GLOBAL PERSPECTIVES AND INSIGHTS

Auditoria interna e conformidade: Clareza e colaboração pa ra uma governança mais forte

The Institute of Internal Auditors | Global

Edições Anteriores

Para acessar as edições anteriores do *Global Perspectives and Insights*, acesse www.theiia.org/GPI.

Feedback dos Leitores

Envie perguntas ou comentários para globalperspectives@theiia.org.

Índice

Agradecimentos

O IIA agradece aos membros e stakeholders que contribuíram para este documento, incluindo Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sorlie, Francis Nicholson, Jill Austin e IIA – Austrália.

Sobre o The IIA

The Institute of Internal Auditors (The IIA) é o mais reconhecido advogado, educador e fornecedor de normas, orientações e certificações da profissão de auditoria interna. Fundado em 1941, o The IIA atende, atualmente, mais de 200.000 membros de mais de 170 países e territórios. A sede global da associação fica em Lake Mary, na Flórida, EUA. Para mais informações, visite www.globaliia.org.

Isenção de Responsabilidade

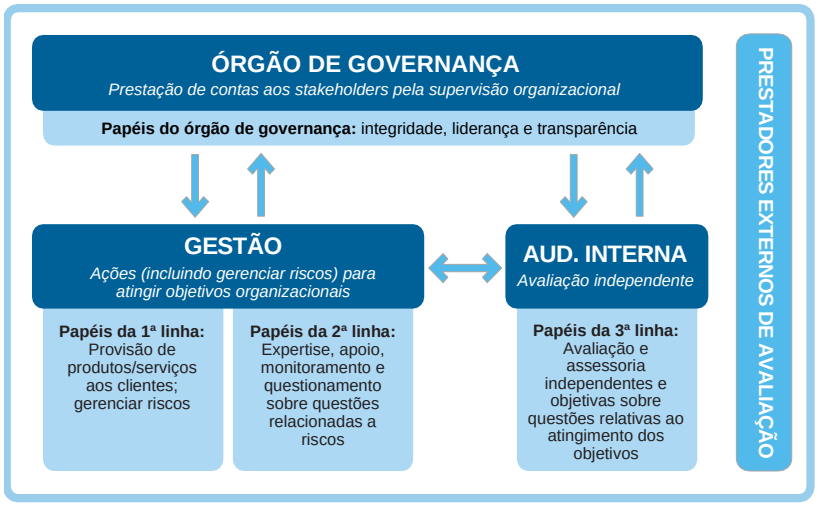
As opiniões expressas no *Global Perspectives and Insights* não são necessariamente as dos contribuintes individuais ou dos funcionários dos contribuintes.

Copyright

Introdução

A relação entre a auditoria interna e a conformidade às vezes não é clara, dando origem a perguntas importantes: a auditoria interna pode ter responsabilidade pela conformidade? Uma função de conformidade é responsável por toda a conformidade em uma organização? Como chefe executivo de auditoria, é normal ser responsável pela conformidade?

Este documento foi elaborado para ajudar a esclarecer essas complexidades e evitar confusão, lacunas e duplicações desnecessárias. A compreensão clara é essencial, a colaboração é fortemente encorajada e a independência da auditoria interna[1] é fundamentalmente importante.



Este não é um artigo sobre como auditar a conformidade. Em vez disso, ele serve como uma ferramenta para conselhos, gestão, profissionais de conformidade e chefes executivos de auditoria, e usa o *Modelo das Três Linhas* como forma de explicar a relação entre a auditoria interna e a conformidade. Os Seis Princípios do *Modelo das Três Linhas* e como eles podem ser aplicados à conformidade são examinados em profundidade posteriormente neste documento.

Os leitores devem usar este documento para identificar, compreender, avaliar e aplicar claramente dentro de uma estrutura de governança — independentemente da jurisdição, indústria, complexidade, maturidade ou tamanho —, conformidade eficaz e gerenciamento do risco de conformidade em seus vários aspectos em relação ao *Modelo das Três Linhas*.[2] Ilustrações práticas de executivos de risco e conformidade e auditores internos sobre questões de conformidade enfrentadas no campo ajudarão na aplicação prática dos Seis Princípios do modelo ao avaliar o alinhamento das atividades de conformidade de acordo com o *Modelo das Três Linhas*. (Veja as páginas 8-16)

[1] A natureza integral da conformidade como parte da governança sustentável é um foco principal e uma ação política recomendada pelo documento *B20 Italy Integrity & Compliance Policy Paper 2021*. Em particular, a Ação Política 2.1 na p. 11 menciona especificamente o papel da auditoria interna conforme descrito no Modelo das Três Linhas.

[2] Em certas jurisdições e indústrias, as funções e responsabilidades relacionadas à conformidade e ao gerenciamento de riscos de conformidade são altamente definidas e são objeto de extensa legislação, regulamentação, jurisprudência e pesquisa acadêmica. Estudos mais detalhados estão disponíveis e os usuários deste artigo prático são encorajados a consultá-los. Por exemplo, consulte *Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 e *Principles of the Law, Compliance and Enforcement* No. 2, do *American Law Institute*.

Prestação de Contas, Ações e Avaliação

O *Modelo das Três Linhas* descreve como a prestação de contas do órgão de governança, as ações da gestão e a avaliação independente pela auditoria interna fornecem a base para uma governança eficaz. Também mostra como os Seis Princípios auxiliam na avaliação dos respectivos papéis e responsabilidades em uma organização. A aplicação dos elementos centrais do modelo e dos Seis Princípios varia para cada organização, de acordo com seus objetivos, recursos e circunstâncias. O modelo ajuda as organizações a identificar estruturas, processos de desenvolvimento e atribuir responsabilidades que melhor auxiliam no atingimento dos objetivos. Isso inclui o gerenciamento do risco de conformidade, que é responsabilidade da gestão,[3] mas é alcançado por meio de um esforço colaborativo.

A gama de requisitos e expectativas de conformidade que uma organização precisa considerar compreende aqueles impostos externamente, como leis, regras e regulamentos, e impostos internamente, como políticas, normas, procedimentos e códigos de conduta ou comportamento. Eles podem ser formal e explicitamente definidos ou mais implícitos, como expectativas sociais, éticas e culturais. Esse amplo espectro dinâmico de considerações é referido neste documento como "requisitos e expectativas".

Os stakeholders esperam que a organização cumpra com seu propósito e maximize o valor de maneira legal e ética. Consequentemente, as organizações investem no monitoramento de conformidade em áreas principais, como saúde e segurança; emprego; proteção de dados e privacidade; pessoa jurídica, leis e códigos comerciais; regulamentação do setor; normas de qualidade; antissuborno e anticorrupção; proteção ao investidor e consumidor; reporte financeiro e tributação; e códigos de conduta individuais. A lista continua. A conformidade pode ser entendida e efetuada no contexto da prestação de contas, ações e avaliação, conforme descrito no *Modelo das Três Linhas*, como parte de uma abordagem geral para uma governança eficaz.

O Que É Conformidade?

As organizações devem aderir (ou cumprir com) as leis aplicáveis e outros requisitos externos que sejam pré-requisitos para fazer negócios. Esses requisitos de conformidade cobrem tudo, desde as relações com os funcionários ao pagamento de impostos. Em certas indústrias, há uma variedade de órgãos de definição de regras, supervisores, reguladores e requisitos definidos, mas outras indústrias têm menos limites, restrições legais e regulatórias impostos externamente. No entanto, é difícil identificar uma organização no setor público ou privado que não tenha requisitos de conformidade externos.

Ao mesmo tempo, as organizações projetam, desenvolvem e implantam expectativas internas na forma de políticas e procedimentos e definem padrões para o comportamento e conduta éticos. Em certos setores regulamentados, os requisitos externos determinam que uma organização deve estabelecer e aderir ao conjunto de políticas, normas e códigos comportamentais internos. Com essa rede de muitas camadas de requisitos, o conceito de “conformidade” em uma organização assume várias dimensões. Consequentemente, é útil considerar a conformidade em cada um de seus aspectos amplos –

[3] Para o propósito deste documento, o termo "*gestão*" é amplamente usado para identificar funções que não são de responsabilidade do órgão de governança ou da auditoria interna.

relacionados, mas distintos – e como ela é discutida nas organizações: como resultado; como categoria de risco[4]; como papel, departamento, função organizacional, etc.[5]; e como conjunto de atividades.

Cada um destes é discutido abaixo.

Conformidade como resultado

As organizações envolvem-se em várias atividades para cumprir com as leis, regras, políticas, códigos, etc., ou para "estar em conformidade". Atingir certos requisitos e expectativas de conformidade costuma ser uma condição necessária para operar e buscar o atingimento de objetivos estratégicos.

Conformidade como categoria de risco

O Framework Internacional de Práticas Profissionais define risco como *a possibilidade de um evento ocorrer, o que afetará o atingimento dos objetivos de uma organização*. Esses impactos podem ser favoráveis ou adversos. Portanto, ao avaliar o risco, é essencial considerar os requisitos e expectativas de conformidade, juntamente com a probabilidade de não conformidade e seu impacto potencial sobre os objetivos.

Existem riscos para as organizações quanto à conformidade e à não conformidade. Seus impactos podem ser na forma de recompensas ou penalidades, que podem ser tangíveis ou intangíveis. A conformidade com as normas da *International Organization for Standardization* (ISO), por exemplo, é projetada para criar eficiências operacionais e outros ganhos, e a atenção favorável obtida por seguir um código voluntário. O descumprimento elimina esses ganhos positivos e pode resultar diretamente em danos, bem como incorrer em penalidades, como imposição de multas, retirada de licenças, sanções, encerramento de operações, processo civil ou criminal e perda de financiamento ou suporte. Além disso, o descumprimento pode causar risco de reputação, na forma de potencial insatisfação dos stakeholders, crítica pública ou outros danos.

A identificação, mensuração e avaliação do risco de conformidade, e a determinação do apetite e tolerâncias ao risco de conformidade ajudam a determinar as respostas apropriadas, incluindo políticas, procedimentos, limites e controles.[6]

Conformidade como papel ou departamento organizacional

Frequentemente, a conformidade também é usada para se referir a uma função ou departamento estabelecido para atender a requisitos e expectativas específicos ou fornecer supervisão, experiência, verificação e questionamento, monitoramento, teste ou garantia em questões relacionadas à

---

[4] Na ampla categoria de risco de conformidade em uma organização, uma taxonomia de risco identifica uma cascata de subcategorias que tratam tanto de riscos específicos quanto de riscos relacionados quanto a leis, regras, regulamentos, políticas ou comportamentos.

[5] Os papéis podem ser definidos com base na cobertura de riscos específicos, como executivo de risco de conduta, executivo de risco de proteção dos dados, etc.

[6] O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) oferece frameworks para gerenciamento de riscos e liderança criativa, incluindo novas orientações sobre a aplicação do framework de riscos de ERM ao gerenciamento de riscos de conformidade.

conformidade. Essas são características de várias funções de primeira ou segunda linha, conforme descrito no *Modelo das Três Linhas*, permanecendo dentro da alçada e responsabilidades gerais da gestão e, dependendo das características específicas da função, potencialmente oferecendo suporte especializado e gerenciamento de riscos àqueles com papéis de primeira linha e executivos seniores.

Sujeito aos requisitos legais e regulatórios e à indústria, tamanho e complexidade da organização, uma função de conformidade sênior, dependendo de suas responsabilidades específicas, pode reportar a uma de várias funções diferentes na organização. Elas incluem a alta administração executiva (por exemplo, o diretor executivo, o diretor de risco, o diretor operacional, o conselho geral ou outros), suas respectivas cadeias de gestão e/ou diretamente ao órgão de governança ou subcomitê designado. Em certos casos, novamente sujeito aos fatores identificados acima e a um mecanismo para garantir a independência da função de auditoria interna, uma função ou departamento de conformidade pode reportar ao chefe executivo de auditoria (CAE) ou a um indivíduo que supervisione tanto o departamento de conformidade quanto o departamento de auditoria interna. Os Seis Princípios descritos no *Modelo das Três Linhas* devem ser aplicados para avaliar o alinhamento das responsabilidades de cada função para a conformidade com os requisitos e expectativas. Conforme descrito no modelo, ações de mitigação devem ser tomadas se um alinhamento apresentar um potencial conflito de interesses ou prejuízo à objetividade ou independência. O conflito ou prejuízo à objetividade, real ou potencial, também deve ser reportado ao órgão de governança para consideração e possíveis ações, incluindo notificação ao regulador, quando aplicável.

Conformidade como conjunto de atividades

A conformidade pode se referir aos processos e controles desenvolvidos para alcançar, apoiar, monitorar, vigiar, verificar, testar, questionar ou confirmar a conformidade. Os indivíduos que executam essas medidas ajudam a garantir que a organização e seus membros cumpram com os requisitos e expectativas.

A conformidade em uma organização é alcançada por meio das ações e dos comportamentos de todos que trabalham para ou com a organização, adequados à sua função e senioridade.

A responsabilidade por processos de rotina, procedimentos e controles desenvolvidos para cumprir com requisitos e expectativas específicos em um determinado nível e com um grau aceitável de certeza pode estar presente em vários lugares da organização e pode ser terceirizada. O *Modelo das Três Linhas* estabelece que um elemento principal na avaliação do alinhamento é a identificação dos direitos de decisão relacionados às atividades de conformidade. (Veja os papéis e atividades detalhados que abrangem a conformidade na seção Anexo.)

O Modelo das Três Linhas

Conformidade

O órgão de governança é, em última instância, responsável pela governança, que é alcançada por meio das ações e comportamentos do órgão, bem como pela gestão e auditoria interna.[7]

Conforme cada organização atribui responsabilidades pelos aspectos de conformidade de acordo com suas próprias circunstâncias, sujeita a quaisquer requisitos externos prescritos, ela deve analisar o quão bem as funções e responsabilidades específicas atribuídas em toda a organização estão alinhadas aos Seis Princípios do *Modelo das Três Linhas.* A análise pode mostrar que algumas responsabilidades estão alinhadas aos papéis do órgão de governança; algumas aos papéis de gestão, incluindo conformidade e gerenciamento de riscos; e outras aos papéis da auditoria interna.

Os papéis da primeira linha incluem fornecer produtos e serviços a clientes ou consumidores, e fornecer o suporte necessário para fazê-lo em conformidade com os requisitos e expectativas. Os papéis da segunda linha fornecem supervisão e assessoria especializadas, avaliam os riscos (especialmente em uma base coletiva ou de portfólio) e executam atividades de gerenciamento de riscos (incluindo monitoramento, vigilância e teste), questionando com credibilidade a primeira linha. O papel de terceira linha da auditoria interna é prestar avaliação independente, incluindo a avaliação de quão bem a segunda linha questiona a primeira linha com credibilidade. Juntos, eles precisam trabalhar de forma eficaz por meio da coordenação, comunicação e colaboração adequadas, para garantir que suas atividades estejam alinhadas de maneira adequada, sem sobreposição, duplicação e lacunas indevidas, e sem conflito ou incompatibilidade.

O gráfico usado para representar o modelo não identifica uma função ou departamento de conformidade, nem outras funções, departamentos ou responsabilidades específicas de segunda linha. Ele descreve os relacionamentos entre as funções centrais de governança, em oposição a uma estrutura organizacional prescrita.

Determinando a responsabilidade pelos papéis e atividades de conformidade

Prestação de contas, ações e avaliação são os ingredientes essenciais da governança. O estabelecimento e as características de departamentos especializados em gerenciamento de riscos, conformidade, ética, sustentabilidade, segurança, privacidade de dados, assessoria jurídica, controle financeiro e assim por diante dependem de muitos fatores. Eles incluem complexidade organizacional, tamanho, setor, recursos, regulamentação, legislação e cultura, tolerância/apetite a risco do órgão de governança e, o que é mais

[7] As estruturas dos órgãos reguladores variam de acordo com a jurisdição, os requisitos regulatórios e a composição de cada instituição. Quando nos referimos a órgãos de governança, incluímos uma ampla gama de estruturas de órgãos de governança encontrados em várias jurisdições e indústrias, e nos setores público e privado. As seguintes responsabilidades do órgão de governança podem ser aplicadas: definir o direcionamento da organização; definição de visão, missão, valores e apetite a risco; e receber relatórios da gestão sobre os resultados planejados, reais e esperados, e sobre os riscos e gerenciamento de riscos.

importante, os objetivos e responsabilidades das funções dentro do respectivo departamento especializado.

Sujeitas a mandatos regulatórios específicos em certas indústrias, as organizações podem não ter um departamento de conformidade designado separado. Muitas não têm, nem podem ter indivíduos cujos títulos ou descrições de funções incluam conformidade.

No entanto, mesmo sem uma função ou departamento de conformidade designado, as organizações ainda podem ter uma governança eficaz e cumprir com os requisitos e expectativas, desde que atribuam funções e responsabilidades, proporcionais à organização, para atingir a conformidade com os requisitos e expectativas aplicáveis, e desde que os indivíduos cumpram com suas funções definidas.

Normalmente, conforme as organizações se tornam maiores, mais complexas, ricas em recursos ou altamente regulamentadas, elas podem decidir ou ser obrigadas a atribuir responsabilidades e recursos separados a papéis e departamentos individuais para vários aspectos de conformidade.

Além disso, um funcionário pode ser responsável por mais de um papel. Nesse caso, deve haver uma avaliação adequada da compatibilidade desses múltiplos papéis, e uma definição clara das responsabilidades de cada papel e da supervisão e avaliação do desempenho desses papéis. Em certos casos, pode ser necessária a aprovação do órgão de governança e do regulador.

Com múltiplos papéis, pode haver maior risco de incompatibilidade, conflito de interesses e menor clareza sobre prestação de contas e responsabilidade. A mitigação pode ser necessária para permanecer dentro do apetite a risco, juntamente com o reporte ao órgão de governança e regulador, quando aplicável.

Um esforço coletivo para atingir a conformidade

Mesmo onde houver uma função ou departamento de conformidade designado, é importante reconhecer que todas as atividades de conformidade não residem em apenas um lugar dentro da estrutura de uma organização. Funcionários em todos os níveis, bem como diretores executivos e não executivos, são obrigados a contribuir para o esforço coletivo de conformidade. Responsabilidade e prestação de contas são distribuídas por toda a hierarquia da organização, funções definidas e estrutura de gestão de linha para atingir a conformidade, mitigar os riscos de conformidade e monitorar a conformidade com os requisitos e expectativas.

A conformidade com os requisitos e expectativas externos e internos geralmente é tratada por departamentos especializados ou indivíduos fora de um departamento de conformidade designado. Seus respectivos papéis e responsabilidades podem ser definidos de forma mais restrita pelas regulamentações do setor industrial ou por um indivíduo específico ou conjunto de requisitos ou expectativas. Os exemplos podem incluir: conformidade com a legislação e regulamentos de recursos humanos (RH) tratados pelo departamento de RH e conformidade com reporte financeiro e requisitos fiscais tratados pelo departamento financeiro.

Conforme sugerido acima, diferentes funções e departamentos podem ser responsáveis por atingir a conformidade, bem como pela supervisão, monitoramento e teste de aspectos de conformidade. Como resultado, é claramente importante aplicar os Seis Princípios na identificação das características relacionadas à conformidade de um papel individual e suas responsabilidades.

A governança eficaz se beneficia da comunicação, coordenação e colaboração formal e informal e promove a transparência. No entanto, se as interações informais nas estruturas de governança e controle contornarem a identificação, escalonamento e mitigação apropriados das questões de conformidade, isso pode prejudicar a eficácia da governança formal e das estruturas de controle, e obscurecer a determinação da prestação de contas e responsabilidade.

Ao avaliar a eficácia de um modelo de governança, é essencial não avaliar apenas a estrutura formal de governança, projetada e desenvolvida para alcançar a conformidade, mas também sondar a organização quanto a linhas informais de comunicação, tomada de decisão e ação, para identificar se, onde e quando a estrutura informal de governança prejudica ou frustra a formal. Fortes interações formais e informais para promover a comunicação, coordenação e colaboração são encorajadas no *Modelo das Três Linhas*. No entanto, uma estrutura informal de governança pode bloquear a conformidade, contornar controles e resultar no gerenciamento ineficaz do risco de conformidade, além de obscurecer a clareza da responsabilidade e prestação de contas. A aplicação do *Modelo das Três Linhas* para identificar papéis, responsabilidades e ações permite que as organizações desenvolvam uma estrutura de governança eficaz, incluindo o desenvolvimento de salvaguardas para mitigar os riscos dos processos informais de governança, tomada de decisões e ações que possam levar a falhas de conformidade.

Um programa eficaz de conformidade não só conduzirá à adoção e adesão a uma estrutura formal de governança e controle documentada, mas também será um elemento essencial no desenvolvimento e manutenção de uma cultura de conformidade e controle, facilitando a eficácia do *Modelo das Três Linhas*.

Aplicando os Seis Princípios

O *Modelo das Três Linhas* incentiva uma abordagem baseada em princípios para avaliar e alinhar papéis e responsabilidades, levando em consideração as circunstâncias de uma organização, incluindo seus requisitos e expectativas de conformidade específicos. Os Seis Princípios do modelo podem ser usados para entender melhor a conformidade — como resultado, categoria de risco, função ou departamento, e como conjunto de atividades — e sua contribuição para um framework bem-sucedido de governança. (Para a linguagem completa dos Seis Princípios, consulte o *Modelo das Três Linhas*.)

Princípio 1: Estabelecer requisitos de governança

O Princípio 1 descreve os requisitos mínimos de governança como:

- Prestação de contas (pelo órgão de governança aos stakeholders, para o sucesso).
- Ações e aplicação de recursos (pela gestão, para atingir metas – inclui o gerenciamento de riscos e conformidade).
- Avaliação e assessoria (de uma função de auditoria interna independente em todos os aspectos, para permitir supervisão e transparência eficazes e para promover confiança e melhoria contínua).

O órgão de governança é, em última instância, responsável por garantir que a organização se comporte de acordo com os padrões aceitos e as normas sociais. A gestão deve gerenciar os riscos associados à conformidade e não conformidade, de acordo com o apetite expresso pelo órgão de governança. Isso pode incluir o estabelecimento de papéis e equipes individuais com foco específico nos aspectos de conformidade, e definir claramente os direitos de decisão entre a primeira linha, que tem propriedade dos riscos, e a segunda linha em apresentar questionamento confiável e em impulsionar a conformidade da primeira linha com o apetite a risco. A auditoria interna oferece avaliação à gestão e ao órgão de governança sobre a adequação e eficácia dos controles de conformidade, e assessoria para melhoria contínua e inovação.

Ilustrações Práticas de Campo

> **A saúde é um setor altamente regulamentado e, como tal, a prestação de quase todos os serviços envolve a conformidade com alguma regra, regulamento ou norma. Enfermeiros, médicos e outros clínicos devem garantir que todos os serviços prestados sejam devidamente autorizados e documentados. Aqueles com responsabilidades de conformidade (funções individuais ou um departamento) podem aconselhar os departamentos clínicos sobre os requisitos de documentação e autorização de um determinado procedimento, mas, em última análise, os cuidadores de primeira linha são responsáveis por implantar os processos, controles e garantir a conformidade com esses requisitos.**
>
> – Diretor de Compliance e Auditoria Interna, Estados Unidos

> **Um exemplo da minha indústria é a classificação dos principais riscos de conformidade para a organização e requisitos regulatórios, e o alinhamento de atividades, controles, monitoramento e responsabilidades para cumprir com os requisitos regulatórios e em proporção a esses riscos. Por exemplo, uma organização pode ter um diretor de conformidade**

contra lavagem de dinheiro, diretor de privacidade, diretor antissuborno e corrupção, etc., em linha com os requisitos regulatórios, e pode ter produto, divulgação, emprego, reclamações, etc., responsabilidades e recursos específicos para apoiar a obtenção de conformidade e de gerenciamento dessas áreas de risco essenciais. O reporte regular é feito ao órgão de governança e todas as atividades estão sujeitas a auditoria interna independente.

– Diretor de Conformidade, Reino Unido

Um bom exemplo dos desafios que as organizações enfrentam hoje é o impulso para adotar e abraçar as normas "ambientais, sociais e de governança", ou "ESG". O órgão de governança é responsável por responsabilizar a gestão pelo comportamento da organização de acordo com a estratégia, padrões e normas sociais definidos pelo órgão de governança. O ESG abrange todos os cantos da organização e cada funcionário, fornecedor e cliente. Portanto, o órgão de governança deve garantir que haja uma articulação clara por parte da gestão sobre os riscos de ESG aplicáveis à organização, as leis e regulamentos externos e as políticas internas e procedimentos, as métricas de desempenho relevantes e dados confiáveis, autênticos e comparáveis para refletir o cumprimento com a conformidade com esses requisitos e expectativas internas. Além disso, tanto a gestão quanto o órgão de governança desejarão ou precisarão de avaliação quanto ao cumprimento com os objetivos de conformidade de ESG. É necessário um mapeamento complexo de responsabilidades e prestação de contas em toda a organização, para capturar as respectivas funções e departamentos e suas atividades necessárias para adotar o ESG e demonstrar conformidade.

– Diretor de Conformidade, Estados Unidos

Princípio 2: Manter supervisão adequada de governança

O Princípio 2 define os papéis do órgão de governança para:

- Governança.
- Supervisionar a gestão.
- Estabelecer e supervisionar uma função de auditoria interna eficaz.

O órgão de governança é, em última instância, responsável pela governança e garante que haja estruturas e processos apropriados em vigor. Isso inclui disposições para conformidade, bem como a supervisão da função da auditoria interna.

O órgão de governança deve determinar o grau de confiança que tem e exige quanto ao cumprimento com os requisitos e expectativas relacionados ao nível de exposição ao risco e ao potencial de impacto sobre os objetivos estratégicos. Ao determinar seu apetite ou tolerância ao risco de conformidade, o órgão de governança supervisionará a execução das atividades da gestão e o cumprimento com as respectivas responsabilidades dos papéis e departamentos designados para alcançar os resultados de conformidade de acordo com o apetite ao risco de conformidade e tolerâncias relacionadas.

O órgão de governança deve garantir que a auditoria interna esteja devidamente posicionada e dotada de recursos para permitir que ela preste avaliação e assessoria independentes e eficazes sobre a conformidade. O CAE deve prestar contas ao órgão de governança, um comitê de auditoria independente ou comitê designado equivalente do órgão de governança, para assegurar sua autoridade e status independente.

Ilustrações Práticas de Campo

Um órgão de governança eficaz é capaz de promover mudanças e ter voz em toda a organização. Às vezes, escalonamentos e reportes são feitos naturalmente, mas isso depende de quão atualizado o órgão regulador está e da qualidade das informações, para fornecer supervisão e direção eficazes no 'agora', em vez de retrospectivamente, com base em dados históricos. A auditoria interna deve validar se o órgão regulador está obtendo visibilidade clara sobre os riscos gerenciados, a fim de antecipar, prestar supervisão e dar orientação a respeito desses riscos. A conformidade desempenha um importante papel de segunda linha ao questionar a gestão sobre a eficácia da conformidade e do controle, e ao fornecer ao órgão de governança uma visão sobre a eficácia do gerenciamento do risco de conformidade dentro do apetite a risco.

– Diretor de Conformidade, Cingapura

Na saúde e em muitos outros setores, um departamento de conformidade pode ter responsabilidade diária por certos elementos do programa de conformidade, incluindo treinamento e educação, monitoramento de canais de denúncia, promulgação de um código de ética, realização de verificações de antecedentes, etc. Algumas dessas atividades são sobre alcançar a conformidade, algumas podem ser sobre o estabelecimento de políticas, monitoramento ou reporte da eficácia da conformidade à alta administração e ao órgão de governança. O departamento de auditoria interna não pode prestar avaliação independente sobre a eficácia do programa de conformidade se o departamento de conformidade reportar ao CAE. No entanto, em tais casos, um terceiro independente pode ser contratado para prestar avaliação ao órgão de governança.

– Diretor de Conformidade e Auditoria Interna, Estados Unidos

O órgão de governança deve procurar garantir que os riscos de conformidade sejam avaliados/considerados exaustivamente no plano de auditoria interna, compreender a cobertura plurianual da auditoria interna dos principais riscos regulatórios e áreas de foco do regulador, e revisar os resultados dos relatórios/atividades relacionados à conformidade.

– Chefe Executivo de Auditoria, Reino Unido

O órgão de governança define o tom para o gerenciamento do risco de conformidade, tanto para a gestão quanto para a auditoria interna. Para que o órgão de governança seja eficaz em sua supervisão da conformidade, deve haver um exame amplo, regular e frequente das informações quantitativas e qualitativas adequadas sobre o estado da conformidade, fornecidas pela gestão e pela auditoria interna. O órgão de governança deve estabelecer, como itens da pauta permanente, a gama de atividades de gerenciamento do risco de conformidade para lidar com o gerenciamento do risco de conformidade voltado para o futuro, e não apenas o foco voltado para o passado, para eventos, sobre violações, invasões e remediação.

– Diretor de Conformidade, Reino Unido

Princípio 3: Definir funções de gerenciamento na primeira e segunda linha

O Princípio 3 descreve as funções de gestão (funções de primeira e segunda linha que podem ser combinadas ou separadas, dependendo dos recursos, objetivos, regulamentação, etc.).

As funções de primeira e segunda linha constituem a gestão. Elas refletem as responsabilidades da primeira linha para fornecer os produtos e serviços aos clientes, e a segunda linha para fornecer supervisão especializada, avaliar os riscos (especialmente em uma base coletiva ou de portfólio) e realizar atividades de gerenciamento de riscos, questionando a primeira linha com credibilidade.

Departamentos separados, como um departamento de conformidade, podem ser estabelecidos, ou o chefe do departamento ou, em organizações menores e menos complexas, um indivíduo pode ser nomeado com linhas de reporte ao órgão de governança, diretamente ou por meio de um comitê do órgão de governança. O chefe do departamento ou o indivíduo também pode reportar conjuntamente ao CEO ou a uma pessoa designada dentro da gestão. Esta linha de subordinação ou responsabilidade perante o órgão de governança pode parecer estabelecer uma maior independência para o chefe do departamento de conformidade ou indivíduo. No entanto, um aspecto fundamental da independência é a ausência de responsabilidades de tomada de decisão. Normalmente, um indivíduo em uma função de conformidade retém um grau de responsabilidade pela tomada de decisões de gestão, desde a aceitação do cliente, concessão de exceções de política, aprovação de novo produto e assim por diante. Consequentemente, uma linha de reporte a um órgão de governança ou ao comitê do órgão de governança não estabelece verdadeira independência para esse departamento, chefe de departamento ou pessoa. A auditoria interna e o CAE, para além da independência da gestão nas suas linhas de reporte, também não têm responsabilidades de tomada de decisões operacionais da gestão, o que confere um grau adicional de independência.

Consequentemente, as características das funções através das linhas podem ser articuladas da seguinte forma:

- Funções de primeira linha: alcançar a conformidade com leis, regulamentos, códigos de comportamento, políticas organizacionais, etc., no fornecimento de produtos e serviços. A conformidade continua sendo responsabilidade da gestão.
- Funções de segunda linha: funções e departamentos de conformidade individuais estabelecem frameworks, realizam supervisão, oferecem assessoria, monitoramento e vigilância, realizam testes, questionam a gestão e geralmente podem manter a tomada de decisões operacionais de gestão, poderes de propriedade de risco (por exemplo, podem incluir aceitação do cliente ou consumidor, aprovação de novo produto ou serviço, aprovação de transação, aprovação de excessos a limite, exceções de política e assim por diante).
- Funções de terceira linha: a auditoria interna presta avaliação independente sobre a conformidade, a eficácia dos esforços da gestão para atingir a conformidade e o trabalho da função ou departamento de conformidade para monitorar e fornecer supervisão e controle de gerenciamento do risco de conformidade, mas não vice-versa. A auditoria interna não tem responsabilidades de tomada de decisão de gestão e reporta de forma independente ao órgão de governança.

Utilizando o *Modelo das Três Linhas*, uma organização pode atingir o cumprimento com os requisitos e expectativas, bem como contribuir para uma governança eficaz e sustentável e combater a ilegalidade e a corrupção. A conformidade deve ser baseada na transparência, estabelecendo um padrão adequado

dentro de uma organização. Além disso, para os stakeholders externos, incluindo acionistas, órgãos governamentais, agências reguladoras e bolsas, fornecedores e a cadeia de suprimento, um programa de conformidade eficaz que promova a transparência inspira confiança na organização.

Ilustrações Práticas de Campo

As funções de primeira e segunda linha devem trabalhar juntas de forma eficaz, para identificar, gerenciar e monitorar a mitigação dos riscos de conformidade da organização. Não deve haver confiança na auditoria interna para monitorar, testar e encontrar coisas. Isso deve ser de propriedade e ser feito pelas funções de primeira e segunda linha.

– Diretor Administrativo, Estados Unidos

Uma função de conformidade deve apoiar o negócio, certificando-se de que os processos e controles estejam claramente alinhados. Existem vários casos em que uma função de conformidade, como segunda linha, oferece assessoria à empresa. Os principais indicadores de desempenho e os principais indicadores de risco apoiarão o negócio para identificar e gerenciar os riscos para a eficácia do controle.

– Diretor de Conformidade, México

Muitos setores estão sujeitos a uma miríade de regulamentos complexos. O departamento de conformidade oferece sua experiência e assessoria sobre os requisitos regulatórios ou mudanças regulatórias recentes em qualquer departamento. Por exemplo, na área da saúde, a gestão dos diversos departamentos clínicos é responsável por projetar e implantar os controles necessários para garantir a conformidade. Devido à sua experiência, o departamento de conformidade está idealmente situado para avaliar a conformidade com esses requisitos.

– Diretor de Conformidade, Estados Unidos

Um desafio importante, mas bem administrado em empresas maiores, é a propriedade e as obrigações dos requisitos e expectativas de conformidade e como são executados por aqueles em papéis ou departamentos de conformidade. Isso requer um gerenciamento de riscos muito claro e um framework de controle que tenha clareza em suas linhas de prestação de contas, funções e responsabilidades, com rotas de escalonamento eficazes por meio de governança robusta. Sem isso, a supervisão de conformidade fica embaçada e difícil de ser executada.

– Diretor de Conformidade, Reino Unido

A conformidade é responsabilidade de todos. Em setores altamente regulamentados, como o de saúde, essa responsabilidade abrange todos os cuidadores e pode incluir a conformidade com os requisitos de autorização e documentação para qualquer procedimento. Se o departamento de conformidade desenvolve as políticas, processos e controles sobre processos ou procedimentos específicos, ou tem responsabilidade de rotina pelo procedimento, não seria capaz de prestar avaliação objetiva. No entanto, oferecer assessoria e consultoria sobre os requisitos regulatórios associados a um processo ou procedimento não prejudicaria necessariamente a objetividade do departamento de conformidade.

– Chefe de Conformidade e Auditoria Interna, Estados Unidos

Princípio 4: Definir o papel da terceira linha

O Princípio 4 descreve o papel da auditoria interna como prestadora de avaliação e consultoria independentes.

O *Modelo das Três Linhas* amplifica a necessidade crítica de avaliação sobre a adequação e eficácia das respostas aos riscos, incluindo controles, como componente fundamental da governança. As respostas aos riscos e controles incluem aqueles com relação a alcançar, monitorar e fornecer supervisão de conformidade e gerenciamento do risco de conformidade. Isso é alcançado por meio da aplicação competente de processos sistemáticos e disciplinados, experiência e visão da auditoria interna, como o único prestador de avaliação da organização que é independente da gestão.

A coordenação e colaboração eficazes entre as funções de conformidade e de auditoria interna podem ser alcançadas para o benefício da organização, sem prejudicar a eficácia de cada uma no cumprimento com suas funções distintas.

Como resultado das diversas funções e responsabilidades em uma organização, podem existir outras fontes de avaliação que, em conjunto, possam oferecer uma perspectiva abrangente e plural da organização. No entanto, é importante analisar e avaliar papéis específicos e seu alinhamento de acordo com o *Modelo das Três Linhas* para avaliar a qualidade e objetividade de tal avaliação.

A auditoria interna mantém a prestação de contas ao órgão de governança e a independência quanto às responsabilidades de gestão. Isso é fundamental para compreender os papéis de avaliação e a posição distinta da auditoria interna na estrutura de governança. Se a independência da atividade de auditoria interna e a objetividade dos auditores internos forem ameaçadas, o CAE deve reportar esse prejuízo ao órgão de governança para ações corretivas.

Os auditores internos, ao avaliar a eficácia dos papéis e departamentos de conformidade, devem estar abertos à comunicação, coordenação e colaboração para alcançar a aplicação eficaz do *Modelo das Três Linhas*, e promover uma cultura de conformidade e controle.

Ilustrações Práticas de Campo

> **Um item fundamental a se observar ao avaliar o gerenciamento do risco de conformidade é a eficácia das atividades que estão sendo executadas na mitigação de problemas. É importante que haja uma avaliação de riscos sólida, sobre itens de risco de conformidade específicos, e o alinhamento das atividades em proporção a esses riscos. Caso contrário, muitas atividades podem estar em andamento sem o benefício de proteger a organização dos riscos de não conformidade.**
>
> – Chefe Executivo de Auditoria, África do Sul

> **Um desafio particular dos auditores internos é a incorporação, em seu trabalho e reporte de auditoria, da identificação explícita de casos de não conformidade: violações de leis e regulamentos, violações de políticas, normas e códigos de conduta. Para prestar tal avaliação, é necessário acesso a recursos qualificados para avaliar e reportar com eficácia a obtenção do resultado de conformidade desejado.**
>
> – Chefe Executivo de Auditoria, Reino Unido

Princípio 5: Manter a independência da terceira linha

O Princípio 5 descreve a importância da independência da auditoria interna.

A auditoria interna, como terceira linha, possui várias características que ajudam a definir sua independência. Isso inclui uma linha de reporte funcional independente ao órgão de governança ou a um comitê do órgão de governança e, o mais importante, independência em relação à tomada de decisões da gestão.

As funções de gerenciamento de riscos (incluindo as funções de gerenciamento do risco de conformidade), embora muitas vezes tenham uma linha de subordinação funcional ao órgão de governança ou a um comitê do órgão de governança, normalmente também têm, dentro de suas respectivas funções, responsabilidades de tomada de decisão da gestão, particularmente com relação a assumir, gerenciar, mitigar, controlar e reportar riscos, incluindo o risco de conformidade.

A segunda linha pode manter sua responsabilidade de oferecer o questionamento eficaz e confiável da primeira linha. No entanto, a independência da auditoria interna em relação à tomada de decisões da gestão é um diferenciador significante entre o papel de terceira linha e os papéis de segunda e primeira linhas, conforme detalhado anteriormente no Princípio 3.

Ilustrações Práticas de Campo

> **Para que a auditoria interna não entre em conflito, os auditores internos não devem ter projetado ou executado controles ou participado da tomada de decisões da gestão; seu foco é a observação, teste e avaliação, para determinar se os principais riscos são identificados e controlados conforme pretendido. Eles não devem ter viés ou expectativas preconcebidas.**
>
> – Chefe Executivo de Auditoria, Austrália

> **O principal stakeholder da auditoria interna é o órgão de governança, e a independência organizacional da auditoria interna permite que ela reporte resultados e recomendações sem filtros. Não há expectativa ou necessidade de garantir que os mecanismos de controle e aqueles que os executam sejam retratados de forma favorável. A auditoria interna tem a responsabilidade final de reportar a verdade.**
>
> – Diretor de Auditoria e Conformidade, Estados Unidos

> **As funções de segunda linha de conformidade definem políticas, aconselham as empresas a respeito da criação de controles, aconselham e analisam os apetites a risco do negócio e prestam avaliação. Os indivíduos ou departamentos de conformidade podem ter responsabilidades atribuídas para executar funções operacionais em nome da primeira linha. Nesses casos, o indivíduo ou departamento de conformidade não é totalmente independente da primeira linha. A auditoria interna é a única atividade totalmente independente, devido à sua independência em relação à tomada de decisões da gestão de primeira e segunda linha.**
>
> – Chefe de Risco Corporativo e Auditoria Interna, Estados Unidos

Princípio 6: Criar e proteger valor por meio da colaboração

O Princípio 6 descreve a importância de garantir a coordenação e colaboração entre todos esses papéis.

A governança eficaz não requer apenas a devida atribuição de responsabilidades, mas também um forte alinhamento entre as atividades por meio da coordenação, colaboração e comunicação. Os órgãos de governança contam com relatórios da gestão, auditoria interna e outros para exercer a supervisão e orientar a gestão para atingir os objetivos, gerenciar riscos e criar valor. Os papéis do órgão de governança, juntamente com os papéis da primeira, segunda e terceira linhas, contribuem coletivamente para a criação e proteção de valor, quando estão alinhadas entre si e com os interesses prioritários dos stakeholders. Consequentemente, a comunicação clara das responsabilidades de conformidade em toda a organização, direitos de decisão, obrigações de reporte, apetite a risco, taxonomias comuns, entidades ou unidades de avaliação bem definidas, reporte de desempenho e de riscos em relação aos requisitos e expectativas, e programas de teste e avaliação servem para melhorar a coordenação e colaboração.

Ilustrações Práticas de Campo

> **Uma ilustração de coordenação e colaboração é, por exemplo, a privacidade de dados. A conformidade - ou, em certas organizações, a conformidade em colaboração com o departamento jurídico - identifica os requisitos regulatórios, comunica-os à organização e garante que os processos e controles apropriados sejam implantados. As equipes de negócios (operações, TI, segurança da informação, etc.) implantam as atividades, incluindo monitoramento, escalonamento e reporte de informações conforme necessário. A equipe de segurança da informação e as equipes de conformidade monitoram as principais áreas de risco, para garantir que as equipes de negócios estejam seguindo os procedimentos, monitorando e reportando adequadamente. A auditoria interna avalia o framework de gerenciamento dos riscos relevantes, incluindo o risco de conformidade, e processos e controles relacionados realizados pelas equipes de negócios durante a auditoria dessas áreas.**
>
> – Diretor de Conformidade, Reino Unido

> **O ESG é um ótimo exemplo de coordenação e colaboração em toda a organização para atingir a conformidade com os requisitos e expectativas. As funções de primeira, segunda e terceira linhas devem trabalhar juntas, dentro de seus respectivos papéis e com a supervisão do órgão de governança, para atingir os resultados desejados de ESG. Aqueles com várias responsabilidades de conformidade trabalharão com outros na organização para atingir os objetivos de ESG da organização:**
>
> - **O órgão de governança determina a estratégia e o apetite a risco, e define o tom para a cultura e o comportamento.**
> - **A gestão integra os requisitos e expectativas de ESG à governança e às operações da organização.**
>   - **Fornece assessoria, framework e requisitos sobre o conteúdo, desenvolvimento e implantação das estruturas, sistemas e processos apropriados para o planejamento estratégico e operacional, definição de metas, coleta de dados, tomada de decisões e reporte relacionados a ESG.**

        - **Avalia os riscos associados ao cumprimento com os requisitos e normas externos de ESG, bem como das políticas e metas internas.**
        - **Desenvolve normas, frameworks, princípios ou modelos que devem ser adotados para mensurar, monitorar e reportar os impactos sobre a obtenção dos resultados de ESG.**
        - **Avalia a precisão e consistência dos dados e metodologias usadas para coletar dados utilizados no reporte de sustentabilidade e ESG.**
        - **Estabelece processos de mensuração e avaliação; definição da materialidade e listagem dos indicadores relevantes (KPIs); introdução de métodos, diretrizes e ferramentas de reporte (interno e externo).**
    - **A auditoria interna presta avaliação independente ao órgão de governança sobre as atividades acima e o cumprimento com os objetivos de ESG pela gestão, bem como sobre a conformidade do reporte da gestão com os requisitos e expectativas.**

– Diretor de Conformidade, Reino Unido

Principais Fatos Sobre Conformidade

Dez lições importantes a observar

1. Pode não haver um recurso, departamento, gerente, etc. que seja dedicado à conformidade. Nem todas as organizações podem ou precisam atribuir recursos dessa maneira. Muitas vezes, conforme as organizações se tornam mais complexas, altamente ou especificamente regulamentadas, maiores, sujeitas a um maior escrutínio, começam a operar em ambientes em rápida mudança (regulatórios, comerciais, etc.) e começam a abordar fatores semelhantes que decidem que indivíduos, equipes, sistemas e/ou outros recursos precisam ser atribuídos a aspectos de conformidade como uma divisão de trabalho e componente formal do projeto organizacional. Esses recursos podem ser externos em algumas organizações; por exemplo, por meio da terceirização de determinado monitoramento de conformidade ou experiência.

2. Ao aplicar os Seis Princípios do *Modelo das Três Linhas* para avaliar as funções relacionadas à conformidade, é útil considerar os resultados pelos quais a função é responsável:

- Atingir a conformidade com leis, regulamentos, contratos, políticas, procedimentos, códigos de conduta ou outros requisitos no fornecimento de produtos e serviços.
- Fornecimento de supervisão especializada; avaliação de riscos (particularmente em uma base coletiva ou de portfólio) e condução de atividades de gerenciamento de riscos; e questionamento com credibilidade da primeira linha, para promover e atingir a conformidade em toda a organização de acordo com os códigos de conduta ou normas, requisitos e expectativas aplicáveis.
- Fornecer uma análise sobre a adequação e eficácia do programa de conformidade.
- Fornecer questionamento especializado sobre a eficácia do programa de conformidade e seus componentes em toda a organização.

3. Uma única função ou departamento de conformidade dentro de uma organização pode não cobrir todos os assuntos relacionados à conformidade para aquela organização [8]. Em tais casos, a organização deve documentar claramente o escopo da(s) função(ões) ou departamento(s) de conformidade, bem como quais funções têm responsabilidade por outros requisitos e expectativas. Isso é tão importante para organizações menores - onde um indivíduo pode receber várias responsabilidades e papéis, e algumas responsabilidades podem ser terceirizadas - quanto para organizações maiores, onde pode haver várias funções ou departamentos encarregados de várias atividades de conformidade.

4. Um papel de conformidade ou chefe de um departamento de conformidade pode, na prática e sujeito a requisitos legais e regulatórios, reportar a um de uma série de papéis diferentes em uma organização,

[8] Ética, sustentabilidade, reporte financeiro, privacidade dos dados, recursos humanos e obrigações legais, por exemplo, podem ter seus próprios recursos, internos e/ou externos, para atingir a conformidade ou oferecer gerenciamento de riscos e supervisão adicionais quanto a componentes específicos de conformidade. Por exemplo, a evolução das questões ambientais, sociais e de governança (ESG) está causando a criação de uma série de novos papéis, responsabilidades, atividades e departamentos em várias organizações, com foco na conformidade com os aspectos abrangentes de ESG.

incluindo: alta administração executiva (por exemplo, o CEO, diretor de riscos, diretor de operações, assessor geral ou outros) e/ou o órgão de governança ou seu comitê. Em alguns casos, a conformidade, embora parte da gestão, pode reportar ao CAE. A adequação da linha de reporte pode ser determinada em parte pela avaliação das responsabilidades de acordo com o *Modelo das Três Linhas* e respectivos requisitos legais e regulatórios.

5. Um papel de conformidade ou chefe de um departamento de conformidade pode ter uma linha de reporte ou prestação de contas a um ou mais comitês do conselho, ou ao presidente de um ou mais comitês do conselho. No entanto, isso não significa independência da gestão e não substitui a necessidade de avaliação independente prestada pela auditoria interna.

6. Os papéis individuais de conformidade e departamentos de conformidade podem englobar responsabilidades que incluem, mas não se limitam a: amplo gerenciamento do risco de conformidade, monitoramento, teste, análise, avaliação, assessoria, avaliação, definição de políticas, desenvolvimento e implantação de sistemas e controles, decisões da gestão, supervisão e treinamento.

7. As funções e departamentos de conformidade também podem incluir responsabilidades que estão intimamente ou diretamente relacionadas ao fornecimento de produtos e serviços. Isso exigiria uma documentação clara das responsabilidades, autoridade e prestação de contas do papel (por exemplo, a capacidade de evitar a não conformidade no fornecimento do produto ou serviço, proibindo uma transação ou vetando uma decisão da gestão).

8. As funções de primeira e segunda linha devem ser separadas. Os membros da primeira linha devem assumir propriedade do risco que assumem, enquanto os da segunda linha devem estabelecer e supervisionar os frameworks e normas para auxiliar a primeira linha no gerenciamento dos riscos dos quais são proprietários, ao mesmo tempo oferecendo questionamento confiáveis às decisões e atividades da primeira linha. Na prática, dependendo dos requisitos jurisdicionais ou da indústria e do tamanho da organização, complexidade e outros fatores, pode haver funções combinadas. Nesse caso, uma avaliação da compatibilidade dessas funções deve ser realizada e quaisquer riscos relacionados devem ser mitigados. Isso pode exigir ajustes da composição das funções para mitigar, com eficácia, os riscos de um conjunto incompatível de atividades dentro de uma função. A responsabilidade pelo gerenciamento de riscos continua sendo parte das funções de primeira linha e está dentro do escopo da gestão.

9. Independentemente de como as organizações estruturam seus recursos dedicados às obrigações de conformidade, a gestão mantém a responsabilidade de garantir que a organização atenda aos seus requisitos e expectativas dentro dos parâmetros de apetite a risco definidos pelo órgão de governança.

10. Uma responsabilidade essencial da função de conformidade de segunda linha é a avaliação da eficácia do programa de conformidade da organização e dos esforços necessários para atingir os requisitos e expectativas de conformidade da organização.

ANEXO: Alinhando a Responsabilidade pelos Papéis e Atividades de Conformidade

As atividades de conformidade são um componente essencial da governança, gerenciamento de riscos e atividades de controle interno de uma organização. A responsabilidade pelas ações necessárias para alcançar, apoiar, verificar e confirmar a conformidade e a execução dessas responsabilidades pode ser atribuída a várias partes da organização. Os responsáveis pelas atividades de conformidade precisam definir os resultados esperados que constituem a conformidade e definir as métricas apropriadas para demonstrar a obtenção desses resultados.

As atividades que abrangem a conformidade podem incluir, mas não estão limitadas a:

- Identificar leis externas, regras, regulamentos e políticas internas, normas, procedimentos e códigos de conduta e comportamento aceitável relevantes consistentes com os objetivos organizacionais.
- Determinar a mensuração de risco apropriada para conformidade e não conformidade com leis externas, regras, regulamentos e políticas internas, normas, procedimentos e códigos de conduta e comportamento aceitável relevantes consistentes com os objetivos organizacionais.
- Realizar avaliação de riscos para conformidade com leis externas, regras, regulamentos e políticas internas, normas e procedimentos relevantes, incluindo riscos futuros e emergentes e códigos de conduta e comportamento aceitável consistentes com os objetivos organizacionais.
- Projetar, desenvolver e implantar processos e controles para atingir a conformidade com as leis externas, regras, regulamentos e políticas internas, normas, procedimentos e códigos de conduta e comportamento aceitável relevantes consistentes com os objetivos organizacionais.
- Executar, manter e gerenciar processos e controles para alcançar a conformidade com leis externas, regras, regulamentos e políticas internas, normas, procedimentos e códigos de conduta e comportamento aceitável consistentes com os objetivos organizacionais.
- Avaliar, testar e monitorar a conformidade com as leis externas, regras, regulamentos e políticas internas, normas, procedimentos e códigos de conduta e comportamento aceitável relevantes consistentes com os objetivos organizacionais.
- Oferecer questionamento confiável à gestão com relação ao risco de conformidade.
- Gerenciar e mitigar o risco de conformidade.
- Determinar casos de conformidade ou não conformidade.
- Informar e escalonar casos de não conformidade.
- Reportar a conformidade ou não conformidade de acordo com os requisitos externos e internos.
- Promover uma cultura que conduza à conformidade.

- Aumentar a conscientização por meio de comunicação, treinamento, promoção e educação.
- Prestar consultoria e assessoria sobre aspectos de conformidade.
- Estabelecer e manter um programa de ética ou denúncia de irregularidades.
- Desenvolver e fornecer treinamento, educação e conscientização sobre conformidade.
- Desempenhar as responsabilidades de intermediação regulatória entre as agências reguladoras e a organização.
- Estabelecer e manter relacionamentos com organizações profissionais e órgãos da indústria para identificar normas, códigos ou diretrizes relevantes, aos quais a organização e suas respectivas atividades devem ou podem optar por aderir, bem como facilitar a coleta e o reporte de informações de benchmarking.
- Estabelecer e manter relações de intermediação com organizações de infraestrutura da indústria que possam estabelecer e exigir conformidade com requisitos ou expectativas para usuários de infraestrutura e contrapartes.

É importante que as responsabilidades e os resultados desejados de cada papel sejam claros. Alguns desses papéis e atividades são incompatíveis com outros, como aprovação de transação, aceitação do cliente ou outra tomada de decisão de risco de negócios dentro das responsabilidades de terceira linha, conforme detalhado no . Quando é solicitado à auditoria interna que assuma tais funções, salvaguardas importantes são necessárias, incluindo o consentimento do órgão de governança ou comitê de auditoria, o uso de um terceiro para prestar avaliação independente quanto às áreas afetadas e, quando apropriado, a aprovação regulatória.

Da mesma forma, mesmo com as melhores intenções de alcançar o resultado de fornecer produtos e serviços aos clientes estando em conformidade, uma organização deve estar vigilante para identificar papéis cujas responsabilidades tenham sido projetadas tanto para atingir a conformidade no fornecimento do produto ou serviço, quanto para fornecer a supervisão e o gerenciamento do risco de conformidade de forma mais ampla. Aplicam-se os princípios básicos de segregação de deveres e independência, bem como a expectativa de mitigação dos riscos decorrentes da identificação de atividades incompatíveis em funções.

Da mesma forma, às vezes, aqueles em funções de supervisão, ao identificar lacunas ou deficiências no gerenciamento de riscos e nas atividades de controle que sustentam o fornecimento de produtos ou serviços, sofrem a tentação de expandir seu próprio escopo além da supervisão, para a execução. O inverso também pode ser verdadeiro, quando a primeira linha pode confiar demais nas funções que fornecem supervisão ou que têm responsabilidades de gerenciamento de riscos. Isso prejudica os benefícios da supervisão objetiva. Em tais casos, cabe à função de supervisão identificar, escalonar e monitorar a lacuna ou deficiência e a correção da gestão. Esses elementos devem ser alinhados e documentados de acordo com os papéis e responsabilidades de governança estabelecidos.

The Institute of Internal Auditors | Global

globaliia.org