre como estão avaliando e gerenciando riscos cibernéticos e a governança de dados. O cenário é ainda mais desafiador para empresas que operam internacionalmente, sujeitas a regras e regulações internacionais, além daquelas em desenvolvimento no Brasil. A divulgação de incidências de ataques cibernéticos vem sendo recorrentemente exigida pelos órgãos reguladores, com o apoio do mercado.

A SEC *(Securities and Exchange Commission)*, dos Estados Unidos, criou recentemente regras de divulgação relativas à segurança cibernética, que tocam os termos da governança sobre o assunto e a divulgação de incidentes, em vigor para as empresas abertas norte-americanas desde 2023. Dentre elas, os seguintes requerimentos que também fazem parte de regulações em outros países:

— Informação sobre a governança, estratégia e o gerenciamento dos riscos relacionados à segurança cibernética. Adicionalmente, sobre as responsabilidades do conselho de administração no monitoramento do gerenciamento dos riscos de ataque cibernético e o papel e responsabilidades da gestão na avaliação e gerenciamento dos riscos de ataque cibernético.

— Divulgação de incidentes de ataques cibernéticos em até quatro dias úteis, após a empresa concluir que o incidente teve consequências materiais (não é a partir da data que o incidente foi descoberto) e seus impactos na empresa.

No Brasil, iniciativas têm sido desenvolvidas pelos reguladores e trarão maiores responsabilidades de ação e divulgação pelas empresas. Além disso, algumas iniciativas governamentais foram lançadas recentemente, destacando-se o Decreto 11.856 de 26/12/23, que instituiu a Política Nacional de Cibersegurança (PNCiber), proposta pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), com o propósito de melhorar a governança nacional sobre a cibersegurança e fortalecer a atuação diligente no ciberespaço, além de contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas nesse ambiente. A PNCiber possui como instrumentos a Estratégia Nacional de Cibersegurança (e-Ciber) e o Plano Nacional de Cibersegurança (p-Ciber). O decreto também instituiu o Comitê Nacional de Cibersegurança (CNCiber) [9]. Vale lembrar também a própria Lei Geral de Proteção de Dados (Lei 13.709/2018), cujos objetivos são assegurar os direitos fundamentais de liberdade e de privacidade e promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil.

9. Comitê Nacional de Cibersegurança (CNCiber), Gabinete de Segurança Institucional, Gov.Br, 2024.

Dessa forma, as empresas vêm sendo cada vez mais exigidas e têm procurado se estruturar para endereçar os riscos de segurança cibernética e manter um controle efetivo sobre os dados de terceiros. Além do prejuízo financeiro derivado de um ataque cibernético ou do não cumprimento às regras de privacidade de dados, danos à reputação e à imagem da empresa podem trazer consequências catastróficas. Nesse contexto, o comitê de auditoria deve se atentar para os seguintes aspectos:

Segurança de Dados.

Embora a governança de dados se sobreponha à segurança cibernética, ela é mais ampla e inclui o *compliance* com leis e regulamentações específicas, bem como normas de privacidade que regem o uso, o armazenamento e o tratamento de dados pessoais. A governança de dados também inclui políticas e controles internos relativos à ética dos dados, sobretudo o gerenciamento das tensões entre a forma como a empresa pode usar os dados dos clientes de maneira legalmente permitida e as expectativas dos clientes sobre como seus dados serão usados[10]. O estudo *Privacy Risk Study 2023*[11], realizado pela Associação Internacional de Profissionais de Privacidade (IAPP), em colaboração com a KPMG, mostra que 83% das organizações reportam informações de risco de privacidade em seu relatório anual. O levantamento ainda revela que os 5 domínios de risco de privacidade com maior prioridade identificados pelos participantes são:

1 - Vazamento de dados;

2 - Tratamento de dados por terceiros em não conformidade;

3 - Implementações inefetivas de *Privacy by Design*;

4 - Gestão de dados pessoais de forma inapropriada;

5 - Treinamentos de privacidade insuficientes para os colaboradores.

Divulgações sobre a governança, estratégia e o gerenciamento de riscos de segurança cibernética.

Essas divulgações se tornarão gradativamente obrigatórias ou as próprias empresas decidirão realizá-las de forma voluntária. Elas exigirão uma maior atenção e atuação do comitê de auditoria e do próprio conselho de administração sobre a estrutura de governança e de gerenciamento de riscos da empresa, bem como uma atuação mais próxima com a gestão. Além disso, a empresa deverá estar preparada para reportar incidentes de ataques cibernéticos e os respectivos planos de ação em resposta a esses ataques. Decidir o quê reportar, como, quando e a quem, demandará revisão e ajustes nas políticas, procedimentos e controles internos da empresa, para estabelecer o nível de materialidade que exige divulgação, bem como definir os planos de ação para investigação e remediação do incidente. Um grupo multidisciplinar será necessário para essa tarefa, além dos responsáveis pela segurança cibernética, proteção de dados e pelo gerenciamento de riscos, com a inclusão dos responsáveis pela área Legal, de RI e TI.

Plano de resposta da gestão a incidentes cibernéticos.

Um Plano de Resposta a um incidente cibernético deve incluir um protocolo de escalonamento para informação, discussão, endereçamento e divulgação de um incidente. Além de monitorar a efetividade do Plano, tanto o comitê de auditoria como o conselho de administração devem fazer parte desse processo de escalonamento, incluindo seus papéis e responsabilidades. Considere também como as comunicações internas e externas devem ser tratadas. Exercícios práticos e testes de estresse periódicos devem ser realizados para avaliar a eficiência dos planos de resposta e identificar quaisquer *gaps* que possam existir. Os procedimentos de resposta a incidentes também devem ser atualizados para considerar as mudanças no ambiente de negócios e respectivos riscos cibernéticos e de proteção de dados emergentes.

[10] On the 2024 audit committee agenda. KPMG UK, 2023.

[11] Privacy Risk Study 2023. KPMG no Brasil, 2023.

KPMG ACI Celebrando 20 anos

KPMG Board Leadership Center
Exploring issues. Delivering insights. Advancing governance

Defina as responsabilidades do comitê de auditoria, com relação à Inteligência Artificial Generativa (IA).

A supervisão dos riscos e das oportunidades da Inteligência Artificial Generativa (GenAI) será prioridade para a maioria dos conselhos de administração em 2024, como indica a publicação *Conselho de Administração: Prioridades para a agenda de 2024*. Muitos conselhos estão considerando qual seria a melhor forma de supervisionar as tecnologias de GenAI no negócio, seja pelo próprio conselho ou por meio dos seus comitês.

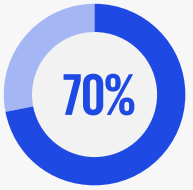
Essa tarefa, no aspecto de monitorar o cumprimento às regras e regulamentos existentes e em desenvolvimento, referentes à GenAI e ao gerenciamento dos riscos relacionados, deverá ficar com o comitê de auditoria, bem como a implantação dos respectivos controles internos e o processo de divulgação do tema ao mercado.

Alguns comitês de auditoria poderão ter responsabilidades adicionais de supervisão da estrutura de governança da empresa para o desenvolvimento e o uso de ferramentas de Inteligência Artificial. Como e quando um sistema ou modelo de IA Generativa — inclusive modelos de terceiros — é desenvolvido e implementado? Quem toma a decisão final? Como os riscos relacionados ao GenAI são mapeados, avaliados e mitigados ou endereçados? A organização dispõe de talentos e recursos adequados para a GenIA?

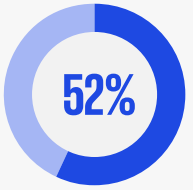
Em linha com o desenvolvimento internacional de regulações e ações governamentais, no Brasil, está em votação no Senado o Projeto de Lei 2338/23, que dispõe sobre o uso de inteligência artificial e estabelece normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial no Brasil, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico.

Dada a volatilidade da situação e o rápido desenvolvimento da GenIA, uma reflexão sobre o papel e as responsabilidades do COAUD sobre o assunto será necessária.

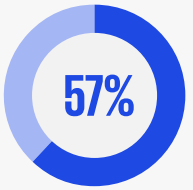
Destaques do "KPMG 2023 CEO Outlook"[12]



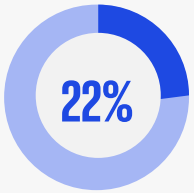
dos CEOs dizem que a IA Generativa é sua prioridade de investimento;



esperam ver retornos sobre os investimentos entre três a cinco anos;



concordam que os desafios éticos são a principal preocupação quando se trata de implementar IA generativa;



citam o aumento na lucratividade como o principal benefício da implementação da IA Generativa.

[12] KPMG 2023 CEO Outlook. KPMG no Brasil, 2023.

Esteja atento à estrutura financeira e contábil da Empresa, com relação à liderança e talentos.

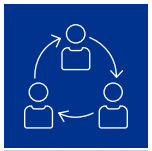
A área financeira e contábil das empresas enfrentam hoje um ambiente desafiador: em meio à escassez de talentos, é exigido da função o estabelecimento de estratégias num ambiente de profunda transformação digital e o desenvolvimento de processos e sistemas robustos e integrados, que possam coletar e manter dados e informações precisas, completas e de forma rápida. Soma-se ainda, a necessidade de atender as expectativas e exigências dos investidores e demais *stakeholders* com relação às demonstrações financeiras, relatórios de sustentabilidade, formulários de referência e outras divulgações ao mercado, de acordo com as regras, leis e regulamentos. Ao mesmo tempo, as incertezas econômicas e de mercado têm trazido dificuldades na elaboração de projeções, planejamento financeiro e do próprio orçamento.

À medida que o comitê de auditoria monitora a adequação da estrutura financeira e contábil da empresa, as seguintes sugestões poderiam ser aplicáveis:

— Esteja atento à estrutura de pessoas na área financeira e contábil. Seja no aspecto de talentos, bem como nas questões de liderança e processo de sucessão. Expertise e conhecimento em contabilidade e finanças devem incorporar também outros assuntos, tais como sustentabilidade, aspectos regulatórios aplicáveis à empresa, comunicação com *stakeholders* e inteligência artificial. Além disso, considere a importância de profissionais com conhecimento em tecnologia, processos, controles internos e sistemas.

— A aceleração da disrupção tecnológica e da digitalização traz também enormes oportunidades para a área contábil e financeira adicionar valor ao negócio. Capacidade analítica *(data & analytics)*, capacidade de transformar em números (orçamento e KPI´s) o planejamento estratégico e atuar no monitoramento contínuo das transações (*continous audit* e *continous monitoring*) são atividades que podem ser realizadas, além do processo tradicional de preparação das demonstrações financeiras e relatórios gerenciais.

É essencial que o comitê de auditoria reserve o seu tempo para entender o plano estratégico da área financeira e contábil nos aspectos de gerenciamento de talentos, digitalização e inovação. Seja no aspecto de transformação estratégico, num horizonte de longo prazo, seja no aspecto de qualidade das pessoas, processos e controles internos, de forma a mitigar riscos derivados de deficiências no processo contábil e de preparação das demonstrações financeiras, num horizonte imediato e de curto prazo.



Monitore a qualidade do auditor independente e assegure uma comunicação efetiva.

A qualidade da auditoria independente é aprimorada por um comitê de auditoria totalmente engajado, que define de forma clara as diretrizes e suas expectativas para o auditor independente e monitora rigorosamente o seu desempenho, por meio de uma comunicação frequente e efetiva e de um processo robusto de avaliação de performance. A importância da comunicação frequente, franca e clara com a auditoria independente fica ainda mais nítida quando considerado que essa é uma das áreas com quem o comitê de auditoria tem maior interação. Segundo a pesquisa global da KPMG, "Desafios e Prioridades do Comitê de Auditoria"[13], 70% dos respondentes brasileiros e 54% globalmente disseram que, além das interações regulares com o conselho de administração, o COAUD tem uma maior interação com a auditoria externa.

Ao apresentar as expectativas para 2024, o COAUD deve discutir com o auditor independente como as demonstrações financeiras e os respectivos riscos e controles internos foram afetadas pelos riscos emergentes derivados do cenário geopolítico, macroeconômico, regulatório, bem como por eventuais mudanças no negócio.

Estabeleça expectativas claras para comunicações frequentes, abertas e francas com o auditor independente para além do que é requerido. A lista de assuntos é extensa, e inclui a independência do auditor, a qualificação da equipe de trabalho, as questões relacionadas ao planejamento e aos resultados da auditoria, entre outros. Ampliar a conversa com os auditores independentes para além desses tópicos pode aprimorar a supervisão do COAUD, sobretudo no que diz respeito à cultura corporativa, o *tone at the top* e a qualidade da área contábil.

O comitê de auditoria deve discutir com os auditores sobre o sistema de controle de qualidade existente para assegurar uma auditoria de qualidade, sustentável e com melhoria contínua. É importante entender quais novas tecnologias estão sendo implementadas como parte dos trabalhos de auditoria — incluindo o uso de ferramentas e da Inteligência Artificial.

Nas conversas com o auditor independente sobre os sistemas de qualidade e controles internos, considere também os resultados das inspeções de órgãos reguladores e de seus pares *(peer review)*, bem como as ações implementadas para endereçar eventuais deficiências identificadas, se for o caso. Lembre-se que a qualidade da auditoria independente é um esforço coletivo e exige comprometimento e engajamento de todos os envolvidos no processo: auditor externo, COAUD, auditoria interna e gestão.

Discuta com detalhes a carta de controles internos (relatório circunstanciado) de forma a entender as deficiências nos controles internos, sejam elas significativas ou não, sobre os motivos da sua existência. A 18ª edição do estudo "A Governança Corporativa e o Mercado de Capitais"[14], demonstrou que das 282 companhias analisadas, 99 empresas (37%) reportaram deficiências ou recomendações nos controles internos apontadas pelos auditores independentes. De acordo com o estudo, as deficiências divulgadas pelos auditores independentes se concentraram em três aspectos: tecnologia da informação, processo contábil e demonstrações financeiras, e a gestão operacional.

Mais importante que discutir a deficiência de forma isolada à transação ou ao fato que trouxe a sua ocorrência, é procurar entender a causa raiz do problema. Discuta com a gestão sobre planos de ação para remediação da deficiência e sobre a sua suficiência dentro de uma visão mais ampla do ambiente de controles internos como um todo.

[13] Desafios e Prioridades do Comitê de Auditoria. ACI Institute e Board Leadership Center da KPMG no Brasil, 2023.
[14] A Governança Corporativa e o Mercado de Capitais – 18ª edição. ACI Institute e Board Leadership Center da KPMG no Brasil, 2023

Certifique-se de que a auditoria interna esteja focada nos riscos críticos da empresa — para além dos trabalhos adicionais — e que ela seja um recurso valioso para o próprio comitê de auditoria.

À medida que os comitês de auditoria enfrentam agendas desafiadoras — e o gerenciamento de riscos tem sido colocado cada vez mais à prova — a auditoria interna tornou-se um recurso e aliado valiosíssimo para o COAUD; e uma voz crucial sobre as questões de risco e controles internos. Isso significa uma mudança no seu trabalho tradicional e um enfoque nos principais riscos do negócio - operacionais, tecnológicos, de terceiros, de segurança cibernética e proteção de dados e relacionados ao ESG.

Os riscos ESG estão evoluindo rapidamente e incluem a gestão do capital humano — desenvolvimento e retenção de talentos, diversidade, liderança e cultura corporativa — mudanças climáticas, segurança cibernética, governança e privacidade de dados e as suas divulgações ao mercado. O processo de divulgação e os respectivos controles internos devem ser uma área de foco para a auditoria interna. Certifique-se do papel da auditoria interna na conexão entre os riscos relacionados ao ESG e a sua inclusão no gerenciamento dos riscos corporativos (ERM). A gestão tem os recursos e os conjuntos de habilidades necessários para endereçar as iniciativas e exigências regulatórias relacionadas às mudanças climáticas e ao ESG?

Reavalie se o plano de auditoria interna é baseado em riscos e suficientemente flexível para se ajustar às mudanças do ambiente de negócios e riscos emergentes. O comitê de auditoria deve atuar de forma coordenada com o responsável pela auditoria interna e o responsável pela área de gerenciamento de riscos para contribuir no processo de identificação dos riscos mais significativos relacionados à reputação, à estratégia e às operações da empresa, assegurando que a auditoria interna esteja focada nesses principais riscos e correspondentes controles internos. Isso pode incluir riscos específicos do setor de atuação da empresa; riscos operacionais e regulatórios; econômicos e geopolíticos; climáticos; de cibersegurança e privacidade de dados; riscos derivados das tecnologias digitais e de IA Generativa; da gestão e retenção de talentos; modelos híbridos de trabalho e associados à cultura organizacional; disrupções nas cadeias de suprimentos e de terceiros; além da adequação dos planos de continuidade dos negócios e de gerenciamento de crises.

A ampliação das responsabilidades da auditoria interna exige o aprimoramento das suas habilidades. Estabeleça expectativas claras e dê suporte à auditoria interna para que ela disponha dos talentos, recursos, habilidades e *expertise* de que precisa para ser bem-sucedida na sua agenda de trabalho — desafiando a auditoria interna a refletir sobre o impacto das tecnologias digitais no seu trabalho de auditoria.

Trabalhe com o líder de auditoria interna *(chief audit executive)* e com o *risk manager (chief risk officer)* para ajudar a identificar os riscos que representam a maior ameaça à reputação, à estratégia e às operações da empresa e assegurar que a auditoria interna esteja focada nesses riscos e nos controles internos relacionados.

Auxilie a empresa a aprimorar o foco em ética, *compliance* e cultura corporativa.

Os custos reputacionais de uma conduta não ética ou de uma falha no *compliance* estão mais elevados do que nunca, sobretudo devido ao aumento dos riscos de fraude, às pressões sobre a gestão para cumprir as metas financeiras e ao aumento da vulnerabilidade a ataques cibernéticos. Para um programa de *compliance* eficaz, a definição do *"tone at the top"* e a manutenção de uma cultura alinhada ao propósito corporativo em todos os níveis são fundamentais, incluindo o compromisso com valores, ética e conformidade legal e regulatória.

À medida que o ambiente de negócios e riscos torna-se mais complexo, o desafio é ainda maior. As empresas estão em constante transformação para inovar e aproveitar oportunidades emergentes, implementar novas tecnologias e fazer melhor uso dos dados, transformar a rede de fornecedores numa cadeia de suprimentos cada vez maior e interconectada. Programas de *compliance* robustos são essenciais para a continuidade das operações e negócios bem-sucedidos.

Monitore atentamente o comportamento e as atitudes da liderança (*"tone at the top"*) e a disseminação da cultura por toda a organização, atentando-se para os possíveis sinais de alerta *(red flags)*:

- A liderança é sensível às pressões contínuas sobre os funcionários (tanto no escritório quanto em casa), com relação a questões de saúde, segurança, produtividade, engajamento e motivação? Liderança, comunicação, compreensão e compaixão são essenciais.
- A cultura da empresa garante um ambiente propício para que os profissionais façam a coisa certa? É importante que os membros do comitê de auditoria passem algum tempo em campo, interagindo com os funcionários para ter uma maior e melhor noção da cultura corporativa e sua aplicação no dia a dia.

Procure assegurar que os programas de monitoramento e de *compliance* estejam atualizados, abrangendo todos os fornecedores da cadeia de suprimentos e que as expectativas da empresa em relação aos padrões éticos tenham sido efetivamente comunicadas. Monitore também a eficiência do canal de denúncias da empresa (incluindo se todas as denúncias são adequadamente endereçadas) e os processos de investigação. A terceira edição da pesquisa "Perfil do *Hotline*"[15], elaborada pela KPMG no Brasil, mostra que o comitê de ética é quem recebe as denúncias em 22% das empresas e 52% responderam que a responsabilidade por definir se a denúncia é procedente ou não é exclusivamente desse comitê.

O comitê de auditoria tem conhecimento de todas as denúncias e recebe relatórios sobre como esses casos são endereçados com informações que permitam identificar tendências? Caso contrário, há um processo de filtragem para que somente as denúncias mais graves e significativas sejam repassadas ao COAUD? Com o aumento radical da transparência, possibilitado pelas redes sociais, a cultura e os valores corporativos, o compromisso com integridade e *compliance* e a reputação da organização ficam totalmente expostos.

Liderança, comunicação, compreensão e compaixão são essenciais.

[15] Perfil do *Hotline* – 3ª edição. KPMG no Brasil, 2023. .

Fale com nosso time

Sidney Ito
CEO do ACI Institute Brasil e
Sócio em Riscos e Governança
Corporativa da KPMG no Brasil

Fernanda Allegretti
Sócia-diretora de Mercados da
KPMG no Brasil e Líder do Board
Leadership Center Brasil

O ACI Institute e o Board Leadership Center da KPMG no Brasil

O ACI Institute (ACI) e o Board Leadership Center são iniciativas globais da KPMG voltadas a membros de conselhos de administração, conselhos fiscais e comitês de auditoria. O ACI chegou ao Brasil em 2004 e, deste então, vem tratando o tema governança corporativa com o propósito de trazer valor às empresas e demais instituições. Ao incentivar a troca de experiências entre seus membros e propiciar um espaço para debates e discussões, o ACI Institute Brasil, o Board Leadership Center e a KPMG procuram contribuir para a evolução das práticas de governança corporativa no Brasil, juntamente com os seus membros, representados por conselheiros de administração, conselheiros fiscais e membros de comitês de auditoria das mais conceituadas empresas.

Saiba mais em: https://kpmg.com/br/pt/home/servicos/aci-institute-brasil.html

KPMG ACI Celebrando 20 anos

KPMG Board Leadership Center
Exploring issues. Delivering insights. Advancing governance