COSO

Comitê das Organizações Patrocinadoras da Comissão Treadway

Governança e controles internos

ALAVANCAR O COSO NAS TRÊS LINHAS DE DEFESA

Por
The Institute of Internal Auditors®

Tradução ao Português Patrocinado pela: FLAI

Douglas J. Anderson | Gina Eubanks

Autores

The Institute of Internal Auditors

Douglas J Anderson, CIA, CPA, CRMA, CMA
Executivo Chefe de Auditoria, Consultor de Assuntos Específicos
para o Audit Executive Center® do The IIA

Gina Eubanks, CIA, CISA, CRMA, CCSA
Vice-presidente de Serviços Profissionais

Agradecimentos

Gostaríamos de reconhecer Richard J. Anderson, Richard Chambers, Sally Dix, Jim DeLoach, Hal Garyn e Paul Marshall pela ajuda e apoio na preparação deste documento.

Membros do Conselho de Administração do COSO

Prefácio

Este projeto foi patrocinado pelo Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO), cuja função é oferecer liderança ponderada através do desenvolvimento de estruturas abrangentes e orientação sobre gestão de risco corporativo, controles internos e impedimento de fraudes elaborados para primorar o desempenho e a governança organizacionais e reduzir a abrangência de fraudes nas organizações.
O COSO é uma iniciativa do setor privado patrocinado e financiado em parceria pelas seguintes organizações:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Comitê das Organizações Patrocinadoras da Comissão Treadway

www.coso.org

Governança e controles internos

ALAVANCAR O COSO NAS TRÊS LINHAS DE DEFESA

Pesquisa patrocinada pelo

COSO

Comitê das Organizações Patrocinadoras da Comissão Treadway

Julho 2015

TRADUÇÃO POR:
* Fundação Latino-Americana de Auditores Internos - FLAI
* Revisão por: PIMPAO, Fabio, CIA, CCSA, CRMA

Índice

	Página
Introdução	1
Sumário Executivo	1
I. Modelo das três linhas de defesa	2
Funções da Alta Administração e do conselho de administração no Modelo das três linhas de defesa	4
A primeira linha de defesa: Administração	5
A segunda linha de defesa: Áreas de GRC (Governança, Risco e *Compliance*)	6
A terceira linha de defesa: Auditoria Interna	7
Auditores externos, responsáveis por regulamentações e outros órgãos externos	9
II. Estruturação e coordenação das três linhas de defesa	10
Estruturação das três linhas de defesa	10
Coordenação das três linhas de defesa	11
III. Alavancar o COSO nas três linhas de defesa	13
IV. Conclusão	14
Principais observações	14
Anexo	15
Sobre os autores	23
Sobre o COSO	24
Sobre o The IIA	24

Gráficos fornecidos do documento *The Three Lines of Defense in Effective Risk Management and Control*, The Institute of Internal Auditors, Janeiro de 2013.

Introdução

Este documento é uma colaboração entre o Comitê das Organizações Patrocinadoras (COSO) e o The Institute of Internal Auditors, Inc. O objetivo deste documento é ajudar as organizações a aprimorarem suas estruturas gerais de governança ao prestar orientações sobre como articular e atribuir funções e responsabilidades específicas com relação aos controles internos relacionando a — *Estrutura Integrada de Controles Internos do COSO* [1] ao Modelo das 3 Linhas de Defesa.[2]

Sumário Executivo

Toda organização tem objetivos os quais ela se empenha para atingir. Em busca desses objetivos, a organização se depara com eventos e circunstâncias os quais podem ameaçar o cumprimento desses objetivos. Esses eventos e circunstâncias em potencial criam riscos os quais a organização precisa identificar, analisar, definir e resolver. Alguns riscos podem ser aceitos, em parte ou como um todo, e alguns podem ser mitigados de maneira parcial ou total até chegarem a um ponto que estejam a um nível aceitável para a organização. Há diversas maneiras de mitigar riscos, sendo um método principal a elaboração e a implementação de controles internos eficazes.

A *Estrutura Integrada de Controles Internos do COSO* – (a *Estrutura*) define os componentes, princípios e fatores necessários para a organização gerenciar com eficácia os seus riscos através da implementação de controles internos. No entanto, a organização não se pronuncia quanto a quem é responsável pelas tarefas específicas definidas a *Estrutura*. Responsabilidades claras precisam ser definidas para que cada grupo entenda a sua função ao abordar os riscos e os controles, os aspectos pelos quais são responsáveis e como coordenarão seus esforços de maneira mútua. Não deve haver "lacunas" na abordagem dos riscos e dos controles nem duplicidade desnecessária ou sem intenção dos esforços.

As três linhas de defesa (o Modelo) aborda como tarefas específicas relacionadas aos riscos e aos controles podem ser atribuídas e coordenadas dentro de uma organização, independentemente do seu porte ou complexidade. Diretores e a gerência devem entender as diferenças críticas em funções e responsabilidades dessas tarefas e como elas devem ser atribuídas de maneira ideal para que a organização tenha uma maior probabilidade de atingir seus objetivos. Em específico, o Modelo esclarece a diferença e a relação entre as atividades de avaliação e outras atividades de monitoramento das organizações; atividades que podem ser mal interpretadas se não estiverem claramente definidas.

Dando prosseguimento, é nossa intenção discorrer com a *Estrutura* e o Modelo com o pressuposto que o leitor já tenha obtido um entendimento básico da *Estrutura*. Para quem não está familiarizado com a Estrutura, mais informações estão disponíveis no site COSO.org. O Modelo está descrito em mais detalhes na **Seção I**, mais adiante neste documento.

Figura 1. Relação entre objetivos, a Estrutura e o Modelo

[1] *Estrutura Integrada de Controles Internos,* Comitê das Organizações Patrocinadoras da Comissão Treadway (Jersey City, New Jersey: American Institute of Certified Public Accountants, Maio 2013. Disponível no site coso.org).

[2] *The Three Lines of Defense in Effective Risk Management and Control,* (Altamonte Springs, Flórida: The Institute of Internal Auditors Inc., Janeiro 2013). Disponível em: 3LinesofDefenseinEffectiveRiskManagementandControl.

I. Modelo das Três Linhas de Defesa

O Modelo apresenta mais entendimento do controle e de gestão dos riscos ao esclarecer as funções e as tarefas. O Modelo parte da premissa que, sob a supervisão e a orientação da Alta Administração e do conselho de administração[3], três grupos distintos (ou linhas de defesa) dentro da organização sejam necessários para a gestão dos riscos e o controle. As responsabilidades de cada um dos grupos (ou linhas) são as seguintes:

1. **Responsabilizar-se e gerenciar** riscos e controles (gerência operacional de 1° e 2° níveis).

2. **Monitorar** riscos e controles em apoio à gerência (funções de risco, controle e *compliance* implementadas pela gerência).

3. **Apresentar avaliação independente** ao conselho e à Alta Administração a respeito da eficácia da gestão de riscos e controles (Auditoria Interna).

Cada uma das três linhas desempenha uma função distinta dentro da estrutura de governança mais abrangente da organização. Quando cada linha desempenha sua respectiva função atribuída com eficácia, há mais probabilidade de a organização ter êxito para atingir seus objetivos gerais.

Cada indivíduo em uma organização tem certa responsabilidade pelos controles internos, mas para ajudar a garantir que as tarefas essenciais sejam realizadas conforme planejado, o Modelo esclarece funções e responsabilidades específicas. Quando uma organização estrutura adequadamente as três linhas, e elas operam com eficácia, não deve haver nenhuma "lacuna" na cobertura, nenhuma duplicidade desnecessária de esforços e os riscos e controles têm maior probabilidade de serem gerenciados com eficácia. O Conselho de Administração tem maior oportunidade de receber informações imparciais a respeito dos riscos mais significativos da organização e sobre como a gerência está respondendo a esses riscos.

O Modelo apresenta uma estrutura flexível que pode ser implementada em apoio à *Estrutura*. As funções de acordo com cada uma das linhas de defesa variam de acordo com a organização, e algumas funções podem ser combinadas ou divididas nas linhas de defesa. Por exemplo, em algumas organizações, partes de uma função de *compliance* na segunda linha podem estar envolvidas na elaboração de controles para a primeira linha, enquanto outras partes da segunda linha focam primariamente no monitoramento desses controles.

Figura 2. Três linhas de defesa

Baseado no The Three Lines of Defense in Effective Risk Management and Control, The Institute of Internal Auditors, Janeiro de 2013.

[3] Condizente com outras publicações do COSO, este documento utiliza o termo "conselho de administração" para se referir a órgãos dirigentes, tais como diretorias, conselho de fiduciários, sócios gerais, proprietários ou conselhos de supervisão.

Independentemente da maneira pela qual uma organização específica estrutura suas três linhas de defesa, há alguns princípios críticos implícitos no Modelo:

1. A primeira linha de defesa compreende o negócio e os responsáveis por processos cujas atividades criam e/ou gerenciam os riscos que podem facilitar ou impedir que os objetivos de uma organização sejam cumpridos. Isso inclui assumir os riscos certos. A primeira linha é responsável pelos riscos e pela elaboração e execução dos controles da organização para responder a esses riscos.

2. A segunda linha é implementada para respaldar a gerência ao oferecer especialização, excelência em processos e monitoramento da gestão, juntamente com a primeira linha, para ajudar a garantir que os riscos e os controles sejam gerenciados com eficácia. As funções da segunda linha de defesa são separadas da primeira linha de defesa, mas continuam sob o controle e a orientação da Alta Administração e geralmente desempenham algumas funções de gerência. A segunda linha é essencialmente uma função de gerência e/ou de supervisão responsável por muitos aspectos da gestão de riscos.

3. A terceira linha apresenta à Alta Administração e ao Conselho de Administração uma avaliação de que os esforços da primeira e da segunda linhas são condizentes com as expectativas do Conselho de Administração e da Alta Administração. A terceira linha de defesa geralmente não tem permissão para desempenhar funções de gerência para proteger sua objetividade e independência organizacional. Além disso, a terceira linha possui uma linha de subordinação principal em relação ao conselho. Sendo assim, a terceira linha é uma função de avaliação, não de gerência, o que a distingue da segunda linha de defesa.

O objetivo de toda organização é atingir seus objetivos. Atingir esses objetivos envolve aceitar oportunidades, buscar o crescimento, assumir riscos e gerenciá-los – tudo para promover a organização. Deixar de assumir riscos apropriados e não gerenciar e controlar adequadamente os riscos assumidos pode impedir que uma organização atinja os seus objetivos. Há, e sempre haverá, tensão entre atividades para criar valor corporativo e atividades para proteger o valor corporativo. A *Estrutura* oferece uma estrutura para considerar os riscos e controles para garantir que sejam apropriados e gerenciados de maneira apropriada. O Modelo apresenta orientações sobre como uma estrutura organizacional deva ser implementada, atribuindo funções e responsabilidade às partes que aumentarão o sucesso da gerência eficaz dos riscos e controles.

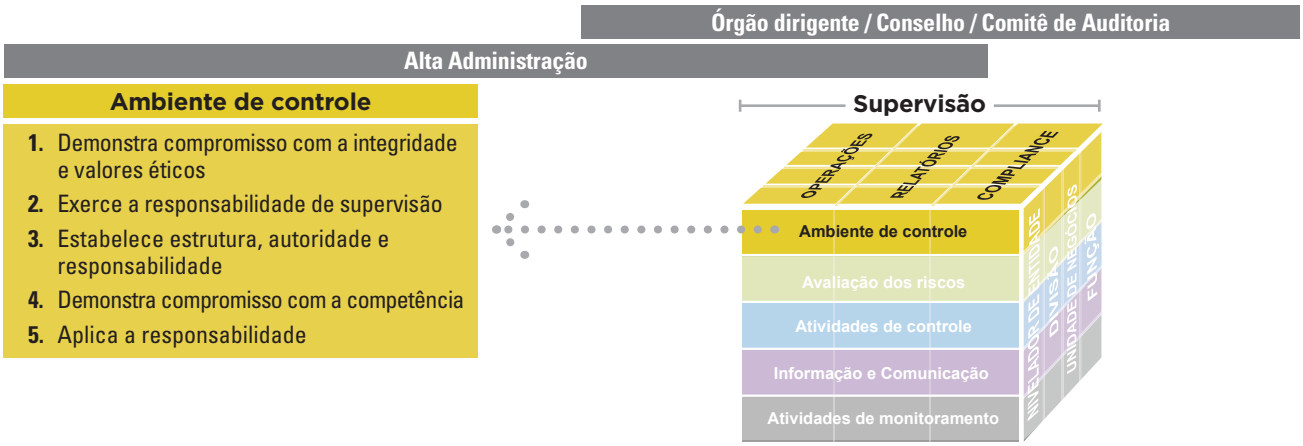
Funções da Alta Administração e do Conselho de Administração no Modelo das três linhas de defesa

A Alta Administração e o Conselho de Administração têm funções integrais no Modelo. A Alta Administração é responsável pela seleção, desenvolvimento e avaliação do sistema de controles internos com supervisão do conselho de administração. Embora nem a Alta Administração nem o Conselho de Administração seja considerada parte de uma das três linhas, essas partes, de maneira coletiva, têm a responsabilidade de estabelecer os objetivos da organização, definir estratégias de alto nível para atingir esses objetivos e estabelecer estruturas de governança para gerenciar os riscos da melhor maneira possível. Também são as partes com melhor posição para garantir a estrutura organizacional ideal para funções e responsabilidades relacionadas com riscos e controles. A Alta Administração precisa dar pleno suporte à sólida governança, à gestão de riscos e aos controles. Além disso, ela tem a responsabilidade final pelas atividades das primeira e segunda linhas de defesa. O envolvimento da Alta Administração é fundamental para o sucesso do modelo.

A *Estrutura* ajuda a esclarecer essas responsabilidades do Conselho de Administração e da Alta Administração. Como mostrado na **Figura 3** abaixo, a Alta Administração e o Conselho de Administração têm a principal responsabilidade pelo ambiente de controle de uma organização, o qual é embasado pelos cinco princípios que definem o compromisso e ética da alta gerência para a organização.

O Modelo apresenta uma estrutura sob a *Estrutura* detalhando a maneira pela qual as funções e responsabilidades são atribuídas. O Modelo é melhor implementado com o suporte ativo e a orientação do Conselho de Administração e da Alta Administração.

Figura 3. Responsabilidades de supervisão para o ambiente de controle



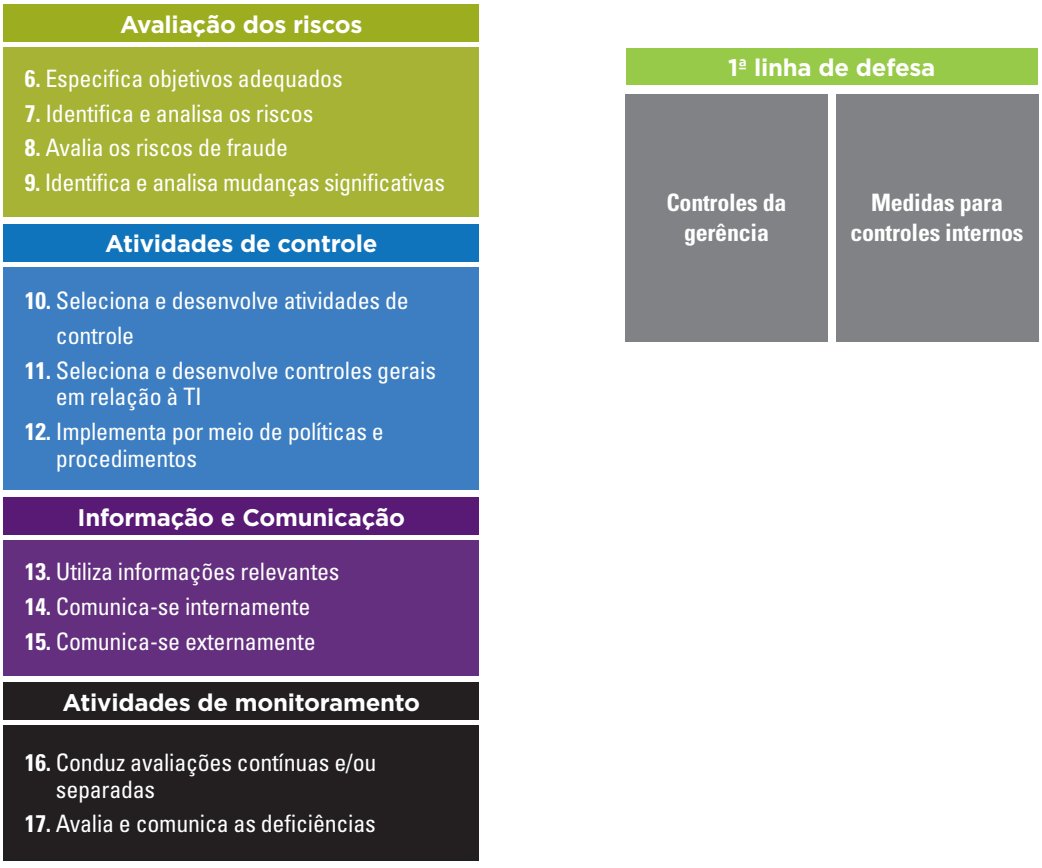
A primeira linha de defesa: Administração

A primeira linha de defesa no Modelo é principalmente tratada pelos gerentes de primeiro e segundo escalões, que têm a responsabilidade e a gerência do dia a dia dos riscos e controles. Os gerentes operacionais desenvolvem e implementam os processos de gestão de riscos e controles da organização. Esses processos incluem os processos de controles internos elaborados para identificar e avaliar riscos significativos, executar as atividades conforme o planejado, destacar processos inadequados, abordar composições dos controles e comunicar a atividade às partes interessadas. Os gerentes operacionais precisam ser adequadamente capacitados para realizar essas tarefas dentro de suas áreas de atuação.

A Alta Administração tem a responsabilidade geral por todas as atividades da primeira linha. Para determinadas áreas de alto risco, a Alta Administração também pode oferecer supervisão direta da gerência de primeiro e de segundo escalões, até mesmo ao ponto de eles mesmos desempenharem algumas das responsabilidades da primeira linha.

Os indivíduos na primeira linha de defesa têm responsabilidades significativas relacionadas com as seções Avaliação de Riscos, Atividades de Controle e Informações/Comunicação da *Estrutura*. Como indicado na **Figura 4** abaixo, os gerentes operacionais têm a principal responsabilidade pelos 12 princípios de controle interno remanescentes descritos na *Estrutura*:

Figura 4. COSO e a primeira linha de defesa



A segunda linha de defesa: Áreas de GRC (Governança, Risco e *Compliance*)

A segunda linha de defesa inclui diversas funções de gestão de riscos e *compliance* implementadas pela gerência para ajudar a garantir que os controles e processos de gestão de riscos implementados pela primeira linha de defesa sejam elaborados apropriadamente e operados conforme planejado. Estas são as funções da gerência; distintas da gerência operacional da primeira linha, mas ainda sob o controle e a orientação da Alta Administração. As funções na segunda linha são geralmente responsáveis pelo monitoramento contínuo de controles e riscos. Essas funções normalmente trabalham perto da gerência operacional para ajudar a definir a estratégia de implementação, oferecer conhecimento especializado no risco, implementar políticas e procedimentos e coletar informações para criar uma visão dos riscos e controles em toda a organização.

A formação da segunda linha pode variar de maneira significativa dependendo do porte e do setor da organização. Em organizações de grande porte, com ações negociadas em bolsas de valores, complexas e/ou altamente regulamentadas, essas funções podem ser totalmente separadas e distintas. Em organizações de porte menor, de capital privado, menos complexas e/ou menos regulamentadas, algumas das funções da segunda linha podem ser combinadas ou não existirem. Por exemplo, algumas organizações podem combinar as funções jurídicas e de *compliance* em um único departamento ou podem combinar um departamento de saúde e segurança com uma função de meio ambiente. Algumas ou todas as tarefas da segunda linha podem também ser retidas pelos gerentes dentro da primeira linha de defesa em certas organizações.

Funções comuns de segunda linha incluem grupos de conhecimento especializado, tais como:

- Gestão de riscos
- Segurança da informação
- Controle financeiro
- Segurança física
- Qualidade
- Saúde e Segurança
- Inspeção
- *Compliance*
- Jurídico
- Meio ambiente
- Cadeia de fornecimento
- Outra (dependendo das necessidades específicas do setor ou da empresa)

A formação da segunda linha pode variar de maneira significativa dependendo do porte da organização e do setor.

Sob a supervisão da gerência, a equipe de segunda linha monitora controles específicos para determinar se os controles estão condizentes com o planejado. As atividades de monitoramento realizadas pela segunda linha geralmente abrangem as três categorias de objetivos, conforme descritos pela *Estrutura*: operacional, hierárquico e *compliance*.

As responsabilidades dos indivíduos da segunda linha de defesa variam muito, mas normalmente incluem:

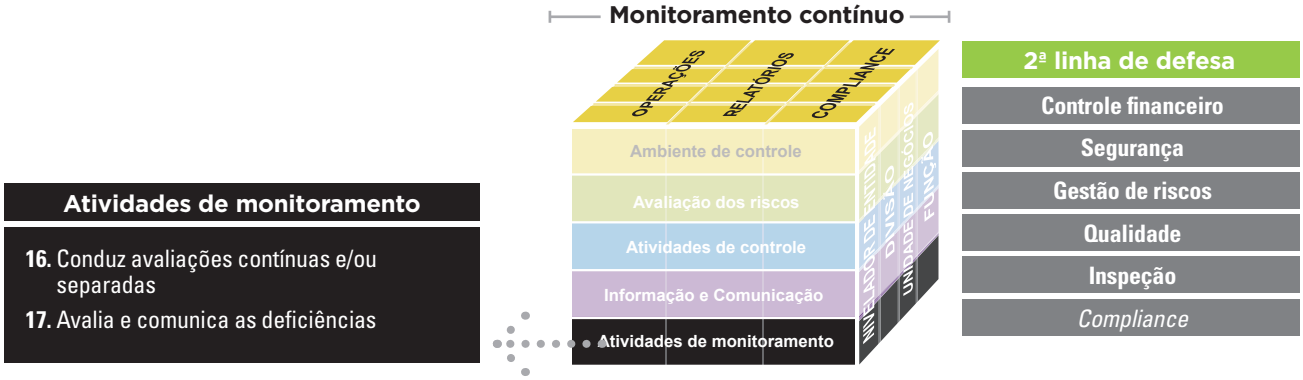
- Auxiliar a gerência na elaboração e no desenvolvimento de processos e controles para gerenciar os riscos.
- Definir atividades para monitorar e como medir o sucesso em relação à comparação com as expectativas da gerência.
- Monitorar a adequação e a eficácia das atividades de controle interno.
- Encaminhar problemas críticos, riscos emergentes e exceções.
- Apresentar estruturas para gestão dos riscos.
- Identificar e monitorar problemas conhecidos e emergentes que afetam os riscos e controles da organização.
- Identificar alterações na ambição e tolerância de risco implícitas da organização.
- Oferecer orientação e treinamento relacionados com gestão de riscos e processos de controle.

O monitoramento realizado pela segunda linha de defesa deve ser personalizado para se adequar às necessidades específicas da organização. De modo geral, essas atividades são separadas das atividades operacionais do dia a dia. Em muitos casos, as atividades de monitoramento são dispersadas por toda a organização. Em algumas organizações, no entanto, as funções de monitoramento podem ser limitadas a uma única área ou a algumas áreas.

Cada função de segunda linha tem certo grau de independência das atividades que constituem a primeira linha de defesa, mas ainda são, por natureza, atividades de gerência. As funções de segunda linha podem desenvolver, implementar e/ou modificar diretamente os processos de risco e controles internos da organização. Elas também podem assumir uma função de tomada de decisões para determinadas atividades operacionais. Até o ponto que o papel das funções de segunda linha exigir que elas estejam diretamente envolvidas em uma atividade de primeira linha, aquela função não poderá ser totalmente independente daquela atividade da primeira linha de defesa.

Embora não independente, a importância de funções de segunda linha sólidas e capacitadas não pode ser exagerada. Espera-se que essas funções operem com um grau adequado de objetividade e forneçam informações úteis e importantes à Alta Administração e ao Conselho de Administração com respeito à gestão dos riscos e controles pela primeira linha de defesa. Elas também podem fornecer informações sobre riscos e controles de toda a organização à Alta Administração e ao Conselho de Administração que não se esperariam receber da primeira linha. Para ser eficaz como uma linha de defesa, precisa ter estatura suficiente com os líderes e Administração em toda a organização. A estatura vem da autoridade e das linhas de hierarquia direta que comandam o respeito.

Figura 5. COSO e a segunda linha de defesa



A terceira linha de defesa: Auditoria Interna

Os auditores internos são como a terceira linha de defesa de uma organização. O The IIA define Auditoria Interna como uma "atividade de consultoria e avaliação objetiva e independente elaborada para agregar valor e aperfeiçoar as operações de uma organização. Ajuda a organização a atingir os seus objetivos apresentando uma abordagem sistemática e disciplinada para avaliar e aprimorar a eficácia dos processos de gestão de riscos, controles e governança".[4]

Entre outras funções, a Auditoria Interna oferece uma avaliação com relação à eficiência e eficácia de governança, gestão de riscos e controles internos. O escopo de um trabalho de auditoria é capaz de abranger todos os aspectos das operações e das atividades de uma organização.

[4] *International Professional Practices Framework (IPPF)®*, (Altamonte Springs, Flórida: The Institute of Internal Auditors Inc., 2013), 2. Também disponível em na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx.

O diferencial entre Auditoria Interna e as outras duas linhas de defesa é o seu alto nível de objetividade e independência organizacional. Os auditores internos não elaboram nem implementam controles como parte de suas responsabilidades regulares, como também não são responsáveis pelas operações da organização. Na maioria das organizações, a independência da Auditoria Interna é mais solidificada por uma relação hierárquica direta entre o executivo chefe de auditoria e o conselho de administração. Em virtude desse alto nível de independência organizacional, os auditores internos ocupam uma posição ideal para apresentar uma avaliação confiável e objetiva ao Conselho de Administração e à Alta Administração com relação à governança, riscos e controles.

Figura 6. COSO e a terceira linha de defesa

Avaliação do projeto e implementação

Ambiente de controle

1. Demonstra compromisso com a integridade e valores éticos
2. Exerce a responsabilidade de supervisão
3. Estabelece estrutura, autoridade e responsabilidade
4. Demonstra compromisso com a competência
5. Aplica a responsabilidade

Avaliação dos riscos

6. Especifica objetivos adequados
7. Identifica e analisa os riscos
8. Avalia os riscos de fraude
9. Identifica e analisa mudanças significativas

Atividades de controle

10. Seleciona e desenvolve atividades de controle
11. Seleciona e desenvolve controles gerais em relação à TI
12. Implementa por meio de políticas e procedimentos

Informação e Comunicação

13. Utiliza informações relevantes
14. Comunica-se internamente
15. Comunica-se externamente

Atividades de monitoramento

16. Conduz avaliações contínuas e/ou separadas
17. Avalia e comunica as deficiências

Avaliação da eficácia

3ª linha de defesa

Auditoria Interna

A Auditoria Interna contribui ativamente com a governança organizacional eficaz contanto que certas condições que promovem a sua independência e profissionalismo sejam atendidas. Estabelecer uma atividade de Auditoria Interna profissional deve, portanto, ser uma prioridade para todas as organizações. Essa medida é importante não apenas para organizações de maior porte, como também para as de menor porte. As organizações de menor porte podem se deparar com ambientes igualmente complexos com uma estrutura organizacional menos formal e robusta para garantir a eficácia dos processos de governança e gestão de riscos, e podem não ter uma segunda linha de defesa eficaz. Toda organização deve estabelecer e manter uma equipe de Auditoria Interna independente, adequada e competente; reportar-se a um nível suficientemente elevado na organização para conseguir realizar suas tarefas de maneira independente; e operar de acordo com um conjunto de normas apropriado e globalmente reconhecido, tal como o *International Standards for the Professional Practice of Internal Auditing* (Normas internacionais para a prática profissional de Auditoria Interna) do The IIA.

Auditores externos, responsáveis por regulamentações e outros órgãos externos

Embora as partes externas não sejam formalmente consideradas para estarem entre as três linhas de defesa de uma organização, grupos como os de auditores externos e os de responsáveis pelas regulamentações geralmente têm uma função importante com relação à estrutura de controle e governança geral de uma organização. Os responsáveis pelas regulamentações estabelecem requerimentos geralmente para solidificar a governança e os controles, e eles analisam e relatam ativamente as organizações as quais eles regulamentam. Da mesma forma, os auditores externos podem apresentar observações e avaliações importantes dos controles da organização em relação às informações financeiras prestadas e aos riscos inerentes.

Quando há uma coordenação eficaz, os auditores externos, os responsáveis pelas regulamentações e outros grupos fora da organização podem ser considerados como linhas de defesa adicionais, fornecendo importantes perspectivas e observações às partes interessadas da organização, incluindo o Conselho de Administração e a Alta Administração. No entanto, o trabalho desses grupos tem objetivos diferentes e geralmente mais focados ou simplificados, sendo assim, as áreas abordadas são menos extensas do que aquelas avaliadas pelas linhas de defesa internas da organização. Por exemplo, auditorias regulatórias específicas podem focar exclusivamente em questões de *compliance*, segurança ou outras questões de escopo limitado. Por outro lado, as três linhas de defesa têm como objetivo abordar toda a gama de riscos operacionais, hierárquicos e de *compliance* enfrentados por uma organização. Partes, como auditores externos e responsáveis pelas regulamentações, embora contribuam com informações valiosas, não devem ser consideradas como substitutos para as linhas de defesa internas já que é responsabilidade da organização gerenciar os seus respectivos riscos, não sendo essa a responsabilidade de uma parte externa.

II. Estruturação e coordenação das três linhas de defesa

Estruturação das três linhas de defesa

O Modelo das três linhas de defesa foi elaborado com a finalidade de ser flexível. Cada organização deve implementar o modelo de maneira que seja adequado para o respectivo setor, porte, estrutura operacional e abordagem à gestão de riscos. No entanto, o ambiente geral de governança e controles é normalmente mais forte quando há três linhas de defesa separadas e claramente definidas. As organizações devem se empenhar para implementar uma estrutura de governança que seja condizente com o Modelo de forma que as três linhas existam de alguma forma, independentemente do porte ou da complexidade da organização. As linhas devem ser distintas, com funções e responsabilidades separadas, claramente articuladas nas políticas e procedimentos apropriados da organização e reforçadas pelo compromisso e ética da alta gerência da organização.

O limite exato das linhas varia dependendo das necessidades específicas de cada organização. Em algumas situações, como algumas empresas de porte menor ou onde certas funções estiverem em transição, é possível que as linhas de defesa não estejam claramente separadas. Por exemplo, ao iniciarem pela primeira vez uma função de gestão de riscos, algumas organizações podem utilizar outra função como catalisadora para a implementação. Em situações nas quais as funções de distintas linhas não estiverem claramente separadas, no entanto, o Conselho de Administração deve considerar com cautela os possíveis impactos da estrutura. Quando for possível, essas situações em que não há a separação clara das linhas de defesa devem ser de curto prazo e, à medida que as funções se fortalecerem, deve-se estabelecer a devida separação. Se durarem mais do que o curto prazo ou forem temporárias, o Conselho de Administração deve entender o impacto de não separar as funções de gestão e avaliação pela falha de deixar de manter três linhas de defesa separadas.

Ao considerar ou atribuir tarefas específicas e coordenar entre as várias funções de riscos e controles da organização, recomendamos considerar a função subjacente de cada grupo no modelo.

Figura 7. Diferenças entre as três linhas de defesa

Funções da gerência		Garantia
1ª linha de defesa	2ª linha de defesa	3ª linha de defesa
Gerência operacional	Independência limitada Relatórios principalmente para a gerência	Auditoria Interna Maior independência Relatórios para o órgão dirigente

Como a objetividade e a independência organizacional são aspectos essenciais da terceira linha de defesa, deve-se ter cautela especial se a organização combina a função de Auditoria Interna com qualquer função da segunda linha de defesa. Se a função de Auditoria Interna estiver combinada com qualquer uma das funções da segunda linha, a Alta Administração e o Conselho de Administração devem se certificar de que as funções não sejam combinadas nem coordenadas de maneira que possam comprometer a objetividade ou a independência organizacional da função da Auditoria Interna. Os auditores internos normalmente não devem assumir nenhuma responsabilidade gerencial pelas operações que auditam. Nas organizações onde a Auditoria Interna estiver envolvida nas atividades da segunda linha, esse envolvimento deve geralmente ser de curto prazo com funções conflitantes alocadas para indivíduos ou grupos distintos. Se o envolvimento da Auditoria Interna com as tarefas da segunda linha não for de curto prazo, a Alta Administração e o Conselho de Administração precisam reconhecer a limitação da capacidade da Auditoria Interna de apresentar uma avaliação objetiva e independente, podendo ser necessário recorrer à partes externas para obter uma avaliação das atividades específicas afetadas.

Coordenação das três linhas de defesa

Cada uma das três linhas tem o mesmo objetivo final: ajudar a organização a atingir seus objetivos com a gestão eficaz dos riscos. As linhas atendem às mesmas partes interessadas finais e geralmente lidam com os mesmos problemas de riscos e controles. A Alta Administração e o Conselho de Administração devem comunicar com clareza a expectativa de que as informações sejam compartilhadas e as atividades coordenadas entre cada uma das três linhas onde isso respalda a eficácia geral do empenho e não diminui nenhuma das principais funções da linha. Por exemplo, muitas organizações implementaram políticas de riscos ao nível de conselho ou de gerência para articular essas expectativas.

Não se deve confundir coordenação e comunicação com estrutura organizacional. Embora tenham o mesmo objetivo, cada linha possui suas funções e responsabilidades únicas. Tratam-se de linhas separadas, porém não devem operar em silos. Elas devem compartilhar informações e coordenar esforços relacionados com riscos, controles e governança. Em muitas situações, poderá haver uma perspectiva compartilhada a respeito de controle e riscos.

É importante ter uma coordenação cautelosa para evitar a duplicidade desnecessária de esforços enquanto garantir que todos os riscos significativos sejam abordados de maneira apropriada. Essa coordenação é tão importante que, de acordo com a *Norma 2050*, os diretores executivos de auditoria são especificamente obrigados a "compartilhar informações e coordenar atividades com outros prestadores internos e externos de serviços de avaliação e consultoria para garantir a cobertura apropriada e minimizar a duplicidade de esforços".[5]

Ao operacionalizar essa coordenação, é imprescindível que os principais cargos de executivos, tais como o de diretor de riscos, diretor de *compliance* ou executivo chefe de auditoria, sejam analisados e estruturados com cautela para que cada um possa cumprir suas responsabilidades únicas enquanto coordenam e se comunicam com os outros executivos de risco e controle.

A primeira linha de defesa tem a responsabilidade principal pelos riscos e métodos utilizados para gerenciá-los. A segunda linha fornece conhecimento especializado em riscos, ajuda a definir a estratégia da implementação e auxilia na implementação de políticas e procedimentos. Embora essas duas linhas tenham responsabilidades diferentes perante os riscos e controles, é fundamental que elas trabalhem em parceria utilizando a mesma terminologia, entendam a avaliação de cada uma com relação aos riscos da organização e, sempre que possível, alavanquem um conjunto comum de ferramentas e processos.

[5] *International Professional Practices Framework (IPPF)*®, (Altamonte Springs, Flórida: The Institute of Internal Auditors Inc., 2013). Também disponível em na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx.

A função de Auditoria Interna da organização, a terceira linha de defesa, deve incluir em seu escopo todas as atividades significativas de riscos e controles da organização. A comunicação com as funções de primeira e segunda linhas de defesa ajudam a Auditoria Interna a utilizar terminologia de risco semelhante e compreender o entendimento de risco dessas duas linhas de defesa.

A Auditoria Interna também deve coordenar seus esforços com os esforços da segunda linha de defesa. Essa coordenação pode ser apresentada de várias formas dependendo da natureza da organização, do trabalho específico realizado por cada parte, da independência organizacional das funções da segunda linha e das expectativas por parte do Conselho de Administração e da Alta Administração. Em alguns casos, a Auditoria Interna consegue fundamentar parte de suas avaliações no trabalho realizado por uma função da segunda linha. Neste caso, a Auditoria Interna deve confirma se o trabalho está devidamente elaborado, planejado, supervisionado, documentado e revisado. A extensão do uso e do nível de confiabilidade no trabalho de outas funções variam de acordo com as circunstâncias específicas. A Auditoria Interna também precisa prestar atenção especial à independência organizacional das funções da segunda linha sobre as quais ela planeja fundamentar uma parte do seu trabalho de avaliação. Como a Auditoria Interna é estruturada com independência organizacional para apresentar avaliações imparciais e objetivas, a função que estiver realizando o trabalho sobre o qual a Auditoria Interna planeja se fundamentar deve demonstrar um nível suficientemente elevado de objetividade e independência organizacional. Capacidade e eficiência não são os únicos critérios. A capacidade de a primeira ou a segunda linha de defesa realizar o trabalho para a Auditoria Interna não significa que apresente um nível indispensável de independência e objetividade. De maneira semelhante, a capacidade de a Auditoria Interna realizar o trabalho da primeira ou da segunda linha não significa que a Auditoria Interna que estiver realizando o trabalho da primeira ou da segunda linha preserve necessariamente a sua independência organizacional e objetividade.

Para ajudar a estabelecer que o trabalho pode ser coordenado com eficiência, o documento da Auditoria Interna deve especificar que a Auditoria Interna tem a responsabilidade de avaliar o desempenho e a eficácia do trabalho das outras funções da segunda linha de defesa ou de qualquer atividade fornecida por um terceiro.

A extensão da coordenação pode ir além das três linhas de defesa até incluir outras partes externas, tais como auditores externos. Os auditores internos podem depender de ou utilizar o trabalho de governança, gestão de riscos e de avaliação de controles prestados por outros prestadores internos ou externos se tiverem um entendimento suficiente do trabalho realizado, dos resultados detalhados e da independência e competência da parte externa. De modo recíproco, o trabalho da Auditoria Interna pode ser intencionalmente planejado e desempenhado para cumprir as exigências das partes externas. A coordenação de esforços com partes externas pode gerar maior eficiência. No entanto, os diretores executivos de auditoria e o Conselho de Administração devem considerar os custos, bem como os possíveis benefícios de elaborar um trabalho de Auditoria Interna para o benefício das partes externas.

[7] *Making Data Governance Programs More Effective*, deloitte.wsj.com/riskand*compliance*/2014/08/04/good-riddance-to-bad-data-data-governance-gains-momentum/.

III. Alavancar o COSO nas três linhas de defesa

A *Estrutura* define cinco componentes de controle interno e 17 princípios que representam os conceitos fundamentais associados a esses componentes. A publicação do COSO, *Estrutura Integrada de Controle Interno,* define que, pelo fato de os 17 princípios serem extraídos diretamente dos cinco componentes de controle interno, pode-se obter um controle interno eficaz com a aplicação de cada um desses princípios. A gerência tem a responsabilidade de atribuir as tarefas essenciais relacionadas aos 17 princípios e confirmar que sejam desempenhadas conforme planejado.

O Anexo apresenta exemplos de como a responsabilidade pelos 17 princípios pode ser alocada entre as três linhas de defesa. *A Estrutura Integrada de Controle Interno* também identifica vários "pontos de foco" relacionados com cada um dos 17 princípios. Como muitos dos pontos de foco representam responsabilidades importantes de indivíduos dentro das três linhas de defesa, os leitores que estiverem familiarizados com a *Estrutura Integrada de Controle Interno* observarão que muitos dos pontos de foco estão indicados na seção a seguir.

As informações no Anexo têm como finalidade apresentar um exemplo de como as tarefas podem ser alocadas entre as três linhas de defesa. Como toda organização é singular, as organizações podem ter motivos plausíveis para definir funções e responsabilidades de maneiras distintas. Independentemente da maneira pela qual as tarefas são atribuídas dentro de uma organização, funções e responsabilidades específicas relacionadas a todos os 17 princípios devem ser claramente estabelecidas e comunicadas a todas as partes relevantes para mitigar lacunas na cobertura dos controles internos e duplicidade desnecessária de esforços.

IV. Conclusão

Toda organização deve definir claramente as responsabilidades relacionadas com governança, riscos e controles para ajudar a minimizar as "lacunas" em controles e duplicidades desnecessárias de tarefas atribuídas pertinentes aos riscos e controles. O Modelo de três linhas de defesa apresenta uma maneira eficaz de aprimorar as comunicações sobre riscos e controles esclarecendo funções e tarefas essenciais. O Modelo pode ser útil para esclarecer como as responsabilidades relacionadas com riscos e controles podem ser coordenadas em uma organização.

O Modelo parte da premissa que, sob a supervisão e a orientação da Alta Administração e do conselho de administração, três grupos distintos (ou linhas de defesa) são necessários para a gestão eficaz dos riscos e controles. Os três grupos:

- **São responsáveis e gerenciam** riscos e controles (gestão operacional).
- **Monitoram** riscos e controles em apoio à gerência (funções de risco, controle e *compliance* implementadas pela gerência).
- **Fornecem avaliação independente** sobre a eficácia da gestão de riscos e controles ao conselho e à Alta Administração (Auditoria Interna).

Cada uma das três linhas tem uma função distinta dentro da estrutura mais ampla de governança da organização e, quando cada uma delas desempenha sua função atribuída com eficácia, a probabilidade de uma composição significativa dos controles é reduzida. Esta estrutura também respalda o Conselho de Administração para receber informações imparciais a respeito dos riscos mais significativos da organização e sobre como a gerência está respondendo a esses riscos.

O Modelo pode ser utilizado juntamente com a *Estrutura Integrada de Controle Interno* para ajudar a garantir que os indivíduos dentro de cada linha de defesa entendam plenamente suas responsabilidades referentes a riscos e controles e como suas tarefas se adequam à estrutura geral de riscos e controles da organização.

Principais observações

1. A Alta Administração e o Conselho de Administração têm a responsabilidade definitiva de garantir a eficiência e a eficácia dos processos de governança, gestão de riscos e controles.

2. A gestão de riscos é mais solidificada quando há três linhas de defesa separadas e claramente identificadas. As três linhas de defesa devem existir em alguma forma em toda organização, independentemente do porte ou da complexidade.

3. Cada grupo dentro das três linhas de defesa deve ter funções e responsabilidades claramente definidas que sejam respaldadas por políticas, procedimentos e mecanismos hierárquicos apropriados.

4. As informações devem ser compartilhadas e as atividades coordenadas entre cada uma das linhas de defesa para aprimorar a eficiência e evitar a duplicidade de esforços enquanto garantem que todos os riscos significativos sejam apropriadamente abordados.

5. As linhas de defesa não devem ser combinadas nem coordenadas de maneira que comprometa sua eficácia. Cada linha de defesa tem uma posição singular na organização e responsabilidades únicas. Deve-se ter cautela especial se a organização combinar funções pelas três linhas de defesa. A eficácia da segunda ou da terceira linha de defesa pode ser adversamente afetada se a combinação prejudicar a singularidade da respectiva linha. Capacidade e eficiência não são os únicos critérios. Independência e objetividade também são elementos essenciais a serem considerados.

Anexo

Princípio 1 A organização demonstra compromisso com a integridade e valores éticos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
Espera-se que todas as linhas de defesa demonstrem por meio de diretivas, ações e comportamento a importância da integridade e dos valores éticos.			
• Lidera pelo exemplo na implementação de valores, uma filosofia e um estilo operacional para a organização. • Implementa objetivos, programas e atividades relacionados com a ética. • Elabora e implementa processos para avaliar o desempenho dos indivíduos e das equipes em relação às normas esperadas de conduta.	• Pode solicitar que membros da 2ª linha prestem suporte às linhas diretas de *compliance*, investiguem possíveis atitudes ilícitas ou desempenhem outras tarefas específicas relacionadas com integridade e valores éticos.	• Avalia o estado da situação ética da organização e a eficácia de suas estratégias, táticas, comunicações e outros processos para atingir o nível desejado de *compliance* jurídica e ética. • Avalia a elaboração, implementação e eficácia dos objetivos, programas e atividades da organização relacionados com ética. • Oferece garantia que os programas de ética atinjam os objetivos definidos, os principais riscos sejam gerenciados com eficácia e os controles continuem a operar com eficácia. • Presta serviços de consultoria para ajudar a organização a estabelecer um programa completo de ética e aprimorar a sua eficácia até chegar o nível desejado de desempenho.	• O conselho supervisiona o ambiente ético e garante que a gerência tenha programas e objetivos sensatos relacionados com ética. • O conselho é responsável por estabelecer "compromissos e ética eficazes por parte da alta gerência". Isso inclui a comunicação das expectativas com relação à integridade, valores éticos e normas de conduta.

Princípio 2 O Conselho de Administração demonstra independência da Administração e supervisiona o desenvolvimento e o desempenho dos controles internos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Fornece ao conselho informações adequadas sobre o desenvolvimento e o desempenho dos controles internos para capacitá-los a cumprir seus deveres fiduciários.	• A supervisão do conselho é respaldada pelas estruturas e processos que a gerência estabelece ao nível de execução dos negócios. Esse respaldo pode ser fornecido pela primeira ou pela segunda linha de defesa. Por exemplo, um comitê da gerência ou um grupo da segunda linha de defesa podem focar em assuntos como TI ou *compliance*.	• Apresenta avaliações sobre o desenvolvimento e o desempenho dos controles internos, avaliando se os controles são apropriadamente elaborados, implementados com eficácia e operacionais conforme o planejado. • Pode auxiliar o conselho sugerindo itens específicos na agenda relacionados ao Princípio 2 para serem discutidos em assembleias do conselho de administração.	• O conselho é responsável por garantir que tenha membros suficientes que sejam independentes da gerência e objetivos nas avaliações e tomadas de decisões. • O conselho tem a responsabilidade de supervisão para a elaboração, implementação e conduta dos controles internos da gerência: - **Ambiente de controle** – Estabelecer integridade e valores éticos, supervisionar estruturas, autoridade e responsabilidade, expectativa de competência e responsabilidade com o conselho. - **Avaliação dos riscos** – Envolver-se com a gerência para definir os níveis de risco. Supervisionar a avaliação que a gerência faz dos riscos para atingir os objetivos, incluindo o possível impacto de mudanças significativas, fraudes e cancelamento de controles internos por parte da gerência. - **Atividades de controle** – Oferecer supervisão à Alta Administração no desenvolvimento e desempenho das atividades de controle. - **Informação e Comunicação** – Analisar e discutir informações relacionadas com os objetivos atingidos pela organização. - **Atividades de monitoramento** – Avaliar e supervisionar a natureza e o escopo das atividades de monitoramento e a avaliação e correção que a gerência faz das deficiências. • O conselho se reúne com a Auditoria Interna e possíveis partes na segunda linha de defesa, independente da gerência.

Princípio 3 A Administração estabelece, com a supervisão do Conselho, estruturas, linhas hierárquicas e autoridades e responsabilidades apropriadas em busca dos objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Estabelece estruturas, linhas hierárquicas e autoridades e responsabilidades apropriadas em busca dos objetivos. • Comunica informações sobre estruturas, linhas hierárquicas e autoridades e responsabilidades ao conselho para capacitá-lo a cumprir suas responsabilidades de supervisão.	• Trabalha com a gerência, estruturas organizacionais, linhas hierárquicas e autoridades e responsabilidades apropriadas para eles executarem suas responsabilidades.	• Apresenta avaliação sobre a adequação e a eficácia das estruturas operacionais, linhas hierárquicas, autoridades e responsabilidades da organização em busca dos objetivos. • Implementa políticas e práticas para executar suas atividades de acordo com os seus documentos, incluindo linhas hierárquicas e autoridades apropriadas. • Confirma periodicamente ao conselho sua independência organizacional e objetividade.	• O conselho aprova os objetivos em toda a organização e é responsável pela supervisão do desenvolvimento e da manutenção das estruturas, linhas hierárquicas e atribuição de autoridades e responsabilidades apropriadas em busca dos objetivos. • O conselho emite documentos apropriados para estabelecer seus comitês, incluindo o comitê de auditoria. • O comitê de auditoria aprova documentos apropriados para as funções de riscos e controles pelas quais é responsável, incluindo Auditoria Interna.

Princípio 4 A organização demonstra um compromisso para atrair, desenvolver e manter indivíduos competentes condizentes com os objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Atrai, desenvolve e mantém indivíduos competentes condizentes com os objetivos.	• Atrai e desenvolve talentos competentes para atingir seus objetivos. • Garante que suas equipes e atividades estejam devidamente alinhadas com a gerência. Isso pode incluir o revezamento de pessoal pelas diversas funções da gerência.	• Atrai, desenvolve e mantém indivíduos competentes e capacitados para cumprir sua missão e documentação. • Pode analisar a apresentar avaliação referente à eficiência e eficácia das políticas e processos, tais como: - Políticas de recursos humanos. - Práticas de recrutamento. - Programas de treinamento e desenvolvimento. - Sistemas de avaliação de desempenho. - Planos de remuneração. - Planos de sucessão.	• O conselho supervisiona para garantir que a gerência demonstre um compromisso para atrair, desenvolver e manter indivíduos competentes condizentes com os objetivos. • Os comitês do conselho garantem que as funções as quais eles supervisionam tenham talentos competentes. • O comitê de remuneração do conselho garante que os planos de incentivo e remuneração estejam alinhados à ambição de riscos e aos objetivos de longo prazo da organização.

Princípio 5 A organização encarrega os indivíduos pelas suas responsabilidades com os controles internos no cumprimento dos objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Encarrega os indivíduos pelas suas responsabilidades com os controles internos no cumprimento dos objetivos. Essa responsabilidade inclui a comunicação de responsabilidades específicas, a implementação de sistemas de avaliação de desempenho e a implementação de processos de pessoal elaborados para responsabilizá-los pelas suas ações.	• Conforme determinação da gerência, os indivíduos da segunda linha de defesa monitoram e relatam o cumprimento de responsabilidades de controles internos específicas.	• Apresenta avaliação sobre o cumprimento de responsabilidades de controles internos específicas. • Os auditores internos podem fazer recomendações sobre responsabilidade, mas normalmente não têm autoridade direta para tomar decisões sobre ações de funcionários ou outros processos elaborados para responsabilizar os indivíduos pelas suas responsabilidades de controles internos.	• O conselho é responsável por garantir que a gerência responsabilize os indivíduos pelas suas responsabilidades de controles internos. • O comitê de remuneração do conselho garante que os planos de incentivo e remuneração estejam alinhados com os objetivos da organização.

Princípio 6 A organização especifica os objetivos com clareza suficiente para permitir a identificação e a avaliação dos riscos relacionados aos objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
Todos os indivíduos que fazem parte do sistema de controles internos precisam entender as estratégias e os objetivos gerais definidos pela organização.			
• A definição dos objetivos é uma parte importante do processo de gerenciamento relacionado ao planejamento estratégico. • Com a supervisão do conselho, define objetivos ao nível da entidade condizentes com a missão, visão e estratégias da organização. • Especifica objetivos apropriados em detalhes adequados para que os riscos para atingir os objetivos possam ser identificados e avaliados. • Aplica tolerância a riscos específicos. • Relaciona os objetivos ao nível da entidade a subobjetivos mais específicos que se propagam por toda a organização. • Os objetivos ao nível da entidade e os subobjetivos associados devem ser específicos, mensuráveis, atingíveis, relevantes e vinculados ao tempo.	• Não é responsável por definir ou aprovar objetivos ao nível de entidade como um todo, mas pode ser considerada para fazer a versão preliminar, implementar, monitorar e relatar sobre os objetivos ou subobjetivos relacionados com suas áreas específicas de conhecimento, tais como os objetivos relacionados com *compliance* ou controle de qualidade. • Avalia se a ambição e a tolerância apropriadas para os riscos são consideradas.	• Verifica se os objetivos estão implementados e se são específicos, mensuráveis ou passíveis de observação, atingíveis, relevantes e vinculados ao tempo. - Análises do processo de definição dos objetivos podem ser feitas em toda a entidade como engajamentos independentes e separados. - Objetivos ou subobjetivos específicos podem também ser analisados durante outros engajamentos de Auditoria Interna. • Para manter a independência organizacional da Auditoria Interna, os auditores normalmente não desenvolvem objetivos (a não ser aqueles específicos para a função de Auditoria Interna).	• O conselho tem a responsabilidade de supervisionar a definição dos objetivos, ajudando a garantir que os objetivos de alto nível reflitam as decisões sobre como a organização busca criar, preservar e resultar lucros para as partes interessadas. • O conselho, junto com a gerência, estabelece tolerâncias e ambições apropriadas ao risco e garante que sejam comunicados na organização.

Princípio 7 A organização identifica os riscos para atingir seus objetivos na entidade e analisa os riscos como base para determinar como eles devem ser gerenciados.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Identifica e controla os riscos relacionados com os objetivos a serem atingidos. • Define a ambição e a tolerância de riscos da organização, estabelece sistemas de gestão de riscos e estipula responsabilidades para controlar riscos específicos com a supervisão do conselho.	• Uma função de gestão de riscos corporativos pode ser atribuída para responsabilidades significativas pertinentes a riscos e controles. Tarefas comuns podem incluir: - Estabelecer uma terminologia comum sobre riscos ou um glossário. - Descrever a ambição e a tolerância da organização em relação aos riscos. - Identificar e descrever os riscos em um "inventário de riscos". - Implementar uma metodologia de classificação dos riscos para priorizar os riscos em todos os níveis das funções. - Estabelecer um comitê de riscos e/ou um diretor de riscos para coordenar determinadas atividades de outras funções de gestão de riscos. - Estabelecer a responsabilidade por riscos e respostas específicos. - Desenvolver planos de ação para garantir que os riscos sejam apropriadamente gerenciados. - Desenvolver relatórios consolidados para diversas partes interessadas. - Monitorar os resultados das providências tomadas para minimizar os riscos. - Garantir cobertura eficiente dos riscos por parte dos auditores internos, equipes de consultoria e outros órgãos de avaliação. - Desenvolver uma estrutura de gestão de riscos que permita a participação de terceiros e funcionários à distância. • Grupos específicos, como os de funções de segurança e *compliance*, podem auxiliar a gerência na identificação dos riscos relacionados com a respectiva área de especialização, levando em consideração os níveis de ambição de risco definidos pela gerência para as distintas atividades ou partes da organização.	• Leva em consideração a estrutura de risco da organização para realizar um plano de auditoria baseado em riscos em toda a organização. • Pode intermediar certas atividades de gestão de riscos corporativos, contanto que a independência e a objetividade não sejam afetadas. • Considerações para desenvolver um plano de Auditoria Interna podem incluir: - Identificação e avaliação dos riscos inerentes e residuais. - Minimização dos controles, planos de contingência e atividades de monitoramento vinculados aos riscos específicos. - Precisão e integridade dos registros de riscos. - Adequação da documentação pertinentes às atividades de risco e controle da gerência.	• O conselho estabelece a estratégia geral da organização e seus objetivos, incluindo o entendimento dos riscos associados com a estratégia. • O conselho oferece supervisão e responsabiliza a gerência pela identificação e gestão dos riscos para atingir os objetivos.

Princípio 8 A organização considera a possibilidade de fraude na avaliação dos riscos para atingir os objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Implementa processos para identificar, deter e detectar fraudes. • Analisa as exposições da organização à fraudes com os auditores internos e externos da organização.	• Garante que as avaliações dos riscos e controles incluam a consideração de risco de fraude. • Grupos, como as unidades de investigações, podem ter um papel importante para deter e detectar fraudes. Esses grupos podem ser encarregados de desenvolver e monitorar políticas e procedimentos sobre fraudes em toda a organização.	• As *Normas* exigem que os auditores internos exerçam devida cautela profissional ao considerarem a probabilidade de fraude significativo nas áreas sob análise. • Os auditores internos são obrigados a ter conhecimento suficiente para avaliar os riscos de fraude e a maneira pela qual isso é gerenciado pela organização, mas não se espera que eles tenham o conhecimento de alguém cuja responsabilidade principal seja detectar e investigar fraudes.	• O conselho é responsável pela supervisão de sistemas e procedimentos cuja finalidade seja deter e detectar fraudes. • O conselho e a Alta Administração definem as regras para prevenção e detecção de fraudes. • O conselho deve receber relatórios periódicos sobre as exposições da organização à fraudes, incluindo fraudes em relatórios financeiros.

Princípio 9 A organização identifica e avaliar mudanças que poderiam afetar de maneira significativa o sistema de controles internos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
Como a mudança pode decorrer de uma ampla gama de fontes internas e externas, os indivíduos dentro das três linhas de defesa devem ficar atentos quanto a problemas emergentes que poderiam afetar de maneira significativa o sistema de controles internos.			
• Tem a principal responsabilidade pelo sistema de controles internos e pela identificação e avaliação das mudanças que poderiam afetar de maneira significativa o sistema de controles internos. • Comunica ao conselho informações em detalhes suficientes sobre as mudanças que poderiam afetar de maneira significativa o sistema de controles internos para capacitá-lo a cumprir suas responsabilidades de supervisão.	• Pode ser solicitada a auxiliar a gerência com avaliações do impacto das mudanças no sistema de controles internos. • Precisa ser proativa para se adaptar às mudanças. • Monitora com regularidade e considera mudanças aos riscos jurídicos, regulatórios e de *compliance* da organização.	• Identifica e avalia mudanças que poderiam afetar de maneira significativa o sistema de controles internos durante as avaliações periódicas dos riscos e no decorrer do trabalho de Auditoria Interna. • Comunica-se com regularidade com a gerência para prever mudanças e o impacto na avaliação dos riscos organizacionais.	• O conselho tem a responsabilidade por garantir que a gerência tenha processos estabelecidos para permitir a identificação e a avaliação das mudanças que poderiam afetar de maneira significativa o sistema de controles internos.

Princípio 10 A organização seleciona e desenvolve atividades de controle que contribuem para a minimização dos riscos para atingir os objetivos em níveis aceitáveis.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Mantém controles internos eficazes e para executar os procedimentos de riscos e controles no dia a dia. A gerência operacional identifica, avalia, controla e minimiza os riscos, orientando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades sejam condizentes com as metas e os objetivos estabelecidos. Através de uma estrutura de responsabilidade em propagação, os gerentes de segundo escalão elaboram e implementam procedimentos detalhados que servem como controles e supervisionam a execução desses procedimentos pelos seus funcionários. • Serve naturalmente como a primeira linha de defesa porque os controles são elaborados nos sistemas e processos sob a orientação da Administração. Deve haver controles adequados de gerenciamento e supervisão implementados para garantir *compliance* e destacar as divisões dos controles, processos inadequados e eventos inesperados.	• As funções na segunda linha de defesa normalmente são responsáveis pelo monitoramento dos controles específicos em nome da gerência. • Conforme designados pela gerência, os indivíduos na segunda linha de defesa também podem participar na seleção e no desenvolvimento de controles específicos. No entanto, a gerência retém a responsabilidade pelo sistema de controles internos.	• Garante que os controles implementados pela gerência são devidamente elaborados, implementados com eficácia e operam conforme o planejado para minimizar os riscos para atingir os objetivos aos níveis aceitáveis. • Oferece sugestões com a finalidade de melhorar a eficiência e a eficácia dos controles internos. No entanto, a gerência retém a responsabilidade pelo sistema de controles internos.	• O conselho avalia as informações e supervisiona para ajudar a garantir que o sistema de controles internos da gerência esteja adequado para minimizar os riscos para atingir os objetivos aos níveis aceitáveis.

Princípio 11 A organização seleciona e desenvolve atividades de controle gerais relacionadas à tecnologia para apoiar o cumprimento dos objetivos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Elabora e implementa atividades de controle relacionadas com tecnologia. Incluem-se a criação e a comunicação de políticas e procedimentos sobre tecnologia e a garantia de que os controles de TI são adequados para apoiar o cumprimento dos objetivos. • Estabelece processos para monitorar e avaliar exposições a riscos em desenvolvimento relacionadas com tecnologias novas e emergentes.	• Os indivíduos na segunda linha de defesa geralmente recebem tarefas relacionadas com o monitoramento de controles específicos de tecnologia. • Grupos, como os departamentos de segurança da informação, também podem ter função importante na seleção, desenvolvimento e manutenção dos controles em relação à tecnologia, conforme designados pela gerência.	• Avalia se os processos de governança de TI da organização respaldam as estratégias e os objetivos da organização. • Apresenta avaliações sobre a eficiência, eficácia e integridade dos controles de tecnologia e, conforme apropriado, pode recomendar aprimoramentos às atividades de controles específicos. • Para preservar a objetividade e a independência da Auditoria Interna, os auditores internos normalmente não selecionam nem desenvolvem atividades de controles gerais em relação à tecnologia. No entanto, eles fazem recomendações sobre os controles de tecnologia. • Os auditores internos precisam ter conhecimento suficiente dos principais riscos e controles de TI para realizarem o respectivo trabalho atribuído. No entanto, não se espera que todos os auditores internos tenham o conhecimento especializado de um auditor interno cuja responsabilidade principal é a auditoria da tecnologia da informação.	• O conselho tem responsabilidades significativas de supervisão com relação à orientação, avaliação e monitoramento dos controles. A função de supervisão do conselho deve abranger aspectos de governança de TI, como: - Estruturas de governança e organização. - Liderança e suporte de nível executivo. - Planejamento estratégico e operacional. - Entrega e avaliação do serviço. - Gerenciamento dos riscos e da organização de TI.

Princípio 12 A organização aplica atividades de controle através de políticas que estabelecem o que se espera e de procedimentos que transformam as políticas em ações.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Estabelece atividades de controle que são incorporadas aos processos de negócios e às atividades cotidianas dos funcionários através de políticas que estabelecem o que se espera e de procedimentos relevantes que especificam ações. • Estabelece responsabilidade pelas atividades de controle com a gerência (ou outra equipe designada) da unidade de negócios ou da função na qual os riscos relevantes existam. • Garante que funcionários competentes com autoridade suficiente realizem as atividades de controle com diligência e foco contínuo, de maneira oportuna, conforme definido pelas políticas e procedimentos. • Garante que funcionários responsáveis investiguem e tomem providências quanto aos assuntos identificados como resultado das atividades de controle realizadas. • Revisa periodicamente atividades de controle para determinar sua relevância continuada e as atualiza conforme necessário.	• Monitora a *compliance* com políticas e procedimentos específicos, conforme designado pela gerência. • Auxilia a gerência no desenvolvimento e na comunicação das políticas e dos procedimentos. • Garante que os riscos são monitorados em relação à ambição de risco estabelecido da organização.	• Garante a elaboração e a implementação de políticas, procedimentos e outros controles. • Faz recomendações sobre políticas e procedimentos, mas normalmente não tem autoridade para elaborar ou implementar políticas e procedimentos para operações existentes fora da função de Auditoria Interna.	• O conselho supervisiona para garantir que um sistema completo de políticas e procedimentos seja implementado para orientar as operações e ajuda a garantir o cumprimento dos objetivos.

Princípio 13 A organização obtém ou gera e utiliza informações relevantes e de qualidade para respaldar o funcionamento dos controles internos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Cria e mantém dados para monitorar as atividades do dia a dia, compartilhando as informações em todos os níveis da organização. • Considera custos e benefícios, garantindo que a natureza, a quantidade e a precisão das informações comunicadas sejam comensuradas e em apoio ao cumprimento dos objetivos. • A confiabilidade e a integridade das informações é uma responsabilidade da gerência. Essa responsabilidade inclui todas as informações críticas da organização, independentemente da forma de armazenamento das mesmas. A confiabilidade e a integridade das informações incluem precisão, integralidade e segurança.	• Compila informações de toda a organização para utilizar nas atividades de monitoramento.	• Apresenta avaliação sobre confiabilidade e integridade de informações e exposições associadas ao risco. Isso inclui exposições internas e externas ao risco, e exposições pertinentes aos relacionamentos da organização com entidades externas. • Avalia periodicamente as práticas de confiabilidade e integridade das informações da organização e recomenda, conforme apropriado, melhorias ou a implementação de novos controles e proteções. Essas avaliações podem ser conduzidas como atividades separadas independentes ou integradas em outras auditorias ou atividades conduzidas como parte do plano de Auditoria Interna. • Determina se a quebra da confiabilidade e da integridade das informações e as condições que possam representar uma ameaça para a organização serão prontamente comunicadas ou não à Alta Administração, ao Conselho de Administração e à atividade de Auditoria Interna.	• A Alta Administração e o conselho utilizam as informações para tomar decisões para monitorar o sucesso da organização, prever riscos e se comunicar com as partes interessadas externas, tais como investidores. • Recebe periodicamente relatórios sobre as operações e a eficácia do sistema de controles internos da organização..

Princípio 14 A organização comunica internamente as informações, incluindo os objetivos e as responsabilidades para os controles internos, necessários para respaldar o funcionamento dos controles internos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Desenvolve e mantém processos para comunicar as informações necessárias para permitir que todos os funcionários entendam e cumpram suas respectivas responsabilidades de controles internos. • Comunica ao Conselho de Administração informações adequadas para permitir que eles exerçam suas respectivas funções com relação aos objetivos da organização. • Estabelece canais de comunicação separados, como linhas diretas para denunciar práticas inadequadas, que servem como mecanismos que minimizam falhas, permitindo a comunicação anônima ou sigilosa quando os canais comuns são ineficazes ou não estão em funcionamento.	• Monitora, compila informações e comunica informações resumidas à primeira e à terceira linha de defesa e ao Conselho de Administração a respeito de controles específicos. • Pode ser responsável por monitorar canais de comunicação separados, como as linhas diretas para denunciar práticas inadequadas.	• Apresenta avaliações relacionadas com a integridade, precisão e qualidade das comunicações de acordo com as necessidades do conselho e da Alta Administração.	• O conselho estabelece e comunica o tom que espera em toda a organização. • O conselho e a Alta Administração devem orientar sobre a natureza das comunicações esperadas dos indivíduos em cada linha de defesa.

Princípio 15 A organização comunica-se com as partes externas a respeito de assuntos que afetam o funcionamento dos controles internos.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Garante que processos sejam implementados para comunicar informações relevantes e oportunas às partes externas, incluindo acionistas, parceiros, proprietários, responsáveis pelas regulamentações, clientes, analistas financeiros e outras partes externas. • Estabelece e garante canais de comunicação aberta para permitir a opinião dos clientes, consumidores, fornecedores, auditores externos, responsáveis pelas regulamentações, analistas financeiros, entre outros, apresentando informações relevantes à Alta Administração e ao conselho de administração. • Comunica ao Conselho de Administração informações relevantes provenientes das avaliações conduzidas pelas partes externas. • Seleciona métodos de comunicação relevantes e garante que o método de comunicação considere o prazo, a audiência e a natureza da comunicação, além dos requerimentos e expectativas legais, regulatórias e fiduciárias. • Estabelece políticas apropriadas para abordar fatores como a autorização necessária para relatar informações fora da organização; diretrizes sobre informações permissíveis e não permissíveis que podem ser relatadas; indivíduos de fora autorizados a receber informações e os tipos de informações que eles podem receber; regulamentações de privacidade relacionadas; requerimentos regulatórios e considerações legais para relatar informações fora da organização; e a natureza das avaliações, conselhos, recomendações, opiniões, orientações e outras informações que podem ser incluídas na comunicação de informações fora da organização.	• Com a exceção de certas comunicações feitas aos responsáveis pelas regulamentações, auditores externos e outros grupos específicos, a segunda linha de defesa normalmente não se comunica com partes externas a respeito de assuntos que afetam o funcionamento dos controles internos. • Se a organização relatar externamente sobre os seus controles internos, as funções da segunda linha de defesa apresentam à gerência os resultados de suas respectivas atividades em respaldo às opiniões da gerência.	• Garante que as comunicações essenciais das outras partes estejam corretas. • A função de Auditoria Interna normalmente não se comunica com partes externas a respeito de assuntos que afetam o funcionamento dos controles internos.	• O conselho deve receber informações e relatórios da gerência sobre o funcionamento e a eficácia dos controles internos e a base para as opiniões da gerência antes das comunicações com as partes externas. • O conselho deve discutir com os auditores externos as perspectivas e opiniões que seriam incluídas em qualquer relatório externo acerca dos sistemas de controle da organização.

Princípio 16 A organização seleciona, desenvolve e realiza avaliações contínuas e/ou separadas para confirmar se os componentes dos controles internos estão presentes e funcionando.

1ª linha de defesa (Responsáveis do Risco/Gerentes)	2ª linha de defesa (Risco, Controle e *Compliance*)	3ª linha de defesa (Auditoria Interna)	Outro
• Seleciona e desenvolve um equilíbrio de avaliações contínuas e separadas, considerando a taxa de mudanças no negócio e nos processos de negócios e variando o escopo e a frequência das avaliações separadas dependendo do risco. (Essas avaliações podem ser realizadas pela 2ª linha de defesa.) • Garante que quem estiver realizando as avaliações contínuas e separadas tenha conhecimento suficiente para compreender o que está sendo avaliado. • O projeto e o estado atual do sistema de controles internos podem ser utilizados para estabelecer uma base para as avaliações contínuas e separadas. • Relata periodicamente ao conselho sobre o desempenho das atividades de gestão de riscos da organização.	• Realiza avaliações contínuas e separadas para monitorar o status de vários componentes do sistema de controles internos, conforme orientada pela gerência. • Realiza avaliações contínuas e separadas para monitorar se o cumprimento dos objetivos está ou não dentro das tolerâncias estabelecidas aos riscos.	• Garante que as avaliações contínuas da gerência sejam incorporadas aos processos de negócios e ajustadas às condições em mudanças, conforme apropriado. • Garante que as informações fornecidas pelas avaliações da gerência sejam imparciais e corretamente apresentadas. • Garante que o sistema de controles internos esteja operando conforme o esperado e que os riscos sejam gerenciados dentro da ambição e da tolerância aos riscos por parte da organização.	• O conselho supervisiona e responsabiliza a gerência pela seleção, desenvolvimento e realização das avaliações dos componentes dos controles internos. • Recebe relatórios periódicos sobre os riscos da organização e a eficácia de suas atividades de gestão dos riscos.

Princípio 17 A organização avalia e comunica as deficiências dos controles internos de maneira oportuna às partes responsáveis pelas medidas corretivas, incluindo a Alta Administração e o conselho de administração, conforme apropriado.			
1ª linha de defesa (Responsáveis do Risco/Gerentes)	**2ª linha de defesa** (Risco, Controle e *Compliance*)	**3ª linha de defesa** (Auditoria Interna)	**Outro**
• Comunica as informações sobre as deficiências às partes responsáveis pelas medidas corretivas e à Alta Administração e ao conselho de administração, conforme apropriado. • Acompanha se as deficiências são corrigidas de maneira oportuna.	• Os indivíduos da segunda linha de defesa podem receber a responsabilidade de monitorar e relatar sobre tipos específicos de deficiências nos controles.	• Os auditores internos estabelecem e mantêm um sistema para monitorar a disposição das descobertas na Auditoria Interna e as recomendações comunicadas à gerência. Esse sistema normalmente aborda: - O prazo dentro do qual a resposta da gerência às observações da atividade e às recomendações é necessário. - Avaliação da resposta da gerência. - Verificação da resposta (se apropriado). - Realização de uma atividade de acompanhamento (se apropriado). - Um processo de comunicação que encaminha respostas/ações insatisfatórias, incluindo a suposição de risco, aos níveis apropriados da Alta Administração ou do conselho.	• O conselho precisa garantir que recebe informações sobre as deficiências nos controles de maneira oportuna e que as medidas corretivas sejam oportunas e suficientes para abordar as deficiências significativas nos controles. • A gerência e o conselho de administração, conforme apropriado, avalia os resultados das avaliações contínuas e separadas.

Sobre os autores

Douglas J. Anderson, CIA, CPA, CRMA, CMA, é Executivo Chefe de Auditoria, Consultor de Assuntos Específicos para o Audit Executive Center® do The IIA, um programa de Residência para Executivos na Saginaw Valley State University, e presta serviços de consultoria com foco em governança, riscos e controles. Anderson tem mais de 30 anos de experiência em Auditoria Interna, auditoria externa, contabilidade e finanças. Suas responsabilidades profissionais fizeram com que viajasse pelo mundo, proporcionando a ele experiência em uma ampla gama de organizações. Anderson já ocupou diversos cargos voluntários no The Institute of Internal Auditors, incluindo o de instrutor, membro/presidente do Comitê de Orientação Vocacional e vice-presidente de Orientação Vocacional no Comitê Executivo do Conselho de Administração. Também serviu no Grupo Consultivo de Apoio da Diretoria de Supervisão de Contabilidade de Empresa Pública e é membro dos grupos de supervisão para dois projetos do COSO.

Gina Eubanks, CIA, CISA, CRMA, CCSA, é vice-presidente de Serviços Profissionais do The IIA, onde lidera os programas de Qualidade, Executivo Chefe de Auditoria e Serviços do Setor. Ela tem mais de 20 anos de experiência em Auditoria Interna, incluindo 15 anos junto a uma empresa das quatro maiores empresas de auditoria do mundo na área de serviços globais de riscos corporativos. A experiência de Gina se deu tanto nos Estados Unidos como no exterior, e passou um tempo significativo na Índia. Ela também atua e é diretora nos setores de varejo e serviços financeiros. Gina também é membro do comitê de auditoria de uma instituição financeira local e foi líder voluntária no The IIA por quase 15 anos.

Sobre o COSO

Criado originalmente em 1985, o COSO é uma iniciativa conjunta de cinco organizações do setor privado que se dedica a oferecer liderança ponderada através do desenvolvimento de estruturas e orientações sobre gestão de risco corporativo (ERM), controles internos e detecção de fraudes. As organizações que apóiam o COSO são: The Institute of Internal Auditors (IIA), American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI) e Institute of Management Accountants (IMA).

Sobre o The IIA

O The Institute of Internal Auditors (The IIA) é a defensora de causas, educadora e fornecedora de normas, orientações e certificações mais amplamente reconhecida pela profissão de Auditoria Interna. Estabelecido em 1941, o The IIA atualmente atende a mais de 180.000 membros de 170 países. A sede global da associação é em Altamonte Springs, Flórida, EUA. Para obter mais informações, acesse theiia.org.

O Audit Executive Center® do The Institute of Internal Auditors é o recurso essencial para capacitar o êxito dos Diretores Executivos de Auditoria (CAEs). O conjunto de informações, produtos e serviços do Center capacita os CAEs a responderem aos desafios singulares e aos riscos emergentes da profissão. Para obter mais informações sobre o Center, acesse theiia.org/cae.

Tradução por:
* Fundação Latino-Americana de Auditores Internos - FLAI
* Revisão por: PIMPAO, Fabio, CIA, CCSA, CRMA

COSO

Comitê das Organizações Patrocinadoras
da Comissão Treadway

www.coso.org

ALAVANCAR O COSO NAS TRÊS LINHAS DE DEFESA

COSO

Comitê das Organizações Patrocinadoras da Comissão Treadway

www.coso.org