

2020

GUIA DE BOAS PRÁTICAS DA FUNÇÃO

CONTROLES INTERNOS

FEBRABAN

Federação Brasileira de Bancos



Índice

1. INTRODUÇÃO	5
2. CONCEITOS GERAIS	7
2.1 Sistema de Controles Internos	7
2.2 Linhas de Defesa	8
3. COMPONENTES E PRÍNCIPIOS DE CONTROLES INTERNOS	12
3.1 Estrutura do COSO (2013)	12
3.2 Abordagem Baseada em Risco	14
4. ATRIBUIÇÕES OU FUNÇÕES DE CONTROLES INTERNOS	16
5. INTERAÇÃO ENTRE A ÁREA DE CONTROLES INTERNOS E AS DEMAIS ÁREAS DA INSTITUIÇÃO.	17
5.1 Áreas de Negócios e Suporte	17
5.2 Área de Compliance	17
5.3 Área de Gestão de Riscos	18
5.4 Auditoria Interna	18
5.5 Diretoria / Alta Administração	18
6. PERFIS DOS PROFISSIONAIS DE CONTROLES INTERNOS	20
7. LIMITAÇÕES DE CONTROLES INTERNOS.	21
8. GLOSSÁRIO.	22
9. REFERÊNCIAS	23
ANEXO I – Principais práticas e ferramentas relacionadas a Controles Internos	24
ANEXO II – Dicionário de tipos de controles	26

1. Introdução

O Guia de Boas Práticas de Controles Internos surge em razão da relevância do tema, do aumento de sua abrangência, da evolução do escopo de atuação das áreas de Controles Internos, bem como para possibilitar o melhor entendimento da interface entre as outras estruturas, como Gestão de Riscos, Compliance e Auditoria Interna. Foi constituído na Subcomissão de Controles Internos da Febraban um grupo de trabalho para a discussão dessas tendências e para oferecer diretrizes básicas para a atuação das áreas de Controles Internos, além de difundir conhecimentos aplicáveis e contribuir com a consecução dos objetivos da função.

Apresentaremos neste guia sugestões de práticas para a função / atuação das áreas de Controles Internos nas Instituições.

É importante ressaltar que os itens aqui abordados devem ser adaptados à natureza, ao porte, à complexidade, à estrutura, ao perfil de risco e ao modelo de negócio das operações realizadas em cada Instituição.

Marco regulatório

O Conselho Monetário Nacional emitiu em 24/09/1998, a Resolução nº 2.554 que dispõe sobre a “Implantação e Implementação de Sistema de Controles Internos”, e cita:

“§ 1º Os Controles Internos, independentemente do porte da Instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas.”.

Dentre as exigências, a referida resolução estabeleceu que são de responsabilidade da diretoria da Instituição:

- A implantação e a implementação de uma estrutura de Controles Internos efetiva mediante a definição de atividades de controle para todos os níveis de negócios da Instituição;
- O estabelecimento dos objetivos e procedimentos pertinentes aos mesmos;
- A verificação sistemática da adoção e do cumprimento dos procedimentos definidos em função de seus objetivos.

Esta resolução teve inspiração nos componentes do *Internal Control – Integrated Framework*, material publicado em 1992 pelo *Committee of Sponsoring Organizations of the Treadway Commission – COSO*, entidade privada criada nos Estados Unidos da América que se dedica a desenvolver estruturas e orientações sobre Controles Internos, gerenciamento de riscos prevenção / mitigação de fraudes, entre outras.



Essa primeira versão com uma linguagem comum, direcionamento e orientação clara, obteve grande aceitação e tem sido amplamente utilizada em todo o mundo por integrar boas práticas de gestão de maneira organizada e transversal para toda organização, além de ser reconhecida como um modelo para desenvolvimento, implementação e condução do Controle Interno, bem como para a avaliação de sua eficácia.

Em 2013 o COSO realizou uma ampla revisão da estrutura e atualizou a definição para Controle Interno: “processo conduzido pela estrutura de governança, administração e outros profissionais da entidade e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade”.

Essa definição de Controle Interno reflete alguns conceitos fundamentais:

- **Conduzido para atingir objetivos em uma ou mais categorias** – operacional, divulgação e conformidade.
- **Um processo que consiste em tarefas e atividades contínuas** – um meio para um fim, não um fim em si mesmo.
- **Realizado por pessoas** – não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e as ações que elas tomam em cada nível da organização para realizar o Controle Interno.
- **Capaz de proporcionar segurança razoável** - mas não absoluta, para a estrutura de governança e Alta Administração de uma entidade.
- **Adaptável à estrutura da entidade** – flexível na aplicação para toda a entidade ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

Segundo o COSO, essa definição é intencionalmente abrangente e captura conceitos fundamentais para a forma como as organizações desenvolvem, implementam e conduzem suas atividades de controle, proporcionando uma base para aplicação a todas as organizações que operam em diferentes estruturas de entidades, indústrias e regiões geográficas.

De acordo também com a definição, verificamos que a responsabilidade pelo ambiente de controle é de todos os envolvidos na Instituição, que devem agir com conduta ética e adequada, além de serem diligentes com as suas atividades.

No item 3.1 detalhamos o Modelo COSO e sua composição e funcionamento e no item 2.2 apresentamos a sugestão de consideração das principais responsabilidades, baseado no Modelo das Três Linhas de Defesa.

2. Conceitos Gerais

2.1 Sistema de Controles Internos

A referência dada pelo CMN ao definir do que trata a resolução merece um destaque para melhor compreensão do que seria o “Sistema de Controles Internos”, e para isso, iremos utilizar uma definição básica que se adequa perfeitamente.

Vindo do grego, o termo “sistema” significa: combinar, ajustar, formar um conjunto.

Esse conjunto possui um objetivo geral a ser atingido e órgãos distintos, cada um com a sua determinada função, e a integração entre esses órgãos pode se dar, por exemplo, através de um fluxo de informações e reportes.

A composição do Sistema de Controles Internos pode ser facilmente demonstrada e compreendida pelo desenho a seguir:



Um adequado e eficiente Sistema de Controles Internos auxilia as entidades a alcançar objetivos importantes e a sustentar e melhorar o seu desempenho. Requer que as organizações desenvolvam atividades de controle que se adaptem aos ambientes operacionais e corporativos em constante mudança, reduzam/mitiguem os riscos para níveis aceitáveis e apoiem um processo sólido de tomada de decisões e de governança da organização.

Recomenda-se que todos os atores que fazem parte desse conjunto compartilhem conhecimento e informações, de modo a retroalimentar o funcionamento adequado e contínuo do Sistema de Controles Internos, contribuindo para que cada área desempenhe de maneira mais eficiente suas atribuições.

2.2 Linhas de Defesa

O engajamento de toda a Instituição no Sistema de Controles Internos, estabelecendo a adequada segregação de funções e independência das áreas/atividades, pode ser alcançado por meio da adoção do modelo de Linhas de Defesa, que tem estrutura flexível e é aplicável a qualquer Instituição, não importando seu tamanho ou complexidade.

As funções, de acordo com cada uma das Linhas de Defesa, variam de acordo com a organização, sendo que algumas funções podem ser combinadas ou divididas nas Linhas. As Linhas de Defesa devem trabalhar de forma complementar, evitando sobreposições e lacunas.

A figura a seguir representa, de forma adaptada, esse modelo.



**As principais atividades associadas a 2ª Linha de Defesa podem conter, entre outras, as funções de: Controles Internos; Compliance; Segurança da informação; Gestão Integrada de Riscos; Qualidade e Supervisão interna, e podem variar de maneira significativa dependendo do porte da organização e do setor.*

Cada uma dessas "Linhas" desempenha um papel distinto dentro da estrutura de governança da Instituição, atuando de forma interdependente, mas não impede que em algumas organizações, por exemplo, partes de uma função na 2ª Linha possam estar envolvidas na assessoria e gestão de riscos para a 1ª Linha, enquanto outras funções da 2ª Linha focam na avaliação e monitoramento desses controles.

1ª Linha de Defesa: Operações e unidades de negócios

Corresponde ao nível de controle da gerência operacional, responsável por manter Controles Internos eficazes e conduzir procedimentos de gerenciamento de seus riscos e controles diariamente.

São os responsáveis primários por identificar, avaliar, tratar, controlar, monitorar e reportar os riscos de suas áreas, de forma alinhada às diretrizes internas, regulamentações, políticas e procedimentos aplicáveis.

2ª Linha de Defesa: Avaliação e Monitoramento da gestão da 1ª Linha de Defesa

Essas unidades corporativas devem ser independentes da gestão das Linhas de Negócio e atuam no monitoramento periódico do desenho e funcionamento dos controles na 1ª Linha de Defesa, bem como fornecendo conhecimento e facilitando as atividades de gerenciamento de riscos, além de dar suporte às áreas da 1ª Linha de Defesa de forma consultiva.

São responsáveis também por certificar a eficiência e a eficácia das atividades de controle da 1ª Linha de Defesa, por meio de mapeamentos, monitoramento e testes de controles, efetuando reportes de sua atuação periodicamente para Diretoria / Alta Administração.

Para serem efetivas, essas funções devem ter acesso a todas as informações, metodologias, documentos e base de dados, necessários para o exercício de sua atividade, assim como, autoridade, recursos e acesso a Diretoria / Alta Administração da Instituição.

3ª Linha de Defesa: Verificação Independente do modelo e dos controles

Responsáveis pela revisão independente sobre o gerenciamento dos riscos, a Auditoria Interna 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, fornecendo aos órgãos de governança e à Alta Administração avaliações abrangentes baseadas no maior nível de independência.

Opinam ainda sobre a forma como a primeira e a segunda Linha de Defesa alcançam os objetivos de sua atuação, contribuindo para o seu aprimoramento.

Audidores Externos e Órgãos Reguladores e Autorreguladores

Embora as partes externas não sejam formalmente consideradas para estarem entre as três Linhas de Defesa, 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.

Algumas instituições, como o BIS – *Bank for International Settlements*, consideram esses entes como Linhas Adicionais de Defesa, que fornecem avaliações às partes interessadas da organização, incluindo os órgãos de governança e a Alta Administração.

Considerando o escopo e objetivos específicos das avaliações realizadas por esses entes, em geral, os resultados são menos extensos do que o escopo abordado pelas três Linhas de Defesa de uma organização. Os principais são:

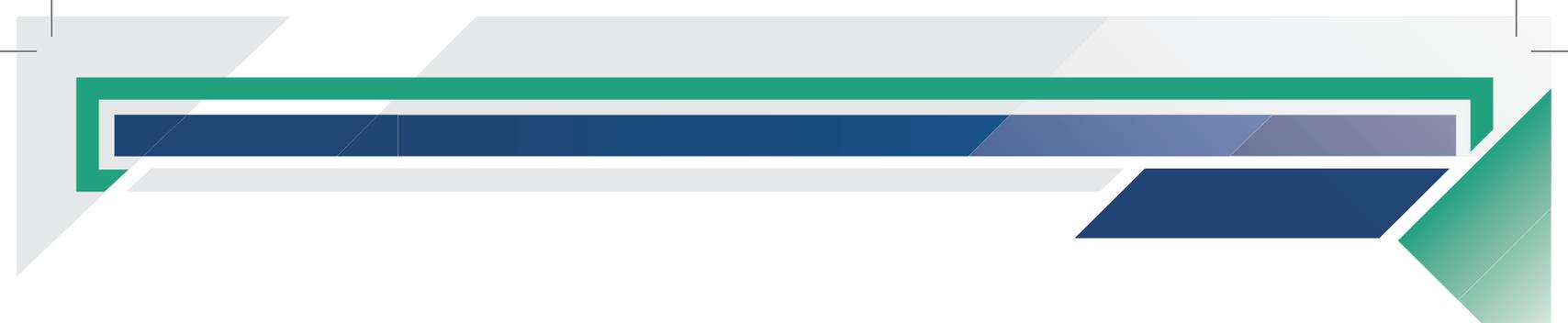
Auditoria Externa: tem o papel de revisar as demonstrações financeiras para garantir que não possuam distorções relevantes e sejam elaboradas de acordo com uma estrutura adequada.

Banco Central do Brasil e Comissão de Valores Mobiliários: avaliam se as instituições financeiras e demais instituições autorizadas a funcionar por estes órgãos possuem infraestrutura adequada para a realização de suas atividades sistêmicas e cumprimento dos normativos existentes.

Anbima, B3, FEBRABAN e outros: supervisionam as regras da autorregulação das Instituições que aderem aos códigos / autorregulações.

Diretoria / Alta Administração

Embora não sejam considerados dentre as três Linhas de Defesa desse modelo, nenhuma discussão estaria completa sem considerar os papéis essenciais da Diretoria e da Alta Administração (Conselho de Administração, Conselho Fiscal, Comitê de Auditoria e órgãos equivalentes), que são as principais partes interessadas atendidas pelas “Linhas” e estão em melhor posição para ajudar a garantir que o modelo de Três Linhas de Defesa seja aplicado aos processos de gerenciamento de riscos e controles da organização.



A Diretoria e a Alta Administração devem estabelecer as diretrizes da estrutura de Controles Internos na Instituição e disponibilizar os recursos necessários conforme o grau de complexidade de suas operações, além de disseminar a cultura de controles pelo exemplo (*Tone at the top*).

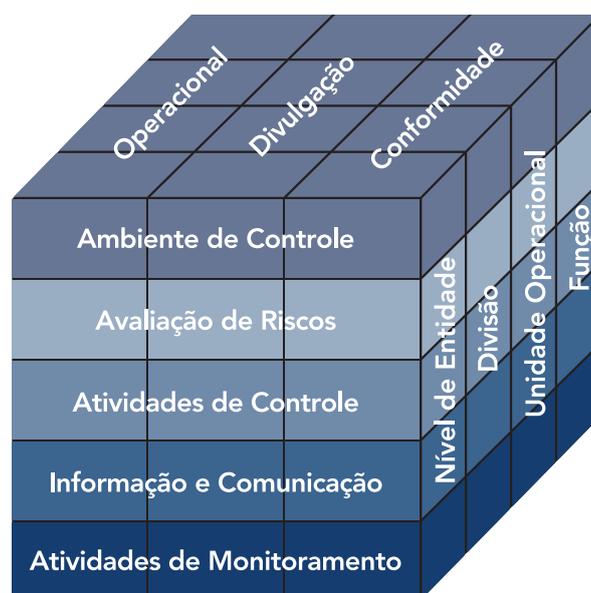
O profissional de Controles Internos deve fornecer à Diretoria / Alta Administração informações sobre o gerenciamento dos variados riscos, mas cabe destacar que cada colaborador, independentemente do nível hierárquico ou do tipo de contrato de trabalho ou serviço que presta à Instituição, deve estar comprometido com a prática e a disseminação da cultura de Controles Internos.

3. Componentes e Princípios de Controles Internos

3.1 Estrutura do COSO (2013)

Grande parte das instituições brasileiras desenvolveu o seu Sistema de Controles Internos baseado nas diretrizes contidas no COSO - *Internal Control – Integrated Framework*, citado anteriormente na introdução.

Dessa forma, a seguir exploraremos de forma simples o referido modelo, representado frequentemente pela figura de um cubo que apresenta a inter-relação dos Objetivos, Componentes (Elementos) e o Objeto (Estrutura Organizacional - Empresa, Divisão, Unidade, Função etc.).



Existe uma relação direta entre os Objetivos, que são o que a entidade busca alcançar, os Componentes, que representam o que é necessário para atingir os objetivos e a Estrutura organizacional da entidade (as unidades operacionais e entidades legais, entre outras).

- Objetivos: operacional, divulgação e conformidade – representadas pelas colunas.
- Componentes: são representados pelas linhas.
- Estrutura organizacional da entidade: representada pela terceira dimensão.

Objetivos

As três categorias de objetivos permitem às organizações se concentrarem em diferentes aspectos do Controle Interno:

- **Operacional** – Utilização eficaz e eficiente dos recursos.
- **Divulgação** – Confiabilidade de relatórios.
- **Conformidade** – Cumprimento de leis e regulamentos aplicáveis.

Componentes

Para cada um dos componentes há princípios estabelecidos que representam os conceitos fundamentais associados a cada um deles. Como esses princípios são originados diretamente dos componentes, uma entidade poderá ter um Controle Interno eficaz ao aplicar todos os princípios. Todos os 17 princípios aplicam-se às categorias de Objetivos (Operacional, Divulgação e Conformidade).

Os princípios que apoiam os componentes estão relacionados a seguir:

COMPONENTES	PRINCÍPIOS
Ambiente de controle: É a base para os outros componentes.	<ol style="list-style-type: none">1. A organização demonstra ter comprometimento com a integridade e os valores éticos.2. A estrutura de governança demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do Controle Interno.3. A administração estabelece as estruturas, os níveis de subordinação e as autoridades e responsabilidades adequadas na busca dos objetivos.4. A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos.5. A organização faz com que as pessoas assumam responsabilidade por suas funções de Controle Interno na busca pelos objetivos.
Avaliação de riscos: Está relacionada ao conhecimento de todos os riscos relevantes.	<ol style="list-style-type: none">6. A organização especifica os objetivos com clareza suficiente, a fim de permitir a identificação e a avaliação dos riscos associados aos objetivos.7. A organização identifica os riscos à realização de seus objetivos por toda a entidade e analisa os riscos como uma base para determinar a forma como devem ser gerenciados.8. A organização considera o potencial para fraude na avaliação dos riscos à realização dos objetivos.9. A organização identifica e avalia as mudanças que poderiam afetar, de forma significativa, o sistema de Controle Interno.

COMPONENTES

PRINCÍPIOS

Atividades de controle

Diz respeito às políticas e procedimentos, que devem ser seguidos por todos os níveis hierárquicos para minimizar a ocorrência e/ou impacto dos riscos inerentes à operação.

Comunicação e informação:

Referem-se à produção de relatórios, tanto operacionais, como financeiros, necessários para o controle e gestão da organização.

Monitoramento:

São atividades contínuas que detectam a qualidade do sistema de Controles Internos e reporta deficiências aos responsáveis para que sejam tratadas.

10. A organização seleciona e desenvolve atividades de controle que contribuem para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos.

11. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar a realização dos objetivos.

12. A organização estabelece atividades de controle por meio de políticas que estabelecem o que é esperado e os procedimentos que colocam em prática essas políticas.

13. A organização obtém ou gera e utiliza informações significativas e de qualidade para apoiar o funcionamento do Controle Interno.

14. A organização transmite internamente as informações necessárias para apoiar o funcionamento do Controle Interno, inclusive os objetivos e responsabilidades pelo controle.

15. A organização comunica-se com os públicos externos sobre assuntos que afetam o funcionamento do Controle Interno.

16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou independentes para se certificar da efetividade do sistema de Controles Internos.

17. A organização avalia e comunica deficiências no Controle Interno em tempo hábil aos responsáveis por tomar ações corretivas, inclusive a estrutura de governança e Alta Administração, conforme aplicável.

3.2 Abordagem Baseada em Risco

Considerando a crescente complexidade e a dinâmica do mercado financeiro em nível global, cada vez mais se faz necessária a adoção de práticas de Controles Internos baseadas em risco, para garantir foco nos aspectos mais relevantes.

Uma atuação voltada exclusivamente à avaliação do funcionamento dos Controles Internos, pode descartar a possibilidade de existirem riscos ainda sem controles. Por isso, uma abordagem baseada em risco pode ser adotada, até porque, é fruto da evolução contínua do processo de gestão de riscos nas organizações.

Se pressupõe que cada Instituição adote uma avaliação de risco de acordo com seu modelo de negócios, apetite ao risco e ambiente regulatório a que está sujeita, não existindo assim um modelo uniforme para todas as Instituições. Ou seja, é uma questão mais principiológica, e cada Instituição tem a liberdade de definir como atuar.



Essa abordagem, associada ao modelo de Três Linhas de Defesa e a metodologia baseada no COSO, pode ser de grande valia, sendo um importante elemento que, alinhado com as estratégias da organização, contribuirá para a eficiência e eficácia geral do processo.

A abordagem baseada em riscos tem como fundamentação o próprio processo de gerenciamento de riscos da organização, e de forma estruturada, deve considerar a natureza, a complexidade e o risco das operações realizadas. Resumidamente, a abordagem ocorre desde a fase de planejamento das atividades de avaliação, não se limitando a ela, e inclui ainda as fases de execução, reporte e monitoramento.

Não se pode deixar de reforçar que o risco é dinâmico e deve ser periodicamente avaliado, sendo essencial que as avaliações reflitam adequadamente os riscos presentes, e que os resultados das avaliações permitam a implementação de medidas práticas para mitigação do risco.

4. Atribuições ou Funções de Controles Internos

As atividades de controle, visando mitigar potenciais perdas originadas da exposição ao risco e fortalecer os processos e procedimentos que refletem o modelo de governança adotado, deve ter sua efetividade constantemente avaliada.

Nesta linha, são atribuições e funções da estrutura de Controles Internos:

- Apoiar a 1ª Linha de Defesa na observação de suas responsabilidades diretas.
- Desenvolver metodologias, ferramentas, sistemas, infraestrutura e governança necessária para suportar a gestão de riscos.
- Disseminar a cultura de riscos e controles e divulgar as práticas líderes e políticas relacionadas a esses temas.
- Monitorar as atividades da 1ª linha de defesa visando garantir a definição das responsabilidades dentro da Instituição, a segregação das atividades de forma a evitar conflito de interesses.
- Mapear e avaliar periodicamente os processos, regras, modelos, sistemas, riscos e atividades de controle executados pela 1ª e 2ª Linha de Defesa (quando esta realiza atividade de 1ª linha), objetivando a mitigação dos riscos e redução de possíveis perdas financeiras.
- Assegurar a existência de governança para avaliação de produtos e serviços, bem como verificar previamente os riscos envolvidos em sua alteração e criação, indicando a necessidade de implantação de controles.
- Efetuar verificações nas unidades de negócio a fim de validar a veracidade das respostas em sistema no formato Self Assessment.
- Disseminar os temas de riscos e controles junto à 1ª Linha de Defesa e aos órgãos de governança / Alta Administração.
- Efetuar reportes de sua atuação periodicamente para Diretoria / Alta Administração por meio de relatórios ou informes pontuais.

5. Interação Entre a Área de Controles Internos e as Demais Áreas da Instituição

Para assegurar o adequado atingimento dos objetivos da organização, todas as áreas que compõem as Linhas de Defesa (Áreas de Negócios e Suporte, Controles Internos, Compliance, Auditoria Interna, entre outras) devem ter atuação e abordagem integrada, com clara divisão de papéis e responsabilidades.

A seguir as principais áreas de interação com a área de Controles Internos.

5.1 Áreas de Negócios e Suporte

A função e a atuação da área de Controles Internos permeiam toda a organização, incluindo negócios, processos, produtos e serviços. Dessa forma, deve existir interação entre essas áreas (1ª Linha de Defesa) e a área de Controles Internos (2ª Linha de Defesa), com o objetivo de construir processos com controles eficazes e eficientes, com menor grau de exposição a riscos, bem como a sustentabilidade dos negócios.

A participação da área de Controles Internos na criação, manutenção e alteração dos produtos e serviços comercializados pela Instituição, visa assegurar que as atividades de controle associadas ao produto ou serviço sejam efetivas e consistentes com a natureza, complexidade e risco dessas operações.

Além disso, cabe a área de Controles Internos avaliar e monitorar os controles implementados nos principais processos, produtos e serviços da organização, bem como assessorar as áreas de negócio na correção dos desvios identificados.

5.2 Área de Compliance

A função de Compliance contribui para a prevenção e mitigação de exposições a riscos regulatórios (locais e internacionais), de conduta e danos à imagem da Instituição, por meio de medidas internas que disciplinam as suas atividades. Compliance transcende a ideia de “estar em conformidade” às leis, regulamentações e autorregulamentações, abrangendo aspectos de governança, conduta, transparência e temas como ética e integridade.

A função Compliance é trabalhar no estabelecimento de regras, nos treinamentos, nos procedimentos rotineiros e na conscientização das normas para as partes interessadas.

Cabe ao Compliance a captura, interpretação das normas legais e infralegais, bem como, atuar junto aos Gestores de 1ª ou 2ª linha nas definições de ações que visem o atendimento/cumprimento regulatório.

5.3 Área de Gestão de Riscos

As atividades de controle estão dentre os principais mecanismos para mitigação de riscos, principalmente o risco operacional, devendo as áreas de Controles Internos e Gestão de Riscos trabalhar em sinergia e de forma complementar, visando conferir segurança e robustez às instituições financeiras no seu mercado/segmento de atuação.

Em determinadas Instituições Financeiras a área de Controles Internos pode ter a função de validar os modelos, metodologias, ambiente tecnológico e base de dados e informações de gestão de riscos e capital.

5.4 Auditoria Interna

As Instituições devem implementar e manter atividade de auditoria interna compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da Instituição. A área de auditoria interna é considerada 3ª Linha de Defesa, independente, respondendo pela avaliação da governança, do gerenciamento de riscos e do Sistema de Controles Internos da Instituição.

Deve realizar auditorias periódicas, avaliando a adequação dos controles, a partir da verificação de sua qualidade, suficiência, cumprimento e efetividade.

As áreas de Controles Internos e Auditoria Interna devem possuir definições claras sobre as atribuições e forma de atuação de cada uma, visando a cobertura apropriada de suas avaliações e minimizando a sobreposição de atuação. Para isso, as duas áreas podem articular a elaboração dos seus escopos de atuação / planejamento, além de compartilhar informações sobre trabalhos realizados.

5.5 Diretoria / Alta Administração

A Diretoria / Alta Administração, com a supervisão da estrutura de governança, fixa objetivos que se alinham com a missão, a visão e as estratégias. Esses objetivos refletem as escolhas feitas pela administração e pela estrutura de governança. A fixação de objetivos é requisito prévio para o Controle Interno e uma parte importante do processo de gestão relacionado ao planejamento estratégico. Dessa forma, é primordial o comprometimento da Alta Administração na implementação e monitoramento do Sistema de Controles Internos da empresa.



Para que o Sistema de Controles Internos de uma Instituição seja eficiente, é imprescindível que a Alta Administração esteja comprometida e engajada, de forma que a cultura de controles seja disseminada e compreendida em todos os níveis da Organização.

Para tanto, deve assegurar independência e autoridade para que a área de Controles Internos execute a bom termo suas atribuições, e com isso proporcione segurança às atividades operacionais, além de fornecer confiabilidade para os *stakeholders* e maximizar o retorno do investimento.

6. Perfis dos Profissionais de Controles Internos

Ainda que não exista uma formação específica para exercer a função na atividade de Controles Internos, o profissional para ser reconhecido e se destacar na área deve possuir experiência, conhecimento e determinadas qualidades, como:

- Sólidos valores éticos e de integridade, demonstrados por meio de sua conduta e atitudes.
- Capacidade de entendimento da Instituição, seu contexto, cultura, princípios e a natureza de suas atividades.
- Rápida assimilação de conteúdo; sendo capaz de assimilar de forma macro e micro as atividades das diversas áreas da Instituição.
- Criatividade e análise crítica, sendo utilizada como ferramentas para trazer benefícios para a Instituição e otimizar as atividades realizadas na função de Controles Internos.
- Independência para expressar a sua opinião técnica sem receio de retaliações ou ameaças e isenção para que suas decisões e julgamentos não sejam influenciados por relações de afinidade.
- Habilidade de comunicação e argumentação com todos os graus e níveis da Instituição, não só, mas também com os Órgãos Reguladores.
- Capacidade de lidar com pressões externas e internas.
- Flexibilidade perante as diversas situações, o profissional que exercer a função de Controles Internos deve possuir habilidade de se adaptar a diferentes situações que podem ocorrer no ambiente de trabalho.
- Habilidade de identificar onde estão os riscos da Instituição.
- Habilidade de se manter atualizado sobre as novas tecnologias disruptivas, tecnologias estas que ocasionam mudanças mercadológicas, criam novos modelos de negócios, produtos e serviços.
- Expertise em resolver problemas complexos com metodologias ágeis, além de apresentar resiliência para enfrentar novos desafios.
- Foco na melhoria de processos objetivando ao alcance dos resultados estratégicos estabelecidos pela Instituição.
- Sólidos conhecimentos dos frameworks de controle, bem como dos processos de negócios e produtos da companhia.

7. Limitações de Controles Internos

A estrutura de Controles Internos tem como seu principal objetivo atuar para verificar se os procedimentos ou atos que possibilitem segurança quanto aos aspectos lógicos e técnicos do processo são realizados de forma eficiente e tempestiva, e neste contexto, mesmo tendo sido realizada de forma adequada em todas as suas etapas, não é possível assegurar um nível de conforto pleno porque há limitações inerentes.

Neste cenário considera-se o julgamento humano no processo de decisão e este pode falhar com erros simples. Outro fator a ser levado em consideração é a possibilidade de existência de conluio o que pode vir a neutralizar os controles existentes, além do fator custo e vantagens observáveis relacionados ao processo de resposta a riscos.

A segurança razoável em relação ao funcionamento e eficácia das atividades de controles, depende de muitos fatores que são considerados isoladamente ou em conjunto e que visam atender a diversos objetivos e finalidades mitigando o risco de uma organização deixar de atingir seus propósitos.

Ainda assim pode acontecer um evento extraordinário, uma ocorrência operacional ou falha na comunicação.

Citamos a seguir situações que exemplificam melhor algumas limitações:

- Negligenciamento de controles por meio de conluio* de colaboradores, incluindo a Alta Administração, e/ ou prestadores de serviços terceirizados.
** atuação de um grupo de pessoas com o objetivo de ocultar ou praticar um fato ilícito, que pode passar despercebido pelas atividades de controle.*
- Erro Humano devido a imperícia, imprudência, instruções mal interpretadas e erros de julgamento**.
*** decisões tomadas na realidade do momento, ou seja, considerando as informações disponíveis, tempo e pressões do negócio, pode-se esperar que eventuais falhas ocorram.*
- Toda e qualquer atividade está sujeita a colapsos, no caso de atividades não realizadas adequadamente, como por exemplo, na substituição de um sistema crítico onde não ocorreu capacitação tempestiva dos usuários, ocorrendo muitos erros, que podem gerar falhas significativas.
- Alterações na realidade operacional dos processos e procedimentos, não refletidas adequadamente nos controles.
- Os custos e os benefícios da implementação de funcionalidades de identificação de eventos e atividades de controle são mensurados com diferentes níveis de segurança dentro de cada Instituição, mas mesmo assim é importante encontrar equilíbrio neste processo, trazendo um nível de conforto em relação ao benefício que o controle trará versus os custos envolvidos.

Qualquer uma dessas situações impede a segurança absoluta, e embora sejam inerentes, a organização deve estar ciente delas ao desenvolver, implementar e executar as atividades de controles, para minimizar, dentro do possível, a ocorrência de tais limitações.

8. Glossário

Apetite a Riscos: A quantidade total de riscos que uma organização está disposta a aceitar para alcançar os objetivos em busca de sua missão ou visão.

Conformidade: Empregada em face aos objetivos e relacionada com o cumprimento do arcabouço legal.

Controles automatizados: Executados por sistemas seguros e confiáveis, não dependendo de julgamentos pessoais para garantir a consistência, precisão e tempestividade.

Controles compensatórios: Executados quando da ausência de implantação dos demais controles.

Controles detectivos: Executados ao longo do processo. Detectam erros que são difíceis de definir ou prever.

Controles diretivos: Controles que direcionam para os comportamentos desejados, porém não garantem ou previnem a ocorrência de falhas e erros intencionais ou não.

Controles manuais: Executados por pessoas sem suporte sistêmico.

Controles preventivos: Executados no início do processo. Previnem o acontecimento de erros ou irregularidades e minimizam os riscos na fonte.

Evento: Incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

Impacto: Resultado ou efeito de um evento. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos de uma organização.

Integridade: A qualidade ou o estado de possuir princípios morais íntegros; retidão, honestidade e sinceridade; fazer aquilo que é certo, professar e viver de acordo com uma série de valores.

Risco: A possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos.

Stakeholders: Partes interessadas.

9. Referências

- Resolução CMN nº 2.554, de 24/09/1998
- Circular BACEN nº 3.467, de 15/09/2009
- Coso.org
- Lei das SAs (6404/76)
- Estrutura Integrada de Controles Internos, Comitê das Organizações Patrocinadoras da Comissão Treadway (coso.org).
- The Three Lines of Defense in Effective Risk Management and Control, (Altamonte Springs, Flórida: The Institute of Internal Auditors Inc., Janeiro 2013).
- Artigo Técnico da Resenha BM&F nº 143, "Controles internos e gestão de riscos operacionais em instituições financeiras brasileiras: classificação, definições e exemplos", de Antonio Marcos Duarte Júnior, Manoel Rodrigues Jordão, Luiz Carlos Galhardo, Rodrigo Ferreira Kannebley, Daniel Scaion, Milena Schidlow, Márcia Akemi Miyazaki Conilio, páginas 42, 43 e 44.

ANEXO I – Principais práticas e ferramentas relacionadas a Controles Internos

A. Ambiente de Controle

Código de Ética

É um documento com diversas diretrizes que orientam as pessoas quanto às suas posturas e atitudes ideais, moralmente aceitas ou toleradas pela Instituição, enquadrando os colaboradores a uma conduta politicamente correta e em linha com a boa imagem que a entidade quer ocupar.

Normativos Internos

Conjunto de políticas, circulares, normas, regulamentos, manuais de procedimento e seus anexos, emitidos pelo conglomerado.

Estrutura organizacional

A estrutura de governança tem independência em relação aos seus diretores e supervisiona o Sistema de Controles Internos.

B. Avaliação de Risco

Matriz de risco e controle

As matrizes de riscos e controles são elaboradas pelos gestores das áreas e têm o objetivo de registrar os processos, etapas e atividades das unidades de negócio, servindo de instrumento para a avaliação da eficiência e eficácia de seus métodos no gerenciamento de riscos que possam causar impactos na busca de seus objetivos.

Gestão de mudanças

A organização identifica e avalia os impactos que as mudanças podem causar, de forma relevante, no funcionamento do Sistema de Controles Internos.

C. Atividade de Controle

Mapeamento de processos

O mapeamento de processos de negócios objetiva determinar a forma em que os insumos recebidos de um fornecedor, são tratados e transformados em produtos que serão entregues aos clientes. A essa transformação, chamada de processo, são alocados recursos destinados a promover essa transformação com efetividade.

Walkthrough

É um processo que consiste na revisão do fluxo de atividades de um determinado processo e na avaliação do desenho dos controles existentes para certificar se os mesmos estão operando e mitigam os fatores de riscos inerentes a este processo.

Controle Chave

Controle ou conjunto de controles que possuem a maior capacidade de mitigar o risco correspondente, sendo considerado elemento essencial ou mais importante de controle em um processo.

D. Informação e Comunicação

Canais de denúncia

Canal estabelecido para recepção e/ou encaminhamento da denúncia relacionadas a fatos ou indícios de condutas irregulares para tratamento.

Canais de reporte

Canal de comunicação com a Diretoria / Alta Administração para: (I) reporte tempestivo das avaliações sobre a qualidade dos controles; (II) andamento dos planos de ação que visam sanar eventuais fragilidades identificadas.

E. Monitoramento

Indicador de Risco (KRI)

Medida que fornece informação sobre o nível de exposição do conglomerado a um dado risco operacional num determinado ponto no tempo.

Teste

O teste de controle é uma atividade que consiste em avaliar a efetividade do funcionamento / operação dos controles.

Avaliação do sistema de Controles Internos

A integridade do Sistema de Controles Internos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas.

ANEXO II – Dicionário de tipos de controles

A seguir, definem-se e exemplificam-se os principais itens que um Sistema de Controles Internos deve abranger para a gestão de riscos corporativos, conforme descritos no Artigo Técnico da Resenha BM&F nº 143 (item 9 – Referências – página 23 deste Guia)

1.1. Alçadas e limites

Envolvem a delimitação do âmbito de atuação ou influência de um gestor, via sistema aplicativo ou de forma manual, quanto a sua condição de vir a aprovar valores ou assumir posições em nome da Instituição, conferida pela hierarquia ou por comitês.

Exemplos:

- a) estabelecimento de alçadas para que um operador de mercado assuma posições para cada horizonte de investimento.
- b) estabelecimento de limites para liberação de transações via SWIFT, sistema para emissão de documento de ordem de crédito (DOC) e outros.
- c) limites de risco de mercado (value at risk, stress testing etc.) impostos à tesouraria.
- d) limites de risco de crédito (margens de garantia para derivativos, scoring/rating mínimo requerido, limites de cheques especial etc.) impostos às áreas comerciais.

1.2. Autorizações

Buscam permitir o encaminhamento de uma operação/transação após conferência, evidenciada por log no sistema ou assinatura/visto em documentação de suporte.

Exemplos:

- a) liberação de documentos para cadastro de conta corrente.
- b) autorização para que um novo produto seja vendido na rede de agências.
- c) assinaturas de gestores em autorizações para movimentação interna de pessoas.

1.3. Conciliação

Consiste no confronto de informações de origens distintas, com o objetivo de detectar inconsistências.

Exemplos:

- a) conferência de informações de relatórios gerenciais, emitidos por sistema aplicativo, com os registros de controle da unidade.
- b) conciliação de posicionamento ao final de um dia por front office e back office.
- c) comparação dos preços de ativos/passivos nos diferentes livros das posições proprietárias, de forma a melhor gerenciar riscos de mercado e crédito.

1.4. Acesso físico

Consiste no controle da entrada/saída de funcionários, clientes e/ou equipamentos em determinadas áreas de uma Instituição.

Exemplos:

- a) permissão de acesso via biometria, cartão magnético ou prévia identificação a áreas do banco consideradas de especial sensibilidade (área de numerário, tesouraria etc.).
- b) redefinição periódica do acesso físico de funcionários a unidades, em face de movimentação interna para outras áreas.
- c) permissão para movimentação de computadores entre diferentes áreas da Instituição.

1.5. Acesso lógico

Busca o controle de acesso/alcance de funcionários e/ou clientes a arquivos eletrônicos e sistemas computacionais, bem como a disponibilização de instruções e treinamento para esses sistemas aos usuários autorizados.

Exemplos:

- a) estabelecimento de senhas, de modo a impedir o acesso generalizado de funcionários a sistemas computacionais.
- b) restrição do acesso de terceiros (concorrentes, clientes etc.) a relatórios, sistemas e informações confidenciais.

1.6. Delimitação de responsabilidades

Determina uma definição clara e formal das responsabilidades e da autoridade sobre os procedimentos criados para certas atividades, focando a limitação de ação acerca dos mesmos, sem envolver valores (cuja delimitação é tratada no Controle Interno de alçadas).

Exemplos:

- a) pagamento de cheques é ação exclusiva da função "caixa", independentemente de eventual necessidade de alçada (em função do valor) ou de autorização (evidenciada por intermédio de um visto).
- b) assinatura de contratos ou cheques que necessitam de procuração ou delegação de diretores executivos.

1.7. Disponibilização e padronização de informações

Visam o estabelecimento de sistemas de comunicação efetivos entre áreas, de maneira a assegurar que as informações cheguem a seu destino, contemplando, inclusive, aspectos como integridade, confiabilidade e disponibilidade.

Exemplos:

- a) definição de política de acesso a informações, visando preservar a confidencialidade necessária.
- b) confecção e divulgação interna, em base regular, de relatórios com dados relativos a perdas de unidades de negócio.
- c) divulgação de atas de comitês, fluxos de processos, definição de responsabilidades, status dos planos de ação definidos pelos Controles Internos e relatórios de auditoria.
- d) descrição de fluxos operacionais, funções e procedimentos.

1.8. Execução de plano de contingência

Busca formalizar e testar ações que permitam dar continuidade às operações de unidades que não possam ser interrompidas, independentemente da adversidade da situação.

Exemplos:

- a) definição de procedimentos em casos de greve, queda de energia, falhas no sistema telefônico e outros.
- b) procedimentos de contingência durante paradas programadas de sistemas computacionais corporativos.

1.9. Manutenção de registros

Consiste em fazer a manutenção atualizada, segura e organizada de registros.

Exemplos:

- a) armazenamento de dados de operações e/ou transações, permitindo formação de banco de dados com histórico das áreas, projetos, documentação de suporte;
- b) organização do arquivo e back-up dos sistemas.
- c) registro de sugestões/reclamações realizados pelos clientes em agência, central de atendimento e outros.
- d) arquivo de dados exigido por órgão regulamentador (microfilmes de cheques, comprovante de despesas para fisco, relatórios de auditoria).
- e) evidência de atividades de controle, exercidas por meio de vistos/assinaturas em documentos, log em sistemas etc.

1.10. Monitoração

Acompanhamento de uma atividade ou processo, para avaliação de sua adequação e/ou desempenho, em relação às metas, aos objetivos traçados e aos benchmarks, assim como acompanhamento contínuo do mercado financeiro, de forma a antecipar mudanças que possam impactar negativamente a Instituição.

Exemplos:

- a) monitoração do comportamento de usuários de cartões de crédito (lugares inusitados, produtos diferentes etc.).
- b) monitoração e questionamento de flutuações abruptas nos resultados de agências, produtos, carteiras próprias e de terceiros.
- c) monitoração de valores realizados e orçados em unidades, com o objetivo de identificar dificuldades/problemas.
- d) acompanhamento da concorrência, visando o lançamento de novos produtos.

1.11. Normatização interna

Compreende o estabelecimento formal de normas internas, para a execução das atividades inerentes à unidade.

Exemplos:

- a) definição de normas/regras para efetiva implantação dos Controles Internos necessários ao gerenciamento de riscos identificados.
- b) definição de procedimentos para contemplar análise de risco no desenvolvimento de novos produtos.
- c) existência de normas certificadoras (como ISO 9000).

1.12. Segregação de funções

Envolve a separação das responsabilidades sobre atividades conflitantes, por meio de organograma ou estabelecimento de regras, a fim de prevenir ou detectar problemas nas tarefas executadas.

Exemplos:

- a) lançamento, conferência e validação de dados realizados por funcionários ou áreas independentes.
- b) independência das áreas de vendas, concessão de limites de crédito e cobrança.
- c) separação da administração de recursos próprios e de terceiros.
- d) separação de atividades de tesouraria e controladoria.
- e) separação entre atividades de normatização (gerenciamento de riscos) e de fiscalização (auditoria).

1.13. Treinamento

Engloba exercícios para apurar habilidades ou transmitir conhecimentos, ampliando competências e capacitações.

Exemplos:

- a) programas institucionais de aprimoramento (idiomas, graduação, pós-graduação, MBA etc.).
- b) programas de treinamento para lançamento de novos produtos, utilização de novos modelos e tecnologias.
- c) programas de autoavaliação em sintonia com as metas da unidade.

1.14. Validação

Consiste em examinar minuciosamente procedimentos relacionados a uma atividade, com o intuito de validar informações (internas e externas), obtidas por funcionários ou clientes, na documentação de operações financeiras ou em eventual modificação desses procedimentos.

Exemplos:

- a) conferência de documentação entregue por clientes nas áreas de crédito, auditoria interna, contratos e outros.
- b) checagem de informações armazenadas em bancos de dados.
- c) conferência para liberação de operações financeiras.
- d) validação de normas e procedimentos internos das áreas.
- e) validação de novos produtos em comitês.



FEBRABAN

Federação Brasileira de Bancos

Av. Brig. Faria Lima, 1.485 - 14º andar
CEP.: 01452-002 - São Paulo

www.autorregulacaobancaria.org.br