As Três Linhas de Defesa

ASSEMBLEIA LEGISLATIVA
ESPÍRITO SANTO

Expediente

Presidente
Dep. Erick Musso

1º Secretário
Dep. Raquel Lessa

2º Secretário
Dep. Enivaldo dos Anjos

Diretor de Controle Interno
André Gomes Giori

Supervisor de Planejamento e Controle Prévio
Fábio Carneiro Passos

Equipe
Alessandra de Castro Henrique
Carlos Alberto Freitas Ribeiro
Eduardo de Queiroz França Pontes
Lígia Cunha Buzin
Valtair da Silva Santos
Otávio Augusto Costa Santos
Valdir Nicchio Netto

Diagramação
Valdir Nicchio Netto

Novembro • 2018

Apresentação

Os conceitos de governança, gestão de riscos e *compliance* decorrem de uma gestão pública cada dia mais responsiva, que assume um papel preventivo no planejamento de suas ações e na orientação de suas condutas, sempre com o objetivo de atingir a finalidade pública a que se destina.

Não é por outra razão que os conceitos de governança, gestão de riscos e *compliance* foram introduzidos no País. Tais conceitos são bem delimitados pela Instrução Normativa Conjunta do Ministério Público Federal e Controladoria Geral da União n. 01/16 MP-CGU:

> "[…] governança: combinação de processos e estruturas implantadas pela alta administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos; […]
>
> […] governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;
>
> […] gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;"

Não basta que diferentes atividades de risco e controle existam - o desafio é determinar funções específicas e coordenar com eficácia e eficiência esses grupos, de forma que não haja " lacunas" em controles, nem duplicações desnecessárias na cobertura.

Responsabilidades claras devem ser definidas para que cada grupo de profissionais de riscos e controle entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de riscos e controle da organização.
Sem uma abordagem coesa e coordenada, os recursos limitados de riscos e controle podem não ser aplicados com eficácia e os riscos significantes podem não ser identificados e gerenciados de forma apropriada.

Nos piores casos, a comunicação entre os diversos grupos de riscos e controle pode regredir a um debate contínuo para entender de quem é o trabalho de realizar tarefas específicas. O problema pode existir em qualquer organização, não

importando se é usada uma estrutura formal de gerenciamento de riscos.

Embora estruturas de gerenciamento de riscos possam identificar com eficácia os tipos de riscos que os negócios modernos devem controlar, essas estruturas, em sua maioria, não definem como responsabilidades específicas devem ser delegadas e coordenadas dentro da organização.

Felizmente, estão surgindo melhores práticas que podem ajudar as organizações a delegar e coordenar tarefas essenciais de gerenciamento de riscos com uma abordagem sistemática.

Adotado na ALES, o modelo de Três Linhas de Defesa é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais.

O modelo apresenta um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização - não importando seu tamanho ou complexidade.

Mesmo em empresas em que não haja uma estrutura ou sistema formal de gerenciamento de riscos, o modelo de Três Linhas de Defesa pode melhorar a clareza dos riscos e controles e ajudar a aumentar a eficácia dos sistemas de gerenciamento de riscos.

AS TRÊS LINHAS DE DEFESA NA ESTRUTURA DA ASSEMBLEIA LEGISLATIVA

No modelo de Três Linhas de Defesa, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa e a avaliação independente é a terceira. Cada uma dessas três “ linhas” desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

MODELO DE TRÊS LINHAS DE DEFESA

Embora os órgãos de governança e a alta administração não sejam considerados dentre as três “ linhas” desse modelo, nenhuma discussão sobre sistemas de gerenciamento de riscos estaria completa sem considerar, em primeiro lugar, os papéis essenciais dos órgãos de governança (i.e., conselho de administração e órgãos equivalentes) e da alta administração. Os órgãos de governança e a alta administração são as principais partes interessadas atendidas pelas “ linhas” e são as partes em melhor posição para ajudar a garantir que o modelo de Três Linhas de Defesa seja aplicado aos processos de gerenciamento de riscos e controle da organização.

A alta administração e os órgãos de governança têm, coletivamente, a responsabilidade e o dever de prestação de contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançar esses objetivos e o estabelecimento de estruturas e processos de governança para melhor gerenciar os riscos durante a realização desses objetivos. O modelo de Três Linhas de Defesa é implementado melhor com o apoio ativo e a orientação do órgão de governança e da alta administração da organização.

1ª LINHA DE DEFESA: GESTÃO OPERACIONAL

O modelo de Três Linhas de Defesa diferencia três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos:

- Funções que gerenciam e têm propriedade sobre riscos.
- Funções que supervisionam riscos.
- Funções que fornecem avaliações independentes.

Como primeira linha de defesa, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

A gerência operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de riscos e controle diariamente. A gerência operacional identifica, avalia, controla e mitiga os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos. Por meio de uma estrutura de responsabilidades em cascata, os gerentes do nível médio desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, por parte de seus funcionários, desses procedimentos.

A gerência operacional serve naturalmente como a primeira linha de defesa, porque os controles são desenvolvidos como sistemas e processos sob sua orientação de gestão operacional. Deve haver controles de gestão e de supervisão adequados em prática, para garantir a conformidade e para enfatizar colapsos de controle, processos inadequados e eventos inesperados.

Em 2018, quando do início do Plano Anual de Auditoria Interna 2018, forma além de analisados riscos nos setores estratégicos da 1ª linha de defesa, foram também mapeados os 103 macroprocessos (principais atividades dos setores), que serão desenvolvidos, padronizados e aprovados por Legislação Interna, dando maior confiabilidade às informações e aos procedimentos realizados na 1ª linha.

2ª LINHA DE DEFESA: FUNÇÕES DE GERENCIAMENTO DE RISCOS E CONFORMIDADE

Em um mundo perfeito, apenas uma linha de defesa talvez fosse necessária para garantir o gerenciamento eficaz dos riscos. No mundo real, no entanto, uma única linha de defesa pode, muitas vezes, se provar inadequada. A gerência estabelece diversas funções de gerenciamento de riscos e conformidade para ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa. As funções específicas vão variar entre organizações e indústrias, mas funções típicas dessa segunda linha de defesa incluem:

- Uma função (e/ou comitê) de gerenciamento de riscos que facilite e monitore a implementação de práticas eficazes de gerenciamento de riscos por parte da

gerência operacional e auxilie os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização.

- Uma função de conformidade que monitore diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade.

- Uma função de controladoria que monitore os riscos financeiros e questões de reporte financeiro.

A gerência estabelece essas funções para garantir que a primeira linha de defesa seja apropriadamente desenvolvida e posta em prática e que opere conforme intencionado. Cada uma dessas funções tem seu nível de independência em relação à primeira linha de defesa, mas são, por natureza, funções de gestão. Como funções de gestão, elas podem intervir diretamente, de modo a modificar e desenvolver o controle interno e os sistemas de riscos. Portanto, a segunda linha de defesa tem um propósito vital, mas não pode oferecer análises verdadeiramente independentes aos órgãos de governança acerca do gerenciamento de riscos e dos controles internos.

As responsabilidades dessas funções variam em sua natureza específica, mas podem incluir:

Apoiar as políticas de gestão, definir papéis e responsabilidades e estabelecer metas para implementação.

Fornecer estruturas de gerenciamento de riscos.

Identificar questões atuais e emergentes.

Identificar mudanças no apetite ao risco implícito da organização. Auxiliar a gerência a desenvolver processos e controles para gerenciar riscos e questões.

Fornecer orientações e treinamento sobre processos de gerenciamento de riscos.

Facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional. Alertar a gerência operacional para questões emergentes e para as mudanças no cenário regulatório e de riscos.

Monitorar a adequação e a eficácia do controle interno, a precisão e a integridade do reporte, a conformidade com leis e regulamentos e a resolução oportuna de deficiências.

3ªLINHA DE DEFESA: AUDITORIA INTERNA

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. Esse alto nível de independência não está disponível na segunda linha de defesa. A auditoria interna provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. O escopo dessa avaliação, que é reportada à alta administração e ao órgão de governança, normalmente cobre:

- Uma grande variedade de objetivos, incluindo a eficiência e a eficácia das operações; a salvaguarda de ativos; a confiabilidade e a integridade dos processos de reporte; e a conformidade com leis, regulamentos, políticas, procedimentos e contratos.

- Todos os elementos da estrutura de gerenciamento de riscos e controle interno, que inclui: o ambiente de controle interno; todos os elementos da estrutura de gerenciamento de riscos da organização (i.e. identificação de riscos, avaliação de riscos e resposta); informação e comunicação; e monitoramento.

  A empresa como um todo, divisões, subsidiárias, unidades de operação e funções - incluindo os processos do negócio, como vendas, produção, marketing, segurança, funções voltadas para o cliente e operações - assim como funções de suporte (ex., contabilidade de receita e despesas, recursos humanos, compras, folha de pagamento, orçamentos, gestão de infraestrutura e ativos, inventário e tecnologia da informação).

Estabelecer uma atividade profissional de auditoria interna deveria ser um requisito de governança para todas as organizações. Não é importante apenas para empresas

de grande e médio porte, mas também pode ser igualmente importante para negócios menores, já que eles podem enfrentar ambientes igualmente complexos com uma estrutura organizacional menos formal e robusta para garantir a eficácia de seus processos de governança e gerenciamento de riscos.

A auditoria interna contribui ativamente para a governança organizacional eficaz, desde que algumas condições - que promovam sua independência e profissionalismo - sejam atendidas. A melhor prática é estabelecer e manter uma função independente de auditoria interna, com uma equipe adequada e competente, que inclua:

- Atuar de acordo com as normas internacionais reconhecidas para a prática de auditoria interna.
- Reportar a um nível suficientemente alto na organização, de modo a cumprir com suas responsabilidades de forma independente.
- Ter uma linha de reporte ativa e eficaz ao órgão de governança.

AUDITORES EXTERNOS, REGULADORES E OUTROS ÓRGÃOS EXTERNOS

Auditores externos, reguladores e outros órgãos externos estão fora da estrutura da organização, mas podem desempenhar um papel importante em sua estrutura geral de governança e controle. Isso vale principalmente para indústrias regulamentadas, como a de serviços financeiros ou seguros. Os reguladores, às vezes, estabelecem requisitos com a intenção de fortalecer os controles em uma empresa e, em outras ocasiões, têm uma função independente e objetiva, para avaliar o todo ou parte da primeira, segunda ou terceira linha de defesa no que tange a esses requisitos. Quando coordenados com sucesso, os auditores externos, reguladores e outros grupos externos à organização podem ser considerados linhas adicionais de defesa, que fornecem avaliações às partes interessadas da organização, incluindo o órgão de governança e a alta administração. Considerando o escopo e objetivos específicos de suas missões, no entanto, as informações de riscos reunidas são, em geral, menos extensas do que o escopo abordado pelas três linhas internas de defesa de uma organização.

COORDENANDO AS TRÊS LINHAS DE DEFESA

Já que cada organização é única e situações específicas variam, não há uma forma " certa" de coordenar as Três Linhas de Defesa. Durante a divisão de responsabilidades específicas e a coordenação entre funções de gerenciamento de riscos, no entanto, pode ser útil ter em mente o papel inerente de cada grupo no processo de gerenciamento de riscos.

As três linhas deveriam existir, de alguma forma, em todas as organizações, não importando tamanho ou complexidade. O gerenciamento de riscos, normalmente, é mais sólido quando há três linhas de defesa separadas e claramente identificadas. No entanto, em situações excepcionais que podem surgir, especialmente em pequenas empresas, certas linhas de defesa podem ser combinadas. Por exemplo, há casos em que foi solicitado que a auditoria interna estabelecesse ou gerenciasse as atividades de gerenciamento de riscos ou conformidade. Nessas situações, a auditoria interna deve comunicar claramente ao órgão de governança e à alta administração o impacto da combinação. Se responsabilidades duplas forem delegadas a uma única pessoa ou departamento, seria apropriado considerar separar a responsabilidade por essas funções em um momento posterior para estabelecer as três linhas.

Independente de como o modelo de Três Linhas de Defesa é implementado, a alta administração e os órgãos de governança devem comunicar claramente a expectativa de que as informações sejam compartilhadas e as atividades coordenadas entre cada um dos grupos responsáveis por gerenciar os riscos e controles da organização. Segundo as Normas Internacionais para Prática Profissional de Auditoria Interna, os diretores executivos de auditoria devem "compartilhar informações e coordenar atividades com outros prestadores internos e externos de serviços de avaliação e consultoria, para assegurar a cobertura apropriada e minimizar a duplicação de esforços".

PRÁTICAS RECOMENDADAS:

- Os processos de riscos e controle devem ser estruturados de acordo com o modelo de Três Linhas de Defesa.
- Cada linha de defesa deve ser apoiada por políticas e definições de papéis apropriadas.

- Deve haver a coordenação apropriada entre as diferentes linhas de defesa para promover a eficiência e a eficácia.

- As funções de riscos e controle em operação nas diferentes linhas devem compartilhar conhecimento e informações apropriadamente, para auxiliar todas as funções a desempenhar melhor seus papéis de forma eficiente.

- As linhas de defesa não devem ser combinadas ou coordenadas de uma forma que comprometa sua eficácia.

- Em situações em que as funções de diferentes linhas forem combinadas, o órgão de governança deve ser aconselhado a respeito da estrutura e seu impacto. Em organizações que ainda não tenham uma atividade de auditoria interna estabelecida, deve-se exigir que a gerência e/ou o órgão de governança explique e divulgue às suas partes interessadas que consideraram como será obtida a avaliação adequada da eficácia das estruturas de governança, gerenciamento de riscos e controle da organização.

ASSEMBLEIA LEGISLATIVA
ESPÍRITO SANTO

Novembro/2018