NORMA
BRASILEIRA

ABNT NBR ISO 37301

Primeira edição
03.06.2021

Sistemas de gestão de *compliance* — Requisitos com orientações para uso

Compliance management systems — Requirements with guidance for use

ICS 03.100.01; 03.100.02; 03.100.70

ISBN 978-85-07-08514-0

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO 37301:2021
47 páginas

[587.995.750-00]
Arquivo de impressão gerado em 18/10/2022 10:26:44 de uso exclusivo de LEONARDO BRANDELLI

ABNT
Av. Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

Sumário

Página

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos internacionais adotados são elaborados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários. Os Documentos Técnicos ABNT não substituem Leis, Decretos ou Regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer Documento Técnico ABNT.

Ressalta-se que os Documentos Técnicos ABNT podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar as datas para exigência dos requisitos de quaisquer Documentos Técnicos ABNT.

A ABNT NBR ISO 37301 foi elaborada pela Comissão de Estudo Especial de Governança de Organizações (ABNT/CEE-309). O Projeto circulou em Consulta Nacional conforme Edital nº 04, de 30.04.2021 a 01.06.2021.

A ABNT NBR ISO 37301 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 37301:2021, que foi elaborada pelo *Technical Committee Governance of organizations* (ISO/TC 309).

O Escopo em inglês da ABNT NBR ISO 37301 é o seguinte:

Scope

This document specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization.

This document is applicable to all types of organizations regardless of the type, size and nature of the activity, as well as whether the organization is from the public, private or non-profit sector.

All requirements specified in this document that refer to a governing body apply to top management in cases where an organization does not have a governing body as a separate function.

Introdução

Organizações que almejam ser bem-sucedidas a longo prazo precisam estabelecer e manter uma cultura de *compliance*, considerando as necessidades e expectativas das partes interessadas. O *compliance* não é, portanto, apenas a base, mas também uma oportunidade para uma organização bem-sucedida e sustentável.

O *compliance* é um processo contínuo e o resultado de uma organização que cumpre suas obrigações. O *compliance* se torna sustentável ao ser incorporado na cultura da organização, e no comportamento e na atitude das pessoas que trabalham para ela. Enquanto mantém sua independência, é preferível que a gestão de *compliance* seja integrada com os outros processos de gestão da organização e os seus requisitos e procedimentos operacionais.

Um sistema de gestão de *compliance* eficaz em toda a organização permite que uma organização demonstre seu comprometimento em cumprir leis pertinentes, requisitos regulamentares, códigos setoriais da indústria e normas organizacionais, assim como normas de boa governança, melhores práticas geralmente aceitas, ética e expectativas da comunidade.

A abordagem de *compliance* de uma organização é moldada pela liderança, por meio da aplicação de valores centrais e padrões geralmente aceitos de boa governança, de ética e da comunidade. Incorporar o *compliance* no comportamento das pessoas que trabalham para uma organização depende acima de tudo da liderança em todos os níveis e dos valores claros de uma organização, assim como do reconhecimento e implementação de medidas para promover o comportamento de *compliance*. Se este não for o caso em todos os níveis de uma organização, há um risco de não *compliance*.

Em um número de jurisdições, os tribunais têm considerado o comprometimento da organização com o *compliance* por meio do seu sistema de gestão de *compliance* ao determinar a penalidade adequada a ser imposta por violação de leis pertinentes. Portanto, órgãos regulatórios e judiciais podem também se beneficiar deste documento como uma referência.

As organizações estão cada vez mais convencidas de que, ao aplicar valores vinculativos e uma gestão de *compliance* apropriada, elas podem salvaguardar a sua integridade e evitar ou minimizar o não *compliance* das obrigações de *compliance* da organização. A integridade e o *compliance* eficaz são, portanto, elementos chave de uma gestão boa e diligente. O *compliance* também contribui para o comportamento socialmente responsável das organizações.

Um dos objetivos deste documento é auxiliar as organizações a desenvolverem e disseminarem uma cultura positiva de *compliance*, considerando que convém que uma gestão de riscos relacionados ao *compliance,* sólida e eficaz, seja considerada como uma oportunidade a ser perseguida e aproveitada, devido aos diversos benefícios que ela provê para a organização, como:

— melhorar as oportunidades de negócio e sua sustentabilidade;

— proteger e melhorar a credibilidade e a reputação da organização;

— considerar as expectativas das partes interessadas;

— demonstrar o comprometimento de uma organização para gerenciar eficaz e eficientemente seus riscos de *compliance*;

— aumentar a confiança de terceiras partes na capacidade da organização de alcançar sucesso sustentado;

— minimizar o risco da ocorrência de uma violação aos custos associados e dano reputacional.

Este documento especifica requisitos, assim como também provê orientação sobre os sistemas de gestão de *compliance* e práticas recomendadas. Tanto os requisitos como as orientações deste documento são destinados a serem adaptados, e a sua implementação pode variar dependendo do tamanho e nível de maturidade do sistema de gestão de *compliance* da organização, e do contexto, natureza e complexidade dos objetivos e atividades da organização.

Este documento é adequado para melhorar os requisitos relacionados ao *compliance* em outros sistemas de gestão e para auxiliar uma organização na melhoria da gestão global de todas as suas obrigações de *compliance*.

A Figura 1 provê uma visão geral dos elementos comuns de um sistema de gestão de *compliance*.

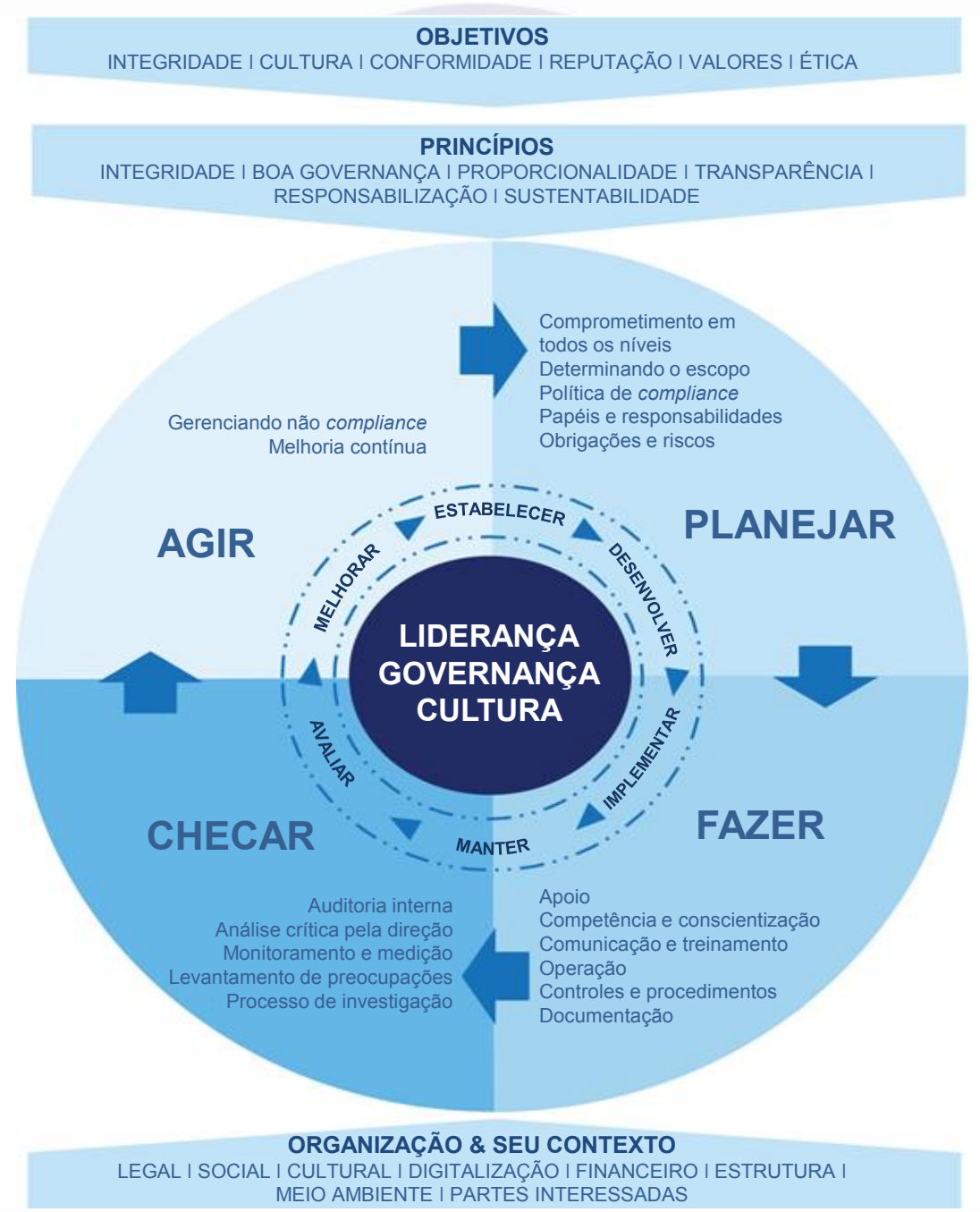

Figura 1 – Elementos de um sistema de gestão de *compliance*

Neste documento, as seguintes formas verbais são empregadas:

— deve” indica um requisito;

— “convém que” indica uma recomendação;

— “pode” (*may*/*can*) indica permissão/possibilidade ou capacidade.

NOTA BRASILEIRA	Em inglês, existem dois verbos (*can*/*may*) para expressar a forma verbal “pode”em português.

Informação indicada como “NOTA” serve como orientação para entendimento ou esclarecimento do requisito associado.

O Anexo A provê orientações para o uso deste documento.

[587.995.750-00]
Arquivo de impressão gerado em 18/10/2022 10:26:44 de uso exclusivo de LEONARDO BRANDELLI

Sistemas de gestão de *compliance* — Requisitos com orientações para uso

1 Escopo

Este documento especifica os requisitos e fornece diretrizes para estabelecer, desenvolver, implementar, avaliar, manter, e melhorar um sistema de gestão de *compliance* eficaz dentro de uma organização.

Este documento é aplicável a todos os tipos de organizações, independentemente do tipo, porte e natureza da atividade, assim como se a organização é do setor público, privado ou sem fins lucrativos.

Todos os requisitos especificados neste documento que se referem a um Órgão Diretivo são aplicáveis à Alta Direção nos casos em que uma organização não tenha um Órgão Diretivo como uma função separada.

2 Referência normativa

Não há referência normativa para este documento.

3 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições.

A ISO e a IEC mantêm bases de dados terminológicos para uso em normalização nos seguintes endereços:

— ISO *Online browsing platform*: disponível em https://www.iso.org/obp

— IEC *Electropedia*: disponível em http://www.electropedia.org/

3.1
organização
pessoa ou grupo de pessoas que têm suas próprias funções com responsabilidades, autoridades e relações para alcançar seus *objetivos* (3.6)

Nota 1 de entrada: O conceito de organização inclui, mas não é limitado a, empreendedor individual, companhia, corporação, firma, empresa, autoridade, parceria, instituição de caridade, ou parte ou combinação destes, seja incorporada ou não, pública ou privada.

Nota 2 de entrada: Se a organização for parte de uma entidade maior, o termo “organização” se refere somente à parte da entidade maior que estiver dentro do escopo do sistema de gestão de *compliance*.

3.2
parte interessada (termo preferido)
stakeholder (termo admitido)
pessoa ou *organização* (3.1) que pode afetar, ser afetada ou se perceber afetada por uma decisão ou atividade

3.3
Alta Direção
pessoa ou grupo de pessoas que dirige e controla uma *organização* (3.1) no nível mais alto

Nota 1 de entrada: A Alta Direção tem o poder de delegar autoridade e prover recursos na organização.

Nota 2 de entrada: Se o escopo do *sistema de gestão* (3.4) cobrir apenas parte de uma organização, então Alta Direção se refere àqueles que dirigem e controlam aquela parte da organização.

Nota 3 de entrada: Para os propósitos deste documento, o termo “Alta Direção” se refere ao nível mais alto da gestão executiva.

3.4
sistema de gestão
conjunto de elementos inter-relacionados ou interativos de uma *organização* (3.1), para estabelecer *políticas* (3.5), *objetivos* (3.6) e *processos* (3.8) para alcançar esses objetivos

Nota 1 de entrada: Um sistema de gestão pode abordar uma única disciplina ou várias disciplinas.

Nota 2 de entrada: Os elementos do sistema de gestão incluem a estrutura da organização, papéis e responsabilidades, planejamento e operação.

3.5
política
intenções e direção de uma *organização* (3.1), como formalmente expressos pela sua *Alta Direção* (3.3)

Nota 1 de entrada: Uma política pode também ser formalmente expressa por um *Órgão Diretivo* (3.21) da organização.

3.6
objetivo
resultado a ser alcançado

Nota 1 de entrada: Um objetivo pode ser estratégico, tático ou operacional.

Nota 2 de entrada: Os objetivos podem se relacionar a diferentes disciplinas (como finanças, saúde e segurança e meio ambiente). Eles podem ser, por exemplo, para toda a organização ou específicos para um projeto, produto, serviço ou *processo* (3.8).

Nota 3 de entrada: Um objetivo pode ser expresso de outras formas, por exemplo, como um resultado pretendido, um propósito, um critério operacional, como um objetivo de *compliance* (3.26) ou pelo uso de outras palavras com significado similar (por exemplo, finalidade, meta ou alvo).

Nota 4 de entrada: No contexto de *sistemas de gestão* (3.4) de *compliance*, objetivos de *compliance* são estabelecidos pela *organização* (3.1), coerentemente com a *política* (3.5) de *compliance*, para alcançar resultados específicos.

3.7
risco
efeito da incerteza nos *objetivos* (3.6)

Nota 1 de entrada: Um efeito é um desvio do esperado – positivo ou negativo.

Nota 2 de entrada: Incerteza é o estado, ainda que parcial, de deficiência de informação relacionada ao entendimento ou conhecimento de um evento, sua consequência ou probabilidade.

Nota 3 de entrada: O risco é muitas vezes caracterizado pela referência a “eventos” (como definido no ABNT ISO Guia 73) potenciais e “consequências” (como definido no ABNT ISO Guia 73), ou uma combinação destes.

Nota 4 de entrada: O risco é muitas vezes expresso em termos da combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a “probabilidade” associada (como definido no ABNT ISO Guia 73) de ocorrência.

3.8
processo
conjunto de atividades inter-relacionadas ou interativas que usam ou transformam entradas para entregar um resultado

Nota 1 de entrada: Se o resultado de um processo é chamado de saída, o produto ou o serviço depende do contexto da referência.

3.9
competência
capacidade de aplicar conhecimento e habilidades para alcançar resultados pretendidos

3.10
informação documentada
informação que se requer que seja controlada e mantida por uma *organização* (3.1) e o meio no qual ela está contida

Nota 1 de entrada: Informação documentada pode estar em qualquer formato e meio e pode ser proveniente de qualquer fonte.

Nota 2 de entrada: Informação documentada pode se referir a:

— o *sistema de gestão* (3.4), incluindo *processos* (3.8) relacionados;

— a informação criada para a organização operar (documentação);

— a evidência de resultados alcançados (registros).

3.11
desempenho
resultado mensurável

Nota 1 de entrada: Desempenho pode se relacionar tanto a constatações quantitativas quanto a qualitativas.

Nota 2 de entrada: Desempenho pode se relacionar à gestão de atividades, *processos* (3.8), produtos, serviços, sistemas ou *organizações* (3.1).

3.12
melhoria contínua
atividade recorrente para melhorar o *desempenho* (3.11)

3.13
eficácia
extensão na qual atividades planejadas são realizadas e resultados planejados são alcançados

3.14
requisito
necessidade ou expectativa que é declarada, geralmente obrigatória ou implícita

Nota 1 de entrada: "Geralmente implícita" significa que é costume ou prática comum para a *organização* (3.1) e *partes interessadas* (3.2) que a necessidade ou expectativa sob consideração esteja implícita.

Nota 2 de entrada: Um requisito especificado é aquele que é declarado, por exemplo, em uma *informação documentada* (3.10).

3.15
conformidade
atendimento de um *requisito* (3.14)

3.16
não conformidade
não atendimento de um *requisito* (3.14)

Nota 1 de entrada: Uma não conformidade não é, necessariamente, um *não compliance* (3.27).

3.17
ação corretiva
ação para eliminar a(s) causa(s) de uma *não conformidade* (3.16) e para prevenir recorrência

3.18
auditoria
processo (3.8) sistemático e independente, para obter evidência e avaliar objetivamente, para determinar a extensão na qual os critérios de auditoria são atendidos

Nota 1 de entrada: Uma auditoria pode ser uma auditoria interna (primeira parte) ou uma auditoria externa (segunda parte ou *terceira parte* (3.30)) e pode ser uma auditoria combinada (combinando duas ou mais disciplinas).

Nota 2 de entrada: Uma auditoria interna é conduzida pela própria *organização* (3.1), ou por uma parte externa em seu nome.

Nota 3 de entrada: "Evidência de auditoria" e "critérios de auditoria" estão definidos na ABNT NBR ISO 19011.

Nota 4 de entrada: Independência pode ser demonstrada pela liberdade de responsabilidade pela atividade que está sendo auditada ou pela liberdade de desvio e conflito de interesse.

3.19
medição
processo (3.8) para determinar um valor

3.20
monitoramento
determinação do estado de um sistema, um *processo* (3.8) ou uma atividade

Nota 1 de entrada: Para determinar a situação, pode haver a necessidade de verificar, supervisionar ou observar criticamente.

3.21
Órgão Diretivo
pessoa ou grupo de pessoas que tem a responsabilidade e autoridade finais pelas atividades, governança e políticas de uma *organização* (3.1), e ao qual a *Alta Direção* (3.3) se reporta e perante o qual a Alta Direção é responsabilizada

Nota 1 de entrada: Nem todas as organizações, particularmente as organizações pequenas, têm um Órgão Diretivo separado da Alta Direção.

Nota 2 de entrada: Um Órgão Diretivo pode incluir, porém não está limitado a, o conselho de administração, os comitês do conselho, um conselho de supervisão, ou curadores.

NOTA BRASILEIRA	O conselho de supervisão é também conhecido como conselho fiscal.

3.22
pessoal
indivíduos em uma relação reconhecida como uma relação de trabalho com base em uma prática ou lei nacional, ou em qualquer relação contratual na qual a sua atividade dependa da *organização* (3.1)

3.23
função de *compliance*
pessoa ou grupo de pessoas com responsabilidade e autoridade para a operação do *sistema de gestão* (3.4) de *compliance* (3.26)

Nota 1 de entrada: Preferencialmente, será atribuída a um indivíduo a supervisão global do sistema de gestão de *compliance*.

3.24
riscos de *compliance*
probabilidade da ocorrência e as consequências de *não compliance* (3.27) com as *obrigações de compliance* (3.25) da *organização* (3.1)

3.25
obrigações de *compliance*
requisitos (3.14) que uma *organização* (3.1) mandatoriamente tem que cumprir, como também os que uma organização voluntariamente escolhe cumprir

3.26
compliance
atendimento a todas as *obrigações de compliance* (3.25) da *organização* (3.1)

3.27
não *compliance*
não atendimento de *obrigações de compliance* (3.25)

3.28
cultura de *compliance*
valores, ética, crenças e *conduta* (3.29) que existem por toda a *organização* (3.1) e interagem com as estruturas e os sistemas de controle da organização para produzir normas comportamentais que contribuem com o *compliance* (3.26)

3.29
conduta
comportamentos e práticas que impactam os resultados para os clientes, pessoal, fornecedores, mercados e comunidade

3.30
terceira parte
pessoa ou órgão que é independente da *organização* (3.1)

Nota 1 de entrada: Todos os parceiros de negócio são terceiras partes, mas nem todas as terceiras partes são parceiros de negócio.

3.31
procedimento
forma especificada de executar uma atividade ou um *processo* (3.8)

[FONTE: ABNT NBR ISO 9000:2015, 3.4.5]

4 Contexto da organização

4.1 Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são pertinentes para o seu propósito e que afetam sua capacidade de alcançar os resultados pretendidos do seu sistema de gestão de *compliance*.

Para este propósito, a organização deve considerar uma gama variada de questões, incluindo, mas não limitadas a:

— o modelo de negócio, incluindo a estratégia, a natureza, o porte e a escala da complexidade e sustentabilidade das operações e atividades da organização;

— a natureza e o escopo dos negócios na relação com terceiras partes;

— o contexto regulatório e legal;

— a situação econômica;

— os contextos ambiental, cultural e social;

— as estruturas internas, as políticas, os processos, os procedimentos e os recursos, incluindo tecnologia;

— a sua cultura de *compliance*.

4.2 Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

— as partes interessadas que são pertinentes para o sistema de gestão de *compliance*;

— os requisitos pertinentes destas partes interessadas;

— quais destes requisitos serão abordados pelo sistema de gestão de *compliance*.

4.3 Determinando o escopo do sistema de gestão de *compliance*

A organização deve determinar os limites e a aplicabilidade do sistema de gestão de *compliance* para estabelecer o seu escopo.

NOTA O escopo do sistema de gestão de *compliance* se destina a esclarecer os principais riscos de *compliance* que a organização está enfrentando e os limites geográficos ou organizacionais, ou ambos, para os quais o sistema de gestão de *compliance* será aplicado, especialmente se a organização é uma parte de uma entidade maior.

Ao determinar esse escopo, a organização deve considerar:

— as questões internas e externas referidas em 4.1;

— os requisitos referidos em 4.2, 4.5 e 4.6.

O escopo deve estar disponível como informação documentada.

4.4 Sistema de gestão de *compliance*

A organização deve estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de *compliance*, incluindo os processos necessários e as suas interações, de acordo com os requisitos deste documento.

O sistema de gestão de *compliance* deve refletir os valores, objetivos, estratégias e os riscos de *compliance* da organização, levando em conta o contexto da organização (ver 4.1).

4.5 Obrigações de *compliance*

A organização deve, sistematicamente, identificar as suas obrigações de *compliance* resultantes das suas atividades, produtos e serviços, e avaliar os seus impactos nas suas operações.

A organização deve ter processos implementados para:

a) identificar as novas e modificadas obrigações de *compliance*, para assegurar o *compliance* contínuo;

b) avaliar o impacto das mudanças identificadas e implementar quaisquer mudanças necessárias na gestão das obrigações de *compliance*.

A organização deve manter informação documentada das suas obrigações de *compliance*.

4.6 Avaliação de riscos de *compliance*

A organização deve identificar, analisar e avaliar seus riscos de *compliance* baseado em um processo de avaliação de riscos de *compliance*.

A organização deve identificar os riscos de *compliance* relacionando as suas obrigações de *compliance* com as suas atividades, produtos, serviços e aspectos pertinentes das suas operações.

A organização deve avaliar os riscos de *compliance* relacionados aos processos terceirizados e de terceira parte.

Os riscos de *compliance* devem ser avaliados periodicamente e sempre que ocorrerem mudanças materiais nas circunstâncias ou no contexto da organização.

A organização deve reter informação documentada sobre o processo de avaliação dos riscos de *compliance* e sobre as ações para abordar seus riscos de *compliance*.

5 Liderança

5.1 Liderança e comprometimento

5.1.1 Órgão Diretivo e Alta Direção

O Órgão Diretivo e a Alta Direção devem demonstrar liderança e comprometimento em relação ao sistema de gestão de *compliance* para:

— assegurar que a política de *compliance* e os objetivos de *compliance* estão estabelecidos e são compatíveis com a direção estratégica da organização;

— assegurar a integração dos requisitos do sistema de gestão de *compliance*, dentro dos processos de negócio da organização;

— assegurar que os recursos necessários para o sistema de gestão de *compliance* estão disponíveis;

— comunicar a importância de um sistema de gestão de *compliance* eficaz e da conformidade com os requisitos do sistema de gestão de *compliance;*

— assegurar que o sistema de gestão de *compliance* alcance os seus resultados pretendidos;

— apoiar e orientar as pessoas para contribuírem com a eficácia do sistema de gestão de *compliance;*

— promover a melhoria contínua;

— apoiar outros papéis pertinentes para demonstrar sua liderança, e como se aplica às suas áreas de responsabilidades.

NOTA As referências a “negócio” neste documento podem ser interpretadas amplamente para significar aquelas atividades que são o núcleo principal dos propósitos de existência da organização.

O Órgão Diretivo e a Alta Direção devem:

— estabelecer e sustentar os valores da organização;

— assegurar que as políticas, processos e procedimentos sejam desenvolvidos e implementados para alcançar os objetivos de *compliance*;

— assegurar que eles sejam informados em um tempo hábil sobre os assuntos de *compliance*, incluindo as instâncias de não *compliance*, e assegurando que ações apropriadas sejam tomadas;

— assegurar que o comprometimento com o *compliance* é mantido e que o não *compliance* e o comportamento não *compliance* sejam tratados adequadamente;

— assegurar que as responsabilidades pelo *compliance* estejam incluídas nas descrições do cargo, conforme apropriado;

— indicar ou nomear uma função de *compliance* (ver 5.3.2);

— assegurar que um sistema para levantar e abordar questões de acordo com 8.3 seja estabelecido.

5.1.2 Cultura de *compliance*

A organização deve desenvolver, manter e promover uma cultura de *compliance* em todos os níveis dentro da organização

O Órgão Diretivo, a Alta Direção e os gestores devem demonstrar um comprometimento ativo, visível, consistente e sustentável, por meio de uma conduta e um comportamento-padrão, que seja requerido por toda a organização.

A Alta Direção deve encorajar um comportamento que crie e apoie o *compliance*. Deve-se prevenir e não tolerar comportamentos que comprometam o *compliance*.

5.1.3 Governança de *compliance*

O Órgão Diretivo e a Alta Direção devem assegurar que os seguintes princípios estejam implementados:

— acesso direto da função de *compliance* ao Órgão Diretivo;

— independência da função de *compliance;*

— autoridade e competência apropriada da função de *compliance*;

NOTA 1 O acesso direto pode incluir: linha de subordinação direta ao Órgão Diretivo, apresentação de relatórios periódicos sobre o Órgão Diretivo e participação em suas reuniões.

NOTA 2 A independência significa a ausência de quaisquer interferências ou pressão, ou ambas, com a operação da função de *compliance*.

5.2 Política de *compliance*

O Órgão Diretivo e a Alta Direção devem estabelecer uma política de *compliance* que:

a) seja apropriada ao propósito da organização;

b) proveja uma estrutura para estabelecer os objetivos de *compliance*;

c) inclua um comprometimento para atender aos requisitos aplicáveis;

d) inclua um comprometimento para a melhoria contínua do sistema de gestão de *compliance*.

A política de *compliance* deve:

— estar alinhada com os valores, os objetivos e a estratégia da organização;

— requerer o *compliance* com as obrigações de *compliance* da organização;

— apoiar os princípios de governança de *compliance* de acordo com 5.1.3;

— fazer referência e descrever a função de *compliance*;

— definir as consequências de estar em não *compliance* com os procedimentos, processos, políticas e obrigações de *compliance* da organização;

— encorajar o levantamento de preocupações e proibir quaisquer formas de retaliação;

— estar escrita em uma linguagem clara de modo que todo o pessoal possa entender facilmente os propósitos e princípios;

— ser adequadamente implementada e aplicada;

— estar disponível como informação documentada;

— ser comunicada dentro da organização;

— estar disponível para as partes interessadas, conforme apropriado.

5.3 Papéis, responsabilidade e autoridades

5.3.1 Órgão Diretivo e Alta Direção

O Órgão Diretivo e a Alta Direção devem assegurar que as responsabilidades e autoridades para os papéis pertinentes estejam atribuídas e comunicadas dentro da organização.

O Órgão Diretivo e a Alta Direção devem atribuir autoridade e responsabilidades para:

a) assegurar que o sistema de gestão de *compliance* esteja em conformidade com os requisitos deste documento;

b) reportar sobre o desempenho do sistema de gestão de *compliance* para o Órgão Diretivo e para a Alta Direção.

O Órgão Diretivo deve:

— assegurar que a Alta Direção é avaliada com base no alcance dos objetivos de *compliance*;

— exercer uma supervisão sobre a Alta Direção com relação à operação do sistema de gestão de *compliance.*

A Alta Direção deve:

— alocar recursos adequados e apropriados para estabelecer, desenvolver, implementar, avaliar, manter e melhorar o sistema de gestão de *compliance*;

— assegurar a existência de sistemas eficazes de reporte de desempenho de *compliance* em tempo hábil;

— assegurar o alinhamento entre as metas operacionais e estratégicas e as obrigações de *compliance*;

— estabelecer e manter mecanismos de responsabilização, incluindo ações disciplinares e consequências;

— assegurar a integração do desempenho do *compliance* nas avaliações de desempenho do pessoal.

5.3.2 Função de *compliance*

A função de *compliance* deve ser responsável pela operação do sistema de gestão de *compliance*, incluindo o seguinte:

— facilitar a identificação das obrigações de *compliance*;

— documentar a avaliação dos riscos de *compliance* (ver 4.6);

— alinhar o sistema de gestão de *compliance* com os objetivos de *compliance*;

— monitorar e medir o desempenho do *compliance*;

— analisar e avaliar o desempenho do sistema de gestão de *compliance* para identificar quais são as necessidades de ação corretiva;

— estabelecer um sistema de documentação e reporte de *compliance*;

— assegurar que o sistema de gestão de *compliance* é analisado criticamente a intervalos planejados (ver 9.2 e 9.3);

— estabelecer um sistema para levantamento de preocupações e assegurando que as questões sejam endereçadas.

A função de *compliance* deve exercer supervisão de modo que:

— as responsabilidades para alcançar as obrigações de *compliance* identificadas estejam adequadamente alocadas ao longo de toda a organização;

— as obrigações de *compliance* estejam integradas com as políticas, os processos e os procedimentos;

— todas as pessoas pertinentes são treinadas, conforme requerido;

— os indicadores de desempenho do *compliance* estejam estabelecidos.

A função de *compliance* deve prover:

— pessoal com acesso aos recursos sobre os procedimentos, processos e políticas de *compliance*;

— aconselhamento para a organização sobre assuntos relacionados ao *compliance*;

NOTA As obrigações específicas da função de *compliance* não dispensam outras pessoas das suas responsabilidades pelo *compliance*.

A organização deve assegurar que a função de *compliance* tenha acesso a:

— tomadores de decisão seniores e a oportunidade de contribuir no início dos processos de tomada de decisão;

— todos os níveis da organização;

— todo o pessoal, informações documentadas e dados necessários;

— orientação especializada sobre leis, regulamentos, códigos e padrões organizacionais pertinentes.

5.3.3 Direção

A direção deve ser responsável pelo *compliance* dentro da sua área de responsabilidade:

— cooperando e apoiando a função de *compliance* e encorajando o pessoal a fazer o mesmo;

— assegurando que todo o pessoal dentro de seu controle esteja cumprindo os procedimentos, os processos, as políticas e as obrigações de *compliance* da organização;

— identificando e comunicando os riscos de *compliance* nas suas operações;

— integrando as obrigações de *compliance* às práticas e aos procedimentos de negócio existentes em suas áreas de responsabilidade;

— apoiando e atendendo as atividades de treinamento de *compliance*;

— desenvolvendo a conscientização junto ao pessoal sobre as obrigações de *compliance*, e orientando-os a cumprir os requisitos de competência e treinamento;

— encorajando seu pessoal a levantar preocupações de *compliance* e apoiando-os e impedindo de quaisquer formas de retaliação;

— participando ativamente na gestão e na resolução de incidentes relacionados a *compliance* e outras questões, conforme requerido;

— assegurando que, uma vez identificada a necessidade de ação corretiva, a ação corretiva apropriada seja recomendada e implementada.

5.3.4 Pessoal

Todo pessoal deve:

— cumprir com os procedimentos, processos, políticas e às obrigações de *compliance* da organização;

— reportar preocupações, questões e falhas de *compliance*;

— participar dos treinamentos, conforme requerido.

6 Planejamento

6.1 Ações para abordar riscos e oportunidades

Ao planejar o sistema de gestão de *compliance*, a organização deve considerar as questões referidas em 4.1, e os requisitos referidos em 4.2, e determinar os riscos e oportunidade que precisam ser considerados para:

— prover garantia de que o sistema de gestão de *compliance* pode alcançar seus resultados pretendidos;

— prevenir ou reduzir efeitos indesejados;

— alcançar a melhoria contínua.

Ao planejar o sistema de gestão de *compliance*, a organização deve considerar:

— seus objetivos de *compliance* (ver 6.2);

— as obrigações de *compliance* identificadas (ver 4.5);

— os resultados da avaliação de riscos de *compliance* (ver 4.6).

A organização deve planejar:

a) ações para abordar estes riscos e oportunidades;

b) como:

   1) integrar e implementar as ações em seus processos do sistema de gestão de *compliance*;

   2) avaliar a eficácia dessas ações.

6.2 Objetivos de *compliance* e planejamento para alcançá-los

A organização deve estabelecer os objetivos de *compliance* para as funções e níveis pertinentes.

Os objetivos de *compliance* devem:

a) ser consistentes com a política de *compliance*;

b) ser mensuráveis (se praticável);

c) considerar os requisitos aplicáveis;

d) ser monitorados;

e) ser comunicados;

f) estar atualizados, conforme apropriado;

g) estar disponíveis como informação documentada.

Ao planejar como alcançar os seus objetivos de *compliance*, a organização deve determinar:

— o que será feito;

— quais recursos serão requeridos;

— quem será o responsável;

— quando estará completo;

— como os resultados serão avaliados.

6.3 Planejamento de mudanças

Quando a organização determinar as necessidades para mudanças do sistema de gestão de *compliance*, estas mudanças devem ser conduzidas de uma forma planejada.

A organização deve considerar:

— os propósitos das mudanças e suas potenciais consequências;

— o projeto e a eficácia operacional do sistema de gestão de *compliance*;

— a disponibilidade de recursos adequados;

— a alocação ou realocação de responsabilidades e autoridades.

7 Apoio

7.1 Recursos

A organização deve determinar e prover os recursos necessários para o estabelecimento, a implementação, a manutenção e a melhoria contínua do sistema de gestão de *compliance*.

7.2 Competência

7.2.1 Generalidades

A organização deve:

— determinar a competência necessária de pessoas que realizam trabalhos sob o seu controle e que afetam o seu desempenho de *compliance*;

— assegurar que essas pessoas sejam competentes com base em educação, treinamento ou experiência apropriados;

— tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas, onde aplicável.

Informação documentada apropriada deve estar disponível como evidência de competência.

NOTA Ações aplicáveis podem incluir, por exemplo, a provisão de treinamento, o *coaching*, ou a mudança de atribuições do pessoal atualmente empregado; ou empregar ou contratar pessoas competentes.

7.2.2 Processo de contratação

Em relação a todo o seu pessoal, a organização deve desenvolver, estabelecer, implementar e manter processos:

a) em que as condições de contratação requeiram que o pessoal cumpra com os processos, os procedimentos, as políticas e as obrigações de *compliance* da organização;

b) que dentro de um período razoável do início da sua contratação, o pessoal receba uma cópia da política de *compliance* e treinamento em relação a essa política, ou tenha acesso a ela;

c) ações disciplinares apropriadas devem ser tomadas contra o pessoal que viole os processos e os procedimentos e as políticas e as obrigações de *compliance* da organização.

Como parte do processo de contratação, a organização deve considerar os riscos de *compliance* impostos pelas funções e pelo pessoal, e aplicar os procedimentos de *due diligence*, conforme requerido, antes de qualquer contratação, transferência ou promoção.

A organização deve implementar um processo que permita realizar uma análise crítica periódica das metas de desempenho, dos bônus por desempenho e de outros incentivos, para verificar se existem medidas apropriadas em vigor para prevenir o encorajamento ao não *compliance*.

7.2.3 Treinamento

A organização deve prover para o pessoal pertinente treinamento em bases regulares, desde o início da contratação e a intervalos planejados determinados pela organização.

O treinamento deve ser:

a) apropriado aos papéis do pessoal e aos riscos de *compliance* aos quais as pessoas estão expostas;

b) avaliado quanto à sua eficácia;

c) analisado criticamente regularmente.

Considerando conta os riscos de *compliance* identificados, a organização deve assegurar que procedimentos estejam implementados para contemplar a conscientização e o treinamento para terceiras partes que atuam em seu nome e que possam causar um risco de *compliance* para a organização.

Os registros de treinamento devem ser retidos como informação documentada.

7.3 Conscientização

As pessoas que realizam trabalho sob o controle da organização devem estar conscientes:

— da política de *compliance*;

— das suas contribuições para a eficácia do sistema de gestão de *compliance*, incluindo os benefícios da melhoria do desempenho de *compliance*;

— das implicações de estarem em não conformidade com os requisitos do sistema de gestão de *compliance*;

— das formas e dos procedimentos para o levantamento de preocupações de *compliance* (ver 8.3);

— da relação da política de *compliance* e das obrigações de *compliance* pertinentes aos seus papéis;

— da importância de apoiar a cultura de *compliance*.

7.4 Comunicação

A organização deve determinar as comunicações internas e externas pertinentes para o sistema de gestão de *compliance*, incluindo:

a) o que comunicar;

b) quando se comunicar;

c) com quem se comunicar;

d) como se comunicar.

A organização deve:

— considerar os aspectos de diversidade e de barreiras potenciais ao considerar suas necessidades de comunicação;

— assegurar que pontos de vista das partes interessadas sejam considerados no estabelecimento dos seus processos de comunicação;

— ao estabelecer seus processos de comunicação:

  — incluir a comunicação sobre sua cultura de *compliance*, obrigações e objetivos de *compliance*;

  — assegurar que a informação sobre *compliance* a ser comunicada seja consistente com as informações geradas dentro do sistema de gestão de *compliance* e confiável.

— responder às comunicações pertinentes sobre o seu sistema de gestão de *compliance*;

— reter informação documentada, como evidência da sua comunicação, conforme apropriado;

— comunicar internamente informações pertinentes do sistema de gestão de *compliance* entre os vários níveis e funções da organização, incluindo mudanças no sistema de gestão de *compliance*, conforme apropriado;

— assegurar que seus processos de comunicação possibilitam que o pessoal contribua para a melhoria contínua do sistema de gestão de *compliance*;

— assegurar que seus processos de comunicação possibilitam ao pessoal levantar preocupações (ver 8.3);

— comunicar externamente informações pertinentes do sistema de gestão de *compliance*, conforme estabelecido pelos processos de comunicação da organização e incluir comunicação sobre a sua cultura de *compliance*, objetivos e obrigações de *compliance*.

7.5 Informação documentada

7.5.1 Generalidades

O sistema de gestão de *compliance* da organização deve incluir:

a) informação documentada requerida por este documento;

b) informação documentada determinada pela organização como sendo necessária para a eficácia do sistema de gestão de *compliance*.

NOTA A extensão da informação documentada para um sistema de gestão de *compliance* pode diferir de uma organização para outra devido:

— ao porte da organização e seu tipo de atividades, processos, produtos e serviços;

— à complexidade dos processos e suas interações;

— à competência do pessoal.

7.5.2 Criando e atualizando a informação documentada

Ao criar e atualizar informação documentada, a organização deve assegurar apropriadamente:

— identificação e descrição (por exemplo, título, data, autor ou um número de referência);

— formato (por exemplo, idioma, versão de *software*, gráficos) e meio (por exemplo, papel, eletrônico);

— análise crítica e aprovação quanto à adequação e suficiência.

7.5.3 Controle da informação documentada

A informação documentada requerida pelo sistema de gestão de *compliance* e por este documento deve ser controlada para assegurar que:

a) ela esteja disponível e adequada ao uso, onde e quando for necessária;

b) ela esteja protegida adequadamente (por exemplo, contra perda de confidencialidade, uso impróprio ou perda de integridade).

Para o controle de informação documentada, a organização deve abordar as seguintes atividades, como aplicável:

— distribuição, acesso, recuperação e uso;

— armazenamento e preservação, incluindo a preservação da legibilidade;

— controle das mudanças (por exemplo, controle de versão);

— retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e operação do sistema de gestão de *compliance*, deve ser identificada, como apropriado, e controlada.

NOTA O acesso pode causar uma decisão quanto à permissão para visualizar a informação documentada, ou a permissão e autoridade para visualizar e alterar a informação documentada.

8 Operação

8.1 Planejamento e controle operacional

A organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos, e para implementar as ações determinadas na Seção 6, para:

— estabelecer critérios para os processos;

— implementar controles dos processos de acordo com os critérios.

A informação documentada deve estar disponível na extensão necessária para ter confiança de que os processos estão sendo conduzidos, conforme planejado.

A organização deve controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não intencionais, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

A organização deve assegurar que os processos, produtos ou serviços providos externamente, que são pertinentes para o sistema de gestão de *compliance*, sejam controlados.

NOTA As operações de terceirização da organização não isentam a organização das suas responsabilidades legais ou das obrigações de *compliance*.

A organização deve assegurar que os processos de terceiras partes sejam controlados e monitorados.

8.2 Estabelecendo controle e procedimentos

A organização deve implementar controles para gerenciar suas obrigações de *compliance* e riscos de *compliance* associados. Estes controles devem ser mantidos, analisados criticamente de forma periódica e testados para assegurar a sua contínua eficácia.

NOTA Controles de teste significa realizar um exercício projetado (simulado) para verificar se o controle realiza o que foi pretendido ou pode não ser contornado, ou se é realmente eficaz para reduzir o impacto ou a probabilidade do risco.

8.3 Levantamento de preocupações

A organização deve estabelecer, implementar e manter um processo para encorajar e permitir o relato (em casos de razoável crença de que a informação é verdadeira) de tentativas, suspeitas ou de violações reais da política de *compliance* ou das obrigações de *compliance*.

Este processo deve:

— ser visível e acessível para toda a organização;

— tratar os relatos de forma confidencial;

— aceitar relatos anônimos;

— proteger aqueles que fazem um relato contra retaliações;

— permitir que as pessoas recebam conselhos.

A organização deve assegurar que todo o pessoal esteja ciente dos procedimentos de notificação, seus direitos e proteção, e seja capaz de usá-los.

8.4 Processo de investigação

A organização deve desenvolver, estabelecer, implementar e manter processos para avaliar, verificar, investigar e encerrar os relatos sobre casos suspeitos ou reais de não *compliance*. Estes processos devem assegurar a tomada de decisão justa e imparcial.

Os processos de investigação devem ser conduzidos de forma independente e sem conflitos de interesses, pelo pessoal competente.

A organização deve utilizar os resultados de investigações para a melhoria do sistema de gestão de *compliance*, conforme apropriado (ver Seção 10).

A organização deve reportar, regularmente, sobre os números e os resultados das investigações para o Órgão Diretivo ou para a Alta Direção.

A organização deve reter informação documentada sobre as investigações.

9 Avaliação do desempenho

9.1 Monitoramento, medição, análise e avaliação

9.1.1 Generalidades

A organização deve monitorar o sistema de gestão de *compliance* para assegurar que os objetivos de *compliance* sejam alcançados.

A organização deve determinar:

— o que precisa ser monitorado e medido;

— os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

— quando o monitoramento e a medição devem ser realizados;

— quando os resultados do monitoramento e medição devem ser analisados e avaliados.

A informação documentada deve estar disponível como evidência dos resultados.

A organização deve avaliar o desempenho do *compliance* e a eficácia do sistema de gestão do *compliance*.

9.1.2 Fontes de retroalimentação sobre o desempenho de *compliance*

A organização deve estabelecer, implementar, avaliar e manter processos para buscar e receber retroalimentação sobre o seu desempenho do *compliance* de várias fontes. A informação deve ser analisada e avaliada criticamente para identificar as causas-raiz do não *compliance*, assegurar que ações apropriadas sejam tomadas, e refletir esta informação na avaliação periódica dos riscos, conforme requerido em 4.6.

9.1.3 Desenvolvimento de indicadores

A organização deve desenvolver, implementar e manter um conjunto de indicadores apropriado que orientem a organização na avaliação do alcance dos seus objetivos de *compliance*, para avaliar o seu desempenho de *compliance*.

9.1.4 Relatório de *compliance*

A organização deve estabelecer, implementar e manter processos para relatos de *compliance*, e assegurar que:

a) sejam definidos critérios apropriados para notificação;

b) sejam estabelecidos prazos para notificações regulares;

c) seja implementado um sistema de notificação de exceção que facilite notificações *ad hoc*;

d) processos e sistemas sejam implementados para assegurar a exatidão e completude da informação;

e) informação precisa e completa seja fornecida às funções ou áreas pertinentes da organização, para permitir que ações reparatórias, corretivas e preventivas sejam tomadas em um tempo hábil.

Quaisquer relatórios emitidos pela função de *compliance* para o Órgão Diretivo ou para a Alta Direção deve ser adequadamente protegidos contra alterações.

9.1.5 Manutenção de registros

Registros precisos e atualizados sobre as atividades de *compliance* da organização devem ser retidos para auxiliar no processo de análise crítica e monitoramento e demonstrar a conformidade com o sistema de gestão de *compliance*.

9.2 Auditoria interna

9.2.1 Generalidades

A organização deve conduzir auditorias internas em intervalos planejados, para prover informações sobre se o sistema de gestão de *compliance*:

a) está em conformidade com:

— os requisitos da própria organização para o seu sistema de gestão de *compliance*;

— os requisitos deste documento;

b) está implementado e mantido eficazmente.

9.2.2 Programa de auditoria interna

A organização deve planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios.

Ao estabelecer o programa de auditoria interna, a organização deve considerar a importância dos processos pertinentes e os resultados de auditoria anteriores.

A organização deve:

a) definir os objetivos da auditoria, os critérios e o escopo para cada auditoria;

b) selecionar auditores e conduzir as auditorias para assegurar objetividade e imparcialidade do processo de auditoria;

c) assegurar que os resultados das auditorias sejam reportados aos gestores pertinentes e à direção.

NOTA 1 A gestão pertinente pode incluir a função de *compliance* à Alta Direção e ao Órgão Diretivo.

Informação documentada deve estar disponível como evidência da implementação do programa de auditoria e dos resultados de auditoria.

NOTA 2 As orientações sobre a auditoria e o sistema de gestão são providas na ABNT NBR ISO 19011.

9.3 Análise crítica pela direção

9.3.1 Generalidades

O Órgão Diretivo e a Alta Direção devem analisar criticamente o sistema de gestão de *compliance* da organização, a intervalos planejados, para assegurar sua contínua adequação, suficiência e eficácia.

9.3.2 Entradas para análise crítica pela direção

A análise crítica pela direção deve incluir:

a) a situação das ações das análises críticas anteriores feitas pela direção;

b) mudanças em questões externas e internas que sejam pertinentes para o sistema de gestão de *compliance*;

c) mudanças nas necessidades e expectativas das partes interessadas que sejam pertinentes para o sistema de gestão de *compliance*;

d) informações sobre o desempenho do *compliance*, incluindo tendências em:

— não conformidades, não *compliance* e ações corretivas;

— resultados de monitoramento e medição;

— resultados de auditoria;

e) oportunidades para melhoria contínua.

A análise crítica pela direção deve considerar:

— a adequação da política de *compliance*;

— a independência da função de *compliance*;

— a extensão na qual os objetivos de *compliance* foram atendidos;

— a adequação dos recursos;

— a adequação da avaliação dos riscos de *compliance*;

— a eficácia dos controles existentes e os indicadores de desempenho;

— a comunicação das pessoas que levantam preocupações, das partes interessadas, incluindo retroalimentação (ver 9.1.2) e reclamações;

— as investigações (ver 8.4);

— a eficácia do sistema de notificação.

9.3.3 Resultados da análise crítica pela direção

Os resultados da análise crítica pela direção devem incluir decisões relacionadas às oportunidades de melhoria contínua e quaisquer necessidades de mudanças do sistema de gestão de *compliance*.

Informação documentada deve estar disponível como evidência dos resultados das análises críticas pela direção.

10 Melhoria

10.1 Melhoria contínua

A organização deve melhorar continuamente a adequação, a suficiência, e a eficácia do sistema de gestão de *compliance*.

10.2 Não conformidade e ação corretiva

Ao ocorrer uma não conformidade ou um não *compliance*, a organização deve:

a) reagir à não conformidade ou ao não *compliance* e, como aplicável:

1) tomar ação para controlá-la e corrigi-la;

2) lidar com as consequências.

b) avaliar a necessidade de ação para eliminar as causas da não conformidade ou do não *compliance*, ou ambos, a fim de que não ocorra novamente ou ocorra em outro lugar, por:

   1) analisar criticamente a não conformidade ou o não *compliance*, ou ambos;

   2) determinar as causas da não conformidade ou do não *compliance*, ou ambos;

   3) determinar se não conformidades ou não *compliance* similares, ou ambos, existem, ou podem potencialmente ocorrer.

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de qualquer ação corretiva tomada;

e) realizar mudanças no sistema de gestão de *compliance*, se necessário.

Ações corretivas devem ser apropriadas aos efeitos das não conformidades ou dos não *compliance*, ou ambos, encontrados.

Informação documentada deve estar disponível como evidência da:

— natureza das não conformidades ou dos não *compliance*, ou ambos, e de quaisquer ações subsequentes tomadas;

— os resultados de quaisquer ações corretivas.

Anexo A
(informativo)

Orientação para o uso deste documento

A.1 Histórico e escopo

A.1.1 Generalidades

O propósito da orientação deste Anexo é indicar abordagens e tipos de ações que uma organização pode tomar ao implementar seu sistema de gestão de *compliance*. Não pretende ser abrangente ou prescritivo, nem uma organização é obrigada a implementar todas as sugestões desta orientação, para ter um sistema de gestão de *compliance* que atenda aos requisitos deste documento. Convém que as medidas tomadas pela organização sejam razoáveis em relação à natureza e à extensão dos riscos de *compliance* que ela enfrenta, para cumprir com as suas obrigações de *compliance*.

Uma organização pode escolher implementar este sistema de gestão de *compliance* como um sistema separado, entretanto, idealmente ele seria implementado em conjunto com outros sistemas de gestão, tais como risco, antissuborno, qualidade, meio ambiente, segurança da informação e responsabilidade social, apenas para dar alguns poucos exemplos. Nestes casos, a organização pode se referir às ABNT NBR ISO 31000, ABNT NBR ISO 37001, ABNT NBR ISO 9001, ABNT NBR ISO 14001, ABNT NBR ISO/IEC 27001, assim como à ABNT NBR ISO 26000.

A.1.2 Escopo

Organizações de qualquer porte, complexidade ou setores podem aplicar este documento para criar um sistema de gestão de *compliance*, seguindo os seus requisitos. Isto dará as organizações um entendimento do seu contexto, das operações do seu negócio, das obrigações resultantes e dos riscos de *compliance* e auxiliará na implementação de passos razoáveis para cumprir com as suas obrigações. Cada um dos requisitos neste documento deve ser seguido. Entretanto, as orientações deste Anexo são simplesmente recomendações.

Na prática, é sempre mais fácil implementar um sistema de gestão de *compliance* alinhado com este documento nas pequenas organizações, porque elas são menos complexas. As pequenas e médias organizações irão melhorar as suas práticas organizacionais, usando os princípios dos requisitos deste documento.

Este documento se refere ao Órgão Diretivo e à Alta Direção e define o que estes termos significam em uma variedade de contextos e localidades. Este documento pode ser usado por todas as organizações, portanto, se uma organização não usar estes termos, procurar a intenção do seu uso: os requisitos ou instruções se aplicarão às pessoas ou grupos de pessoas que tenham a autoridade e a responsabilidade no topo da organização.

A.2 Referências normativas

Este documento não tem referências normativas. Os usuários podem se referir à bibliografia para outras informações e normas internacionais que sejam pertinentes ao *compliance*.

A.3 Termos e definições

Este documento adotou a estrutura de alto nível (HLS) desenvolvida pela ISO para melhorar o alinhamento entre as suas normas internacionais de sistemas de gestão. A estrutura HLS estabelece uma sequência de Seções, termos e definições comuns, e textos centrais idênticos que formam o núcleo das normas de sistemas de gestão (MSS). Isto significa que algumas das definições podem ser usadas de uma forma que não é familiar. As definições apresentadas podem prover esclarecimentos ao utilizar este documento.

Esta abordagem comum das MSS aumenta o valor dessas normas para os usuários. Isto é particularmente útil para aquelas organizações que escolham operar um único sistema de gestão (algumas vezes chamado "integrado") que possa atender simultaneamente aos requisitos de duas ou mais MSS. As organizações que não tenham adotado uma MSS ou uma estrutura de gestão de *compliance*, podem facilmente adotar este documento como um guia único dentro das suas organizações.

Informações adicionais sobre MSS e HLS podem ser encontradas em: https://www.iso.org/management-system-standards.html.

A.4 Contexto da organização

A.4.1 Entendendo a organização e seu contexto

A intenção da Seção é que as organizações estabeleçam um entendimento de alto nível (por exemplo, estratégico) das questões importantes que possam afetar o seu sistema de gestão de *compliance*. O conhecimento obtido é então usado para orientar a abordagem do planejamento, implementação, operação e melhoria do sistema de gestão de *compliance*.

Este é o processo de analisar criticamente todas as informações disponíveis sobre a organização: o que ela faz, onde, como e por que. Fatores externos e fatores-chave são avaliados por seus impactos sobre a organização em termos das suas obrigações de *compliance*.

As obrigações de *compliance* mais óbvias surgem dos contextos regulamentares e legais onde uma organização opera, mas as obrigações ou riscos podem também surgir de outros fatores, conforme sugerido neste documento. Convém que uma organização considere também tendências futuras pertinentes que possam ter um impacto.

Convém que fatores internos sejam considerados. Alguns exemplos são apresentados neste documento. Esta lista não é exaustiva e podem existir outras que sejam pertinentes para uma organização.

A.4.2 Entendendo as necessidades e as expectativas das partes interessadas

Convém que as organizações estabeleçam um entendimento das necessidades e expectativas das pessoas ou organizações que possam afetar, ser afetadas ou se perceberem afetadas pelo sistema de gestão de *compliance*.

Algumas são mandatórias porque precisam ser incorporadas como requisitos formais, como leis, regulamentos, permissões e licenças, e ações governamentais ou judiciais. Podem existir outros requisitos formais, não apresentados aqui, que sejam aplicados.

Outras necessidades e expectativas de uma parte interessada podem se tornar uma obrigação quando elas são especificadas, e a organização decide que irá adotá-las, voluntariamente, por meio de um acordo ou contrato. Uma vez que a organização tenha decidido sobre elas, elas se tornam obrigações de *compliance*.

Exemplos de partes interessadas externas incluem:

— agências governamentais e governos;

— órgãos regulatórios;

— clientes;

— parceiros de negócio;

— fornecedores;

— terceiras partes intermediárias;

— proprietários, acionistas e investidores;

— organizações não governamentais;

— sociedade e grupos comunitários;

— associações de negócios.

Exemplos de partes interessadas internas incluem:

— Órgão Diretivo;

— gestores;

— funcionários;

— funções internas como gestão de risco, controles internos, auditoria interna, e recursos humanos.

A.4.3 Determinando o escopo do sistema de gestão de *compliance*

Determinar o escopo de um sistema de gestão de *compliance* é o processo pelo qual as organizações estabelecem os limites físico e organizacional, onde o sistema de gestão de *compliance* será aplicado. Ao fazer isso, a organização tem a liberdade e a flexibilidade para escolher implementar o sistema de gestão de *compliance* em toda a organização, em uma unidade específica ou função específica dentro da organização.

Tipicamente, um sistema de gestão de *compliance* será implementado em toda a organização e, nos casos de grupos de organizações, em todo o grupo de organizações, para evitar padrões em duplicidade de condutas éticas e de *compliance*.

Convém que o escopo seja razoável e proporcional, considerando a natureza e a extensão dos riscos de *compliance* enfrentados pela organização.

Um entendimento do contexto e dos requisitos das partes interessadas pertinentes é uma consideração a ser contemplada quando do estabelecimento do escopo do sistema de gestão de *compliance* e quando determinando quais requisitos a organização irá adotar.

A.4.4 Sistema de gestão de *compliance*

Um sistema de gestão de *compliance* é uma estrutura que integra procedimentos, processos, políticas e estruturas essenciais para alcançar os resultados de *compliance* pretendidos, e agir para prevenir, detectar e responder a um não *compliance*.

Tipicamente, a estrutura de um sistema de gestão de *compliance* é uma questão estrutural: a infraestrutura necessária sobre a qual se constrói este sistema. Em seguida, ela precisa se tornar operacional por meio de toda a implementação de políticas, processos e procedimentos. Em seguida, isto necessita ser mantido e melhorado continuamente.

Existem muitos elementos para um sistema de gestão de *compliance*. Alguns elementos do sistema de gestão serão projetados para apoiar os comportamentos desejados, enquanto outros serão projetados para prevenir comportamentos indesejáveis. Alguns elementos são apenas para monitorar o desempenho do *compliance* da organização ou prover alertas caso o não *compliance* aconteça.

O sistema de gestão de *compliance* reconhecerá quais erros podem ocorrer e terá processos para assegurar que haja reações apropriadas. Uma reação apropriada incluirá processos de remediação, sistemas e partes impactadas.

Convém que o sistema de gestão de *compliance* seja baseado nos princípios de boa governança, proporcionalidade, integridade, transparência, responsabilização e sustentabilidade.

Convém que o sistema de gestão de *compliance* esteja disponível como informação documentada.

A.4.5 Obrigações de *compliance*

Convém que a organização considere as obrigações de *compliance* como uma base para estabelecer, desenvolver, implementar, avaliar, manter e melhorar seu sistema de gestão de *compliance*.

Os requisitos que uma organização, mandatoriamente deve cumprir podem incluir:

— leis e regulamentos;

— permissões, licenças ou outras formas de autorização;

— ordens, regras ou orientações emitidas por agências regulamentadoras;

— decisões de côrtes de justiça ou tribunais administrativos;

— tratados, convenções e protocolos.

Os requisitos que uma organização, voluntariamente, escolhe cumprir podem incluir:

— acordos com grupos comunitários ou organizações não governamentais;

— acordos com autoridades públicas e clientes;

— requisitos organizacionais, como políticas e procedimentos;

— princípios voluntários ou códigos de prática;

— rotulagem voluntária ou comprometimentos ambientais;

— obrigações decorrentes de acordos contratuais com a organização;

— normas setoriais e organizacionais pertinentes.

Convém que a organização identifique as suas obrigações de *compliance* por departamentos, funções e diferentes tipos de atividades organizacionais, para determinar quem é afetado por estas obrigações de *compliance*.

Os processos para obter informações sobre mudanças nas leis e em outras obrigações de *compliance* podem incluir:

— estar nas listas de endereços de órgãos regulamentadores pertinentes;

— membros de grupos profissionais;

— subscrição de serviços de informações pertinentes;

— participação em seminários e fóruns do setor;

— monitoramento de *sites* dos órgãos reguladores;

— reuniões com órgãos reguladores;

— arranjos com consultores jurídicos;

— monitoramento das fontes de obrigações de *compliance* (por exemplo, anúncios de órgãos regulamentadores, decisões judiciais).

Convém que uma abordagem de avaliação de risco seja tomada, isto é, convém que as organizações comecem com a identificação das obrigações de *compliance* mais importantes, que sejam pertinentes aos negócios, e então se concentrem em todas as outras obrigações de *compliance* (princípio de Pareto).

Quando apropriado, convém que a organização estabeleça e mantenha um único documento (como um registro ou uma anotação) estabelecendo todas as suas obrigações de *compliance* e tendo um processo para atualizar o documento regularmente.

Além de estabelecer as obrigações de *compliance*, convém que o documento inclua, mas não se limite a:

— o impacto das obrigações de *compliance*;

— a gestão das obrigações de *compliance*;

— os controles relacionados às obrigações de *compliance*;

— a avaliação de risco.

A.4.6 Avaliação de riscos de *compliance*

A avaliação de riscos de *compliance* constitui a base para a implementação do sistema de gestão de *compliance* e a locação de recursos e processos adequados e apropriados para gerenciar os riscos de *compliance* identificados.

Os riscos de *compliance* podem ser caracterizados pela probabilidade de ocorrência e as consequências do não *compliance* com a política e as obrigações de *compliance* da organização.

Os riscos de *compliance* incluem os riscos de *compliance* inerentes e os riscos de *compliance* residuais. Os riscos de *compliance* inerentes se referem a todos os riscos de *compliance* enfrentados por uma organização em uma situação descontrolada sem qualquer medida correspondente de tratamento dos riscos de *compliance*. Os riscos de *compliance* residuais são os riscos de *compliance* não controlados efetivamente pelas medidas existentes de tratamento de risco de *compliance* de uma organização.

Convém que a organização analise os riscos de *compliance* considerando as causas-raiz e as fontes do não *compliance* e as consequências destas, ao mesmo tempo em que inclui a probabilidade de que estas ramificações possam ocorrer. As consequências podem incluir, por exemplo, danos ambientais e pessoais, perdas econômicas, danos à reputação, mudanças administrativas e responsabilidades civis e criminais.

A identificação dos riscos de *compliance* inclui a identificação das fontes de risco de *compliance* e a definição das situações de risco de *compliance*. Convém que as organizações identifiquem as fontes de riscos de *compliance* dentro dos vários departamentos, funções e diferentes tipos de atividades organizacionais, de acordo com as responsabilidades do departamento, as responsabilidades profissionais e os diferentes tipos de atividades organizacionais. Convém que a organização identifique regularmente as fontes dos riscos de *compliance* e defina as correspondentes situações de riscos de *compliance* para cada fonte de risco de *compliance* de modo a desenvolver uma lista das fontes de risco de *compliance* e uma lista de situações de riscos de *compliance*.

A avaliação de risco envolve comparar o nível de risco de *compliance* que é aceitável pela organização com o nível de risco de *compliance* estabelecido na política de *compliance*.

Convém que os riscos de *compliance* sejam reavaliados periodicamente e quando houver:

— atividades, produtos ou serviços novos ou alterados;

— mudanças na estrutura ou estratégia da organização;

— mudanças externas significativas, como circunstâncias econômicas e financeiras, condições de *marketing*, responsabilidades e relacionamento com clientes;

— mudanças nas obrigações de *compliance*;

— fusões e aquisições;

— não *compliance*(s) (mesmo um simples incidente de não *compliance* pode constituir uma mudança material nas circunstâncias) e quase falha.

NOTA BRASILEIRA O termo “quase falha” foi o termo utilizado para tradução da expressão em inglês “*near misses*”.

A extensão e o nível de detalhe da avaliação dos riscos de *compliance* dependem da situação do risco, do contexto, do porte e dos objetivos da organização, e podem variar para subáreas específicas (por exemplo, ambiental, financeira, social).

A abordagem baseada no risco para a gestão do *compliance* não significa que para situações de baixo risco de *compliance*, o não *compliance* é aceito pela organização. Ele auxilia as organizações a focar a atenção primária e os recursos mais altos como uma prioridade, e, em última instância, cobrir todos os riscos de *compliance*. Todas os riscos/situações de *compliance* identificados estão sujeitos a monitoramento e tratamento.

Ao conduzir uma avaliação de riscos (ver ABNT NBR ISO 31000 para orientação), convém que seja dada atenção às técnicas apropriadas (como detalhado na IEC 31010).

A.5 Liderança

A.5.1 Liderança e comprometimento

A.5.1.1 Órgão Diretivo e Alta Direção

Um *compliance* efetivo requer um comprometimento ativo do Órgão Diretivo e da Alta Direção que permeia toda a organização.

É vital para o sistema de gestão de *compliance* que o Órgão Diretivo e a Alta Direção demonstrem, clara e visivelmente, seus comprometimentos para alcançar as metas do sistema de gestão de *compliance*.

O não *compliance* pode resultar em um impacto negativo para os negócios, como dano reputacional, perda de licença para operar, perda de oportunidade e custo significativo. Portanto, convém que o Órgão Diretivo e a Alta Direção reconheçam a importância estratégica de um sistema de gestão de *compliance* eficaz.

Este documento apresenta muitas maneiras da liderança demonstrar o seu comprometimento. O mais importante fundamento é por meio de um apoio ativo e visível para o estabelecimento e a manutenção do sistema de gestão de *compliance*.

O nível de comprometimento é indicado pelo grau do qual:

— o Órgão Diretivo e todos os níveis da administração demonstram ativamente o comprometimento para estabelecer, desenvolver, implementar, avaliar, manter e melhorar um sistema de gestão de *compliance* efetivo e com resultados por meio das suas ações e decisões;

— a política de *compliance* é formalmente aprovada pelo Órgão Diretivo;

— a Alta Direção assume a responsabilidade por assegurar que o comprometimento com o *compliance* da organização é totalmente realizado;

— todos os níveis da administração transmitem consistentemente, para todas as pessoas, uma mensagem clara (demonstrada por palavras e ações) que a organização cumprirá com as suas obrigações de *compliance*;

— o comprometimento com o *compliance* é comunicado amplamente para todo o pessoal e para as partes interessadas pertinentes, em uma declaração clara e convincente, apoiada pelas ações;

— a função de *compliance* tenha uma equipe com competência apropriada, independência e autoridade com o *status,* que reflita a importância de um *compliance* eficaz e que tenha acesso direto ao Órgão Diretivo;

— recursos adequados são alocados para estabelecer, desenvolver, implementar, avaliar, manter e melhorar uma sólida cultura de *compliance* por meio de atividades de conscientização e treinamento para todo o pessoal e partes interessadas pertinentes;

— políticas, processos e procedimentos refletem não apenas os requisitos legais, mas também códigos voluntários e os valores principais da organização;

— a organização atribui e exige responsabilização para o *compliance* a todos os gestores ao longo de todos os níveis da organização;

— uma análise crítica regular do sistema de gestão de *compliance* seja realizada (recomenda-se pelo menos anualmente);

— o desempenho do *compliance* da organização seja continuamente melhorado;

— a ação corretiva seja tomada em um tempo hábil;

— o Órgão Diretivo e a Alta Direção estejam seguindo o sistema de gestão de *compliance* da organização.

A.5.1.2 Cultura de *compliance*

Fatores que apoiam o desenvolvimento de uma cultura de *compliance* podem incluir:

— um conjunto de valores publicado de forma clara;

— uma gestão ativa e que visivelmente implementa e respeita os valores;

— consistência no tratamento das não *compliance*, independentemente da posição;

— mentoriamento, *coaching* e liderança pelo exemplo;

— uma apropriada avaliação na pré-contratação de pessoas potenciais para as funções críticas, incluindo *due diligence*;

— um programa de indução ou orientação que enfatize o *compliance* e os valores da organização;

— treinamento contínuo do *compliance*, incluindo atualizações para o treinamento de todas as pessoas e partes interessadas pertinentes;

— comunicação contínua sobre questões de *compliance*;

— sistemas de avaliação de desempenho que considerem a avaliação do comportamento do *compliance* e considerem o pagamento por desempenho para alcançar os resultados e os indicadores-chave de desempenho do *compliance*;

— um reconhecimento visível das realizações na gestão e nos resultados de *compliance*;

— um ágil e proporcional processo disciplinar para os casos de violações dolosas ou negligentes, das obrigações de *compliance*;

— uma clara relação entre a estratégia da organização e os papéis individuais, enfatizando o *compliance* como essencial para alcançar os resultados organizacionais;

— comunicação apropriada e aberta sobre *compliance*, tanto internamente como externamente.

A evidência sobre uma cultura de *compliance* é indicada pelo grau no qual:

— os itens anteriores estão implementados;

— as partes interessadas (especialmente as pessoas) acreditam que os itens anteriores foram implementados;

— o pessoal entende a relevância das obrigações de *compliance* relativas as suas próprias atividades como também as de sua unidade de negócios;

— ações corretivas para abordar não *compliance* são “de propriedade” e acionadas em todos os níveis apropriados da organização, conforme requerido;

— o papel da função de *compliance* e seus objetivos são valorizados;

— as pessoas estão capacitadas e encorajadas para levantarem preocupações de *compliance* aos níveis apropriados da direção, incluindo a Alta Direção e o Órgão Diretivo.

Convém que a organização:

a) meça a sua cultura de *compliance*;

b) busque informação de todo o pessoal para determinar se eles percebem o comprometimento do *compliance* pelo Órgão Diretivo, Alta Direção e pela gestão intermediária com o *compliance*;

c) estabeleça planos de ação baseados nos resultados dos indicadores de cultura de *compliance* da organização.

A.5.1.3 Governança de *compliance*

A governança de *compliance* está baseada nos seguintes princípios fundamentais.

A função de *compliance* tem acesso direto ao Órgão Diretivo e à Alta Direção. Eles podem se sobrepor a outros na organização, e convém que suas necessidades e comunicação sejam diretas com a pessoa ou pessoas que tenham a maior autoridade para agir. Isto beneficia diretamente o Órgão Diretivo e a Alta Direção, para que eles possam exercer as suas obrigações. Convém que este acesso seja planejado e sistemático. Por exemplo, a função de *compliance* pode ter um acesso direto ao CEO, e uma “linha paralela” de reporte ao comitê de auditoria, ao presidente do Órgão Diretivo ou a toda a direção.

Convém que a função de *compliance* seja independente e não seja conflitante com a estrutura organizacional ou outros elementos. Ela é livre para agir sem interferência da gestão de linha.

A função de *compliance* tem autoridade. A função de *compliance* não é uma posição júnior que possa ser anulada ou que tenha relatórios ou informações alteradas por aqueles que estão acima dela em autoridade. A função de *compliance* pode direcionar outras funções, conforme necessário. Convém que a função de *compliance* tenha “voz ativa”, para defender e apresentar quaisquer preocupações de *compliance*.

NOTA BRASILEIRA O termo “voz ativa” é uma expressão idiomática e foi utilizada neste contexto para assegurar que esta função será ouvida e respeitada, pois entende-se por voz ativa, a participação real e reconhecida no sistema de gestão de *compliance*.

A função de *compliance* tem recursos adequados para apoiar a organização na condução das responsabilidades e dos trabalhos necessários do sistema de gestão de *compliance*, sem restrições, incluindo o acesso à tecnologia que permite que o sistema de gestão de *compliance* seja efetivo e detalhado para apoiar a organização em alcançar os seus objetivos de *compliance*.

A.5.2 Política de *compliance*

A política de *compliance* estabelece o comprometimento e os princípios gerais para ações, para que uma organização alcance o *compliance*. Ela estabelece o nível de responsabilidade e de desempenho requerido, e estabelece as expectativas para as quais as ações serão avaliadas. Convém que a política seja apropriada às obrigações de *compliance* da organização, que surgem de suas atividades.

Convém que a política de *compliance* seja aprovada pelo Órgão Diretivo.

Convém que a política de *compliance* especifique:

— o contexto e a aplicação do sistema de gestão de *compliance* em relação ao porte, natureza e complexidade da organização e seu ambiente de operação;

— a abrangência na qual o *compliance* será integrado com outras funções, como governança, risco, auditoria e jurídico;

— os princípios nos quais as relações com as partes interessadas internas e externas são gerenciados.

Não convém que a política de *compliance* seja um documento único, mas convém que ela seja apoiada por outros documentos, incluindo processos e políticas operacionais.

Convém que a política de *compliance* seja traduzida em outros idiomas, se necessário.

Convém que a política de *compliance* seja apropriada às obrigações de *compliance* da organização, que surgem das atividades e do seu escopo.

Convém que no desenvolvimento da política de *compliance* sejam consideradas:

a) as obrigações locais, regionais ou internacionais específicas;

b) a cultura, os objetivos, as estratégias da organização e o enfoque da governança;

c) a estrutura da organização;

d) a natureza e o nível de riscos associados com o não *compliance*;

e) procedimentos e políticas internas, códigos e normas adotadas;

f) normas setoriais.

A política de *compliance* pode contemplar:

— uma declaração da missão;

— uma declaração geral da política;

— estratégias da gestão e a locação de recursos e responsabilidades;

— procedimentos-padrão de *compliance*;

— auditoria, *due diligence* e *compliance*.

A.5.3 Papéis, responsabilidades e autoridades

A.5.3.1 Órgão Diretivo e Alta Direção

O envolvimento ativo e a supervisão por um Órgão Diretivo é uma parte integral de um sistema de gestão de *compliance* eficaz. Isto ajuda a assegurar que o pessoal entende completamente, a política de *compliance* da organização e os procedimentos operacionais de *compliance*, e como estes se aplicam a seus cargos e que eles cumpram as obrigações de *compliance* eficazmente.

Para um sistema de gestão de *compliance* ser eficaz, o Órgão Diretivo e a Alta Direção precisam liderar pelo exemplo, aderindo e apoiando, ativa e visivelmente o *compliance* e o sistema de gestão de *compliance*.

Muitas organizações, dependendo do seu porte, também têm alguém que tem a responsabilidade global pela gestão do *compliance*, embora isto possa ser uma adição a outros papéis ou funções, incluindo os comitês existentes, as unidades organizacionais ou os elementos terceirizados para especialistas de *compliance*.

Convém que a Alta Direção encoraje o comportamento que cria e apoia o *compliance* e não convém que a Alta Direção tolere o comportamento que comprometa o *compliance*.

Convém que a Alta Direção assegure:

— o alinhamento do comprometimento da organização com *compliance* com seus valores, objetivos e estratégias de modo a posicionar o *compliance* adequadamente;

— o encorajamento de todo o pessoal para aceitar a importância de alcançar os objetivos de *compliance* para os quais eles tenham responsabilidade ou responsabilização;

— a criação de um ambiente onde o relato de um não *compliance* é encorajado e a pessoa que relatou esteja segura e livre de retaliações;

— que o *compliance* seja incorporado dentro da cultura da organização e às iniciativas de mudança de cultura;

— a identificação do não *compliance* e a ação imediata para corrigi-la ou para tratá-las;

— que as metas e objetivos operacionais não comprometam o comportamento de *compliance*.

Convém que a Alta Direção analise criticamente o desempenho do sistema de gestão de *compliance* em intervalos planejados (por exemplo, trimestral ou mensalmente), referenciando KPI e outras informações-chave para assegurar que o sistema de gestão de *compliance* esteja alcançando seus objetivos.

A eficácia de um sistema de gestão de *compliance* requer um comprometimento da Alta Direção, por meio do estabelecimento de padrões e do exercício de supervisão razoável. Convém que a Alta Direção tenha conhecimento sobre o conteúdo e a operação do sistema de gestão de *compliance* e convém que ele assegure de que a organização tenha processos adequados para um sistema de gestão de *compliance* eficaz.

A.5.3.2 Função de *compliance*

Muitas organizações tem uma pessoa dedicada (por exemplo, *compliance officer*) responsável pela gestão do *compliance* no dia-a-dia e algumas têm um comitê de *compliance* interfuncional, para coordenar o *compliance* em toda a organização. A função de *compliance* trabalha em conjunto com a gestão.

Nem todas as organizações criarão uma função de *compliance* discreta; algumas atribuirão esta função a uma posição já existente ou irão terceirizar esta função. Ao terceirizar, convém que a organização considere não atribuir toda a função de *compliance* para terceiras partes. Mesmo se ela terceirizar parte desta função, convém que ela considere manter a autoridade sobre ela e que supervisione estas funções.

Ao alocar a responsabilidades pelo sistema de gestão de *compliance*, convém que seja considerada a possibilidade de assegurar que a função de *compliance* demonstre:

— integridade e comprometimento com o *compliance*;

— comunicação eficaz e habilidades para influenciar;

— uma capacidade e posição para comandar a aceitação de conselhos e orientações;

— competência pertinente no projeto, na implementação e na manutenção do sistema de gestão do *compliance*;

— assertividade, conhecimento do negócio e experiência para testar e desafiar;

— uma estratégia, e uma abordagem proativa para o *compliance*;

— tempo suficiente disponível para cumprir as necessidades da função.

Convém que a função de *compliance* tenha autoridade, *status* e independência. Autoridade significa que a função de *compliance* é atribuída de grande poder pelo Órgão Diretivo e pela Alta Direção. *Status* significa que outras pessoas estão na posição de ouvir e respeitar a sua opinião. Independência significa que a função de *compliance* não está, na medida do possível, envolvida pessoalmente nas atividades que estão expostas a riscos de *compliance*.

Convém que a função de *compliance* esteja livre de conflitos de interesses para cumprir integralmente o seu papel.

A.5.3.3 Direção

Não convém que as responsabilidades da Alta Direção sejam vistas como absolvendo outros níveis da gestão das suas responsabilidades pelo *compliance*, pois todos os gestores têm um papel a desempenhar em relação ao sistema de gestão de *compliance*. Portanto, é importante que as suas respectivas responsabilidades estejam claramente definidas e incluídas nas descrições de suas funções.

As responsabilidades dos gestores pelo *compliance* serão, necessariamente, de acordo com os níveis de autoridades, influência e outros fatores, como a natureza e o porte da organização. Entretanto, algumas responsabilidades provavelmente serão comuns em uma variedade de organizações.

A.5.3.4 Pessoal

O *compliance* com as obrigações de *compliance* é esperado de todas as pessoas.

Convém que o pessoal se assegure de que eles estejam cientes das suas responsabilidades pelo *compliance* e que as cumpram eficazmente. Eles serão apoiados nesta atividade por meio dos elementos do sistema de gestão de *compliance*, como treinamento, políticas e procedimentos, e do código de conduta.

Convém que o pessoal seja proativo quanto à sua contribuição de ideias e melhorias que possam auxiliar no desempenho do sistema de gestão do *compliance*.

A.6 Planejamento

A.6.1 Ações para abordar riscos e oportunidades

O planejamento do sistema de gestão de *compliance* é conduzido em um nível estratégico, em comparação com o planejamento operacional feito para o planejamento e controle operacional.

O propósito do planejamento é para antecipar cenários e consequências potenciais e é, como tal, preventivo. Com base nos resultados de uma avaliação de riscos de *compliance*, convém que a organização planeje como abordar os efeitos indesejados antes que eles ocorram e como se beneficiar de condições ou circunstâncias favoráveis que possam apoiar a eficácia do sistema de gestão de *compliance*.

Convém que o planejamento também inclua situação sobre como incorporar as ações consideradas necessárias ou benéficas, para o sistema de gestão de *compliance*, dentro das atividades e processos do negócio. A incorporação pode tanto ser alcançada por meio da definição dos objetivos, controle operacional ou outras Seções específicas (por exemplo, provisão de recursos, competências). Convém que medidas para avaliar a eficácia do sistema de gestão de *compliance* também sejam planejadas. Isto pode incluir monitoramento, técnicas de medição, auditoria interna ou análise crítica pela direção.

A.6.2 Objetivos de *compliance* e planejamento para alcançá-los

Convém que os objetivos sejam especificados de forma que permitam que os resultados sejam medidos.

Um exemplo de um objetivo de *compliance*: realizar treinamento de *compliance* para o pessoal pertinente, pelo menos anualmente.

Convém que as ações necessárias para alcançar os objetivos (isto é, “o que”), um período de tempo específico (isto é, “quando”) e o responsável (isto é, “quem”) sejam determinadas. Convém que a situação e o progresso dos objetivos de *compliance* sejam periodicamente monitorados, registrados, avaliados e atualizados, conforme requerido.

A.7 Apoio

A.7.1 Recursos

Os recursos incluem recursos financeiros, humanos e técnicos, assim como o acesso a aconselhamento externo e habilidades especializadas, infraestrutura organizacional, desenvolvimento profissional, tecnologia e material de referência contemporâneo sobre gestão de *compliance* e obrigações legais.

A.7.2 Competência

A.7.2.1 Generalidades

O termo “competência” significa a capacidade de aplicar conhecimentos e a habilidade para alcançar resultados pretendidos. Competência requer conhecimentos, experiência e habilidades para que a pessoa possa desempenhar sua função de maneira eficaz. Convém que a organização determine para todo o pessoal a experiência e o conhecimento necessários para cumprir as suas atribuições, para que a organização possa prover seus produtos e serviços ao cliente. Convém que a organização estabeleça evidências de competência (por exemplo, descrição de cargo, declaração de posição), que possam ser considerados quando do preenchimento destas posições.

Convém que medidas (por exemplo, treinamento) sejam tomadas para assegurar que as competências existentes sejam mantidas e que novas competências sejam adquiridas. Convém que existam documentação adequada de competências, assim como medidas tomadas para manter ou adquirir estas competências.

A.7.2.2 Processo de contratação

Antes de contratar pessoas ou de promover o pessoal existente, convém que a organização realize uma *due dilingence*, a qual pode incluir verificações de referências ou de antecedentes.

A.7.2.3 Treinamento

Convém que o Órgão Diretivo, a direção e o pessoal que têm obrigações de *compliance* sejam competentes para cumpri-las eficazmente. O atendimento da competência pode ser alcançado de várias maneiras, incluindo habilidades e conhecimentos requeridos por meio da educação, treinamento ou experiência de trabalho.

O objetivo de um programa de treinamento é assegurar que as pessoas são competentes para cumprir os seus papéis de forma consistente com a cultura de *compliance* da organização e com o seu comprometimento com o *compliance*.

Um treinamento adequadamente projetado e executado pode prover uma maneira eficaz para o pessoal comunicar riscos de *compliance* previamente não identificados.

Convém que a educação e o treinamento sejam:

— quando apropriados, com base em uma avaliação de lacunas de conhecimento e competência dos funcionários;

— suficientemente flexíveis para responder a uma série de técnicas para acomodar as diferentes necessidades das organizações e do pessoal;

— projetados, desenvolvidos e disponibilizados por pessoal qualificado e experiente;

— disponibilizados no idioma local, quando aplicável;

— avaliados e estimados quanto a sua eficácia, em bases regulares.

Treinamento interativo pode ser a melhor forma de treinamento se o não *compliance* puder resultar em sérias consequências.

Convém que a organização proveja treinamento nas áreas onde a má conduta tiver ocorrido.

Convém que o retreinamento em *compliance* seja considerado sempre que ocorrer:

— uma mudança de posição ou de responsabilidades;

— uma mudança nos procedimentos, processos e políticas internas;

— uma mudança na estrutura organizacional;

— uma mudança nas obrigações de *compliance*, especialmente nos requisitos legais e nos requisitos de partes interessadas;

— uma mudança nas atividades, produtos ou serviços;

— uma questão que surja do monitoramento, da auditoria, da análise crítica, das reclamações e não *compliance*, incluindo retroalimentação das partes interessadas.

A.7.3 Conscientização

A conscientização envolve assegurar que as políticas de *compliance* sejam tornadas acessíveis e disponíveis a todo o pessoal e que elas são entendidas.

As questões de conscientização de *compliance* podem ser alcançadas por métodos como, mas não limitados a:

— treinamento (presencial ou *on-line*);

— comunicação da Alta Direção;

— materiais de referência fáceis de seguir e prontamente acessíveis;

— atualizações regulares das questões de *compliance*.

Comunicando o comprometimento com o *compliance*:

— construa e motive o pessoal a adotar o sistema de gestão de *compliance*;

— encoraje os pessoal a apresentarem sugestões que facilitem a melhoria contínua no desempenho do *compliance*.

A.7.4 Comunicação

Convém que uma abordagem prática para uma comunicação externa, visando todas as partes interessadas, seja adotada de acordo com a política da organização.

As partes interessadas podem incluir órgãos reguladores, clientes, parceiros de negócio, fornecedores, investidores, serviços de emergência, organizações não governamentais e vizinhos.

Convém que a organização aloque recursos apropriados e pessoas com conhecimento pertinente para coordenar e facilitar a interação regulatória.

Os métodos de comunicação podem incluir *sites* e *e-mails*, comunicados à imprensa, anúncios e boletins periódicos, relatórios anuais (ou outra periodicidade), discussões informais, dias abertos, grupos de focos, diálogos com a comunidade, envolvimento em eventos da comunidade e linhas telefônicas diretas. Estas abordagens podem encorajar o entendimento e a aceitação do comprometimento da organização com o *compliance*.

Convém que as comunicações estejam alinhadas com os princípios de transparência, conveniência, credibilidade, capacidade de resposta rápida, acessibilidade e clareza.

A.7.5 Informação documentada

A.7.5.1 Generalidades

Informação documentada pode incluir:

— os procedimentos e as políticas de *compliance* da organização;

— os objetivos, as metas, a estrutura e o conteúdo do sistema de gestão de *compliance*;

— a alocação de papéis e a responsabilidade pelo *compliance*;

— um registro das obrigações de *compliance* pertinentes;

— os registros dos riscos de *compliance* e a priorização do tratamento baseados no processo de avaliação de risco de *compliance*;

— um registro dos não *compliance*, investigações e quase falha;

— planos anuais de *compliance*;

— registros de pessoal, incluindo, mas não se limitando, a registros de treinamento;

— o processo de auditoria, o cronograma de auditoria e os registros de auditoria associados.

Informação documentada pode incluir assuntos relacionados aos requisitos de notificação regulatórios. Informação documentada pode contemplar todos os tipos de mídia (digital e não digital).

A.7.5.2 Criando e atualizando informação documentada

Convém que a informação documentada seja atualizada para refletir as mudanças internas e externas, para assegurar que elas sejam de uso corrente e atualizadas.

A.7.5.3 Controle da informação documentada

Informação documentada pode ser preparada com o propósito de obter aconselhamento legal e, portanto, podendo ser objeto de privilégio legal.

A.8 Operação

A.8.1 Planejamento e controle operacional

Um sistema de gestão de *compliance* bem projetado compreende medidas (por exemplo, políticas, processos, procedimentos) que fornecem tanto o conteúdo quanto o efeito para uma cultura de *compliance*. Estas medidas abordam e visam reduzir os riscos identificados como parte do processo de avaliação de riscos de *compliance*.

Um elemento básico do controle operacional é um código de conduta que estabelece, entre outras coisas, o total comprometimento da organização com as obrigações de *compliance* pertinentes. Convém que um código de conduta seja aplicável a todo o pessoal e seja acessível para eles. Convém que baseado e derivado do código de conduta, medidas de *compliance* sejam incorporadas no dia-a -dia das operações da organização para fomentar uma cultura de *compliance*.

Controles operacionais são requeridos para situações relacionadas aos processos de negócio onde uma ausência de controles pode levar a desvios da política de *compliance* ou a uma violação das obrigações de *compliance*. Estas situações podem estar relacionadas a todas as atividades, situações ou processos (por exemplo, produção, instalação, serviços, manutenção) ou aos parceiros de negócios, fornecedores ou vendedores.

O grau de controle pode variar dependendo de vários fatores, como a importância ou complexidade das funções desempenhadas, as consequências potenciais de não *compliance* ou o apoio técnico envolvido ou disponível.

Quando os controles operacionais falham, são necessárias ações para tratar quaisquer resultados ou efeitos indesejados.

Se houver qualquer uso de terceiras partes ou de processos terceirizados nas atividades da organização, convém que a organização conduza uma *due diligence* eficaz para assegurar que as suas normas e comprometimento com o *compliance* não serão desconsiderados. Um exemplo de terceiras partes se relaciona ao provimento de produtos e serviços, e à distribuição de produtos. Convém que a organização assegure que acordos apropriados de níveis de serviços (SLA), especificando as obrigações de *compliance* para o serviço prestado, sejam concluídos.

NOTA BRASILEIRA A sigla SLA é utilizada como abreviação de Acordo de Níveis de Serviços. Este é o acordo de níveis de serviços firmado entre o cliente e o prestador de serviço.

Um processo bem projetado de terceirização considera o seguinte:

— *due diligence* inicial e programada;

— implementação de controles apropriados;

— realização de monitoramento contínuo;

— uma análise crítica apropriada dos acordos legais/contratuais;

— consideração sobre os SLA;

— utilização de terceiras partes certificadas neste documento.

Ao fazer um contrato com terceiras partes, convém que a organização implemente controles para assegurar que a aquisição, os aspectos operacionais, comerciais e outros aspectos não financeiros de suas atividades estejam sendo adequadamente gerenciados. Dependendo do porte da organização e da transação, a aquisição, os controles operacionais, comerciais e outros controles não financeiros implementados por uma organização podem reduzir os riscos de *compliance*.

A.8.2 Estabelecendo controles e procedimentos

Controles eficazes são necessários para assegurar que as obrigações de *compliance* da organização sejam atendidas, e que os não *compliance*s sejam prevenidos, detectados e corrigidos. Convém que controles sejam projetados com rigor suficiente para facilitar o alcance das obrigações de *compliance* que são particulares às atividades e ao ambiente operacional da organização. Convém que estes controles, quando possível, sejam incorporados aos processos normais da organização.

Os controles podem incluir:

— políticas operacionais, processos, procedimentos e instruções de trabalho documentados claros, práticos e fáceis de serem adotados;

— sistemas e relatórios de exceções;

— aprovações;

— segregação de responsabilidades e papéis incompatíveis;

— processos automatizados;

— planos anuais de *compliance*;

— planos de desempenho do pessoal;

— avaliações e auditorias de *compliance*;

— demonstração de comprometimento da direção e comportamento exemplar, a outras medidas para promover o comportamento de *compliance*;

— comunicação frequente, ativa e aberta sobre o comportamento esperado do pessoal (normas e valores, códigos de conduta).

Convém que, ao desenvolver procedimentos para apoiar a gestão do *compliance*, sejam observadas as seguintes considerações:

— integração das obrigações de *compliance* nos procedimentos, incluindo sistemas computadorizados, formulários, sistemas de relatório, contratos e outras documentações legais;

— consistência com outras análises críticas e funções de controles dentro da organização;

— medição e monitoramento contínuo;

— avaliação e relatórios (incluindo a supervisão da direção) para assegurar de que o pessoal cumpra os procedimentos;

— acordos específicos para identificar, reportar e escalonar os casos de não *compliance* e dos riscos de não *compliance*.

A.8.3 Levantando preocupações

Quando apropriado, convém que a escala seja feita à Alta Direção e ao Órgão Diretivo, incluindo os comitês pertinentes.

Mesmo quando não requerido pela regulamentação local, convém que as organizações considerem desenvolver um mecanismo de denúncia para permitir o anonimato ou a confidencialidade, pelo qual o pessoal da organização e agentes possam reportar ou procurar orientação de não *compliance*, sem medo de retaliação.

Para mais orientações sobre sistemas de gestão de denúncias, ver ISO 37002.

A.8.4 Processo de investigação

Uma característica de um sistema de gestão de *compliance* eficaz é um mecanismo que funciona bem para uma investigação completa e em tempo hábil de quaisquer alegações ou suspeitas de má conduta pela organização, de seu pessoal ou de terceiras partes pertinentes. Isto inclui a documentação de resposta da organização, incluindo qualquer medida disciplinar ou de remediação tomada, e de revisões do sistema de gestão de *compliance* considerando as lições aprendidas.

Um mecanismo de investigação eficaz identifica as causas-raiz da má conduta, das falhas de responsabilização e das vulnerabilidades do sistema de gestão de *compliance*, entre os gestores,

a Alta Direção e o Órgão Diretivo. Uma análise cuidadosa da causa-raiz contempla a extensão e a abrangência do não *compliance*, o número e o nível do pessoal envolvido, a duração e a frequência do não *compliance*.

Convém que as organizações verifiquem se as investigações são isentas e independentes. Convém que elas considerem, quando apropriado, a criação de comitês independentes para supervisionar a investigação e assegurar a sua independência e completeza.

Convém que a organização estabeleça um mecanismo de relatório sobre as investigações, incluindo o nível ao qual as constatações das investigações serão reportadas.

NOTA As organizações são algumas vezes obrigadas por lei a reportar um não *compliance*. Nesses casos, as autoridades regulamentadoras são informadas de acordo com os regulamentos aplicáveis, ou conforme acordado de outra forma.

Mesmo se as organizações não forem obrigadas por lei a relatar um não *compliance*, elas podem considerar a autodivulgação do não *compliance* às autoridades regulamentadoras, para mitigar as consequências do não *compliance*.

A.9 Avaliação de desenvolvimento

A.9.1 Monitoramento, medição, análise e avaliação

A.9.1.1 Generalidades

O monitoramento é o processo de coleta de informação com o propósito de avaliar a eficácia do sistema de gestão de *compliance* e o desempenho do *compliance* da organização.

O monitoramento do sistema de gestão de *compliance* tipicamente inclui:

— a eficácia do treinamento;

— a eficácia dos controles (por exemplo, por amostra de resultado de testes);

— a locação eficaz de responsabilidades para o cumprimento das obrigações de *compliance*;

— a atualização das obrigações de *compliance*;

— a eficácia no tratamento das falhas de *compliance* identificadas previamente;

— as situações onde as inspeções de *compliance* internas não são desempenhadas conforme programadas;

— as análises críticas das estratégias de negócio comparadas com os riscos de *compliance* para permitir atualizações apropriadas.

O monitoramento do desempenho de *compliance* tipicamente considera:

— o não *compliance* e a “quase falha” (por exemplo, incidentes sem efeitos adversos);

— os casos onde as obrigações de *compliance* não são cumpridas;

— os casos onde os objetivos não são alcançados;

— a situação da cultura de *compliance*;

— o estabelecimento de indicadores de liderança e de atraso.

A.9.1.2 Fontes de retroalimentação sobre o desempenho do *compliance*

As fontes incluem:

— pessoal (por exemplo, por meio de canais de denúncia, canais de ajuda, retroalimentação, caixa de sugestão);

— clientes (por exemplo, por meio de um sistema de tratamento de reclamações);

— terceiras partes;

— fornecedores;

— parceiros de negócio;

— órgãos reguladores;

— processo de controle de registro e registros de atividades (incluindo tanto o registro em papel como em computador).

A retroalimentação sobre o desempenho de *compliance* pode incluir:

— questões de *compliance*;

— não *compliance* e preocupações de *compliance*;

— questões de *compliance* emergentes;

— mudanças organizacionais e regulatórias em andamento;

— comentários sobre o desempenho e a eficácia do *compliance*.

Existem vários métodos para coletar informações. Cada um dos métodos listados a seguir é pertinente em diferentes circunstâncias e convém que se tome cuidado para selecionar a variedade de ferramentas apropriadas ao porte, escala, natureza e complexidade da organização.

A coleta da informação pode incluir:

— relatórios *ad hoc* sobre não *compliance* à medida que os não *compliance* surgem ou são identificados;

— informação obtida por meio de linhas diretas, reclamações e outras formas de retroalimentação, incluindo denúncias;

— discussões informais, reuniões e grupos de discussão;

— amostragem e testes de integridade, como compras misteriosas;

— resultados de pesquisa de percepção;

— observações diretas, entrevistas formais, inspeções e visitas às instalações;

— auditorias e análises críticas;

— questionários das partes interessadas, solicitações de treinamento e retroalimentação apresentada durante o treinamento (particularmente aquelas do empregado).

Convém que um sistema seja desenvolvido para classificar, armazenar e recuperar a informação.

Convém que os sistemas de gestão de informações capturem tanto as reclamações quanto as manifestações para permitir a classificação e a análise daquelas que se relacionam com o *compliance*. Convém que análise considere os problemas sistêmicos e recorrentes para retificação ou melhoria, pois estes provavelmente podem representar riscos de *compliance* significativos para a organização e podem ser mais difíceis de identificar.

Os critérios para classificação das informações podem incluir:

— fonte;

— departamento;

— descrição do não *compliance*;

— referências obrigatórias;

— indicadores;

— severidade;

— impacto real ou potencial.

A.9.1.3 Desenvolvendo os indicadores

Convém que este processo considere os resultados da avaliação dos riscos de *compliance* para assegurar que os indicadores se relacionem às características pertinentes dos riscos de *compliance* da organização. A questão do que e como medir o desempenho do *compliance* pode ser desafiador em alguns aspectos, porém é, entretanto, uma parte vital para demonstrar a eficácia do sistema de gestão de *compliance*. Além disso, os indicadores necessários irão variar com a maturidade da organização e com o tempo e abrangência de programas novos ou revisados que estiverem sendo implementados.

Os indicadores podem incluir:

— o percentual de pessoas efetivamente treinadas;

— a frequência de contato por órgãos reguladores;

— o uso de mecanismos de retroalimentação (incluindo comentários sobre o valor desses mecanismos pelos usuários).

Os indicadores reativos podem incluir:

— questões e não *compliance* identificados, reportados por tipo, área e frequência;

— as consequências do não *compliance*, que podem incluir uma avaliação do impacto resultante sobre compensação monetária, multas e outras penalidades, custo da remediação, reputação ou custo do tempo do pessoal;

— a quantidade de tempo gasta para reportar e tomar a ação corretiva.

Os indicadores preditivos podem incluir:

— riscos de não *compliance* medidos como o potencial de perdas/ganhos dos objetivos (receita, saúde e segurança, reputação, entre outros) ao longo do tempo;

— tendências do não *compliance* (a taxa de *compliance* esperada baseada nas tendências passadas).

A.9.1.4 Relatório de *compliance*

Embora o relatório de problemas recorrentes e sistemáticos seja particularmente importante, um não *compliance* pode ser de igual preocupação se for crítico ou deliberativo. Mesmo uma pequena falha pode indicar uma séria fragilidade no processo atual e no sistema de gestão de *compliance*. Caso não seja reportado em um tempo hábil, pode ser entendido como uma falha sem importância e pode resultar que esta falha se torne um problema sistemático.

Convém que os relatórios de *compliance* incluam:

— quaisquer assuntos que a organização seja obrigada a notificar para qualquer autoridade regulamentadora;

— mudanças nas obrigações de *compliance*, seus impactos sobre a organização e as ações propostas em andamento para cumprir as novas obrigações;

— medição do desempenho do *compliance*, incluindo não *compliance* e melhoria contínua;

— número e detalhes de possíveis não *compliance*s e subsequente análise deles;

— ações corretivas tomadas;

— informações sobre a eficácia do sistema de gestão de *compliance*, alcances e tendências;

— contatos e desenvolvimento nas relações com órgãos reguladores;

— resultados de auditorias, assim como atividades de monitoramento ;

— monitoramento da execução completa dos planos de ação, especialmente aqueles derivados dos relatórios de auditoria ou de requisitos regulamentadores, ou ambos.

Convém que a política de *compliance* promova o reporte imediato de assuntos críticos que surjam fora dos prazos para relatórios regulares.

A.9.1.5 Manutenção de registros

Convém que a manutenção dos registros inclua os registros e a classificação das questões de *compliance* e os não *compliance*s identificados, como também os passos tomados para resolvê-los.

Convém que os registros sejam armazenados de forma que assegure que eles permaneçam legíveis, prontamente identificáveis e recuperáveis.

Convém que estes registros sejam protegidos contra quaisquer inclusão, exclusão, modificação, uso não autorizado ou ocultação.

Os registros do sistema de gestão de *compliance* da organização podem incluir:

— informação sobre o desempenho do *compliance*, incluindo os relatórios de *compliance*;

— detalhes de não *compliance* e ações corretivas;

— resultados de análises críticas e auditorias do sistema de gestão de *compliance* e as ações tomadas.

A.9.2 Auditoria interna

Convém que as funções de auditoria, internas ou externas, sejam livres de conflitos de interesse e independentes para cumprir integralmente o seu papel.

Ver ABNT NBR ISO 19011 para informações sobre como conduzir uma auditoria de um sistema de gestão.

A.9.3 Análise crítica pela direção

Convém que a análise crítica pela direção também inclua recomendações sobre:

— as necessidades de mudanças na política de *compliance*, e seus objetivos associados, sistemas, estrutura e pessoal;

— as mudanças nos processos de *compliance* para assegurar a integração eficaz com as práticas e sistemas operacionais;

— as áreas a serem monitoradas para potenciais não *compliances*;

— as ações corretivas relacionadas a não *compliance*;

— as lacunas, ou as falhas nos sistemas de *compliance* atuais e iniciativas de melhoria contínua de longo prazo;

— o reconhecimento de comportamentos exemplares de *compliance* e dentro da organização.

Convém que uma cópia dos resultados documentados e de quaisquer recomendações da análise crítica pela direção seja fornecida ao Órgão Diretivo.

A.10 Melhoria

A.10.1 Melhoria contínua

A eficácia de um sistema de gestão de *compliance* é caracterizada pelo fato de que ele tem a capacidade de melhorar continuamente e evoluir. Os ambientes interno e externo da organização e os negócios mudam ao longo do tempo, assim como a natureza de seus clientes e as obrigações de *compliance* aplicáveis.

Convém que a eficácia e a adequação do sistema de gestão de *compliance* sejam avaliadas de forma contínua e regular, por meio de vários métodos, por exemplo, análises críticas ou por auditorias internas.

Convém que a organização estabeleça medidas para analisar criticamente o seu sistema de gestão de *compliance* e para assegurar que ele permaneça atual e atenda ao propósito. Ao determinar a extensão e a escala de tempo das ações que apoiam a melhoria contínua, convém que a organização considere o seu contexto, os fatores econômicos e outras circunstâncias pertinentes.

Algumas organizações realizam pesquisas junto ao pessoal para medir a cultura de *compliance* e avaliar a robustez dos controles. Fontes adicionais de informação para melhoria contínua podem

ser os resultados de pesquisas de clientes, dos relatórios de levantamento de preocupações, do monitoramento regular, das auditorias periódicas ou das análises críticas pela direção.

Convém que a organização considere os resultados e as saídas de avaliações para determinar se há a necessidade ou oportunidade de mudança do sistema de gestão do *compliance*.

Para ajudar a assegurar que a integridade do sistema de gestão de *compliance* e a sua eficácia seja mantida, convém que as mudanças em elementos individuais do sistema de gestão considerem a dependência e o impacto destas mudanças sobre a eficácia do sistema de gestão como um todo.

Ao realizar mudanças no sistema de gestão de *compliance*, convém que a organização considere as implicações destas mudanças no sistema de gestão de *compliance*, suas operações, a disponibilidade de recursos, as avaliações de risco de *compliance*, as obrigações de *compliance* da organização e seus processos de melhoria contínua.

A.10.2 Não conformidade e ação corretiva

A falha em prevenir ou detectar um não *compliance* pontual não significa necessariamente que o sistema de gestão de *compliance* não seja geralmente eficaz na prevenção e detecção de um não *compliance*.

Informações sobre análise de uma não conformidade ou um não *compliance* podem ser usadas para considerar:

— a avaliação do desempenho dos produtos e serviços;

— a melhoria ou a reprojeção dos produtos e serviços;

— as mudanças nas práticas e procedimentos organizacionais;

— o retreinamento das pessoas;

— a reavaliação da necessidade de informar as partes interessadas;

— o provimento de aviso prévio sobre um potencial não *compliance*;

— a reprojeção ou a análise crítica dos controles;

— o reforço das etapas de notificação e de escalonamento (interno e externo);

— a comunicação de fatos relacionados ao não *compliance* e a posição de organização em relação ao não *compliance*.

Convém que a organização identifique as causas-raiz do não cumprimento das políticas ou dos procedimentos, ou ambos, que contribuíram para a má conduta, e atualize a política e o procedimento baseados nas lições aprendidas.

Bibliografia

[1] ABNT NBR ISO 9000, *Sistemas de gestão da qualidade – Fundamentos e vocabulário*

[2] ABNT NBR ISO 9001, *Sistemas de gestão da qualidade – Requisitos*

[3] ABNT NBR ISO 14001, *Sistemas de gestão ambiental – Requisitos com orientações para uso*

[4] ABNT NBR ISO 19011, *Diretrizes para auditoria de sistemas de gestão*

[5] ABNT NBR ISO 22000, *Sistemas de gestão de segurança de alimentos – Requisitos para qualquer organização na cadeia produtiva de alimentos*

[6] ABNT NBR ISO 26000, *Diretrizes sobre responsabilidade social*

[7] ABNT NBR ISO/IEC 27001, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos*

[8] ABNT NBR ISO 31000, *Gestão de riscos – Diretrizes*

[9] IEC 31010, *Risk management – Risk assessment techniques*

[10] ABNT NBR ISO 37001, *Sistemas de gestão antissuborno – Requisitos com orientações para uso*

[11] ISO 37002, *Whistleblowing management systems – Guidelines*

[12] ABNT ISO Guia 73, *Gestão de riscos – Vocabulário*