Pesquisa Maturidade do Compliance no Brasil

2ª edição

O futuro do compliance

www.kpmg.com.br

Índice

Introdução

O investimento em *compliance*

Atualmente as empresas têm o desafio de enfrentar diversas mudanças regulatórias e de negócios, as quais estão atribuindo novas exigências à área de Compliance. O ritmo das mudanças regulatórias e a convergência da regulamentação global, atrelados à concorrência de novas empresas, ao aumento da pressão dos *stakeholders* e *shareholders* e ao rápido avanço tecnológico criaram um ambiente complexo para os Compliance Officers em todas as indústrias. Além deste desafio está o risco dos danos à reputação e sanções financeiras significativas que frequentemente acompanham as falhas de *compliance*.

Para algumas empresas, os custos de *compliance* e riscos inerentes ditaram mudanças significativas nas operações de negócios. Atualmente os executivos estão vendo o *compliance* como um investimento e não como simplesmente um custo. Antecipar riscos e atender às exigências normativas tornam o *compliance* cada vez mais integrado aos objetivos estratégicos das empresas.

Essas mudanças também aumentaram a importância e a autoridade do diretor de Compliance (CCO – Chief Compliance Officer) e elevaram a importância de uma governança eficaz, gestão de riscos proativa e necessidade de melhoria contínua de *compliance*. Os CCOs estão no centro de uma estrutura de *compliance* que exige a capacidade de trabalhar em todas as funções e fornece uma oportunidade de olhar a amplitude dos riscos enfrentados pelas empresas.

Isso significa que a área de Compliance deve estar idealmente integrada em toda a empresa e posicionada para contribuir com as decisões de negócios e se adaptar rapidamente às constantes mudanças inerentes ao negócio. Com uma maior integração e agilidade, os líderes de *compliance* podem tomar medidas imediatas para melhorar a efetividade e eficiência de *compliance*.

O avanço do Programa de Compliance

Uma estrutura de *compliance* engloba vários componentes que contribuem na prevenção, detecção e resposta nas três "linhas de defesa". Em uma estrutura de *compliance*, os responsáveis pelos processos de negócios são a primeira linha de defesa, as funções de *compliance* e de gestão de riscos centralizada são a segunda linha de defesa e a auditoria interna é a terceira linha. Cada linha desempenha um papel importante na estrutura e governança de Compliance. O modelo de três linhas de defesa ajuda as empresas a promover a agilidade de *compliance*, identificar riscos emergentes e esclarecer os pontos fortes e fracos do Programa de Compliance.

A KPMG desenvolveu uma estrutura de Programa de Compliance que consiste em oito elementos, com a cultura e governança ao centro.

Esta estrutura integra as sugestões de Programas de Compliance alinhados às boas práticas de *compliance* disponíveis globalmente e vai além desses conceitos para incorporar requisitos e orientações regulamentares de órgãos regulatórios multissetoriais e principais iniciativas de *compliance*.

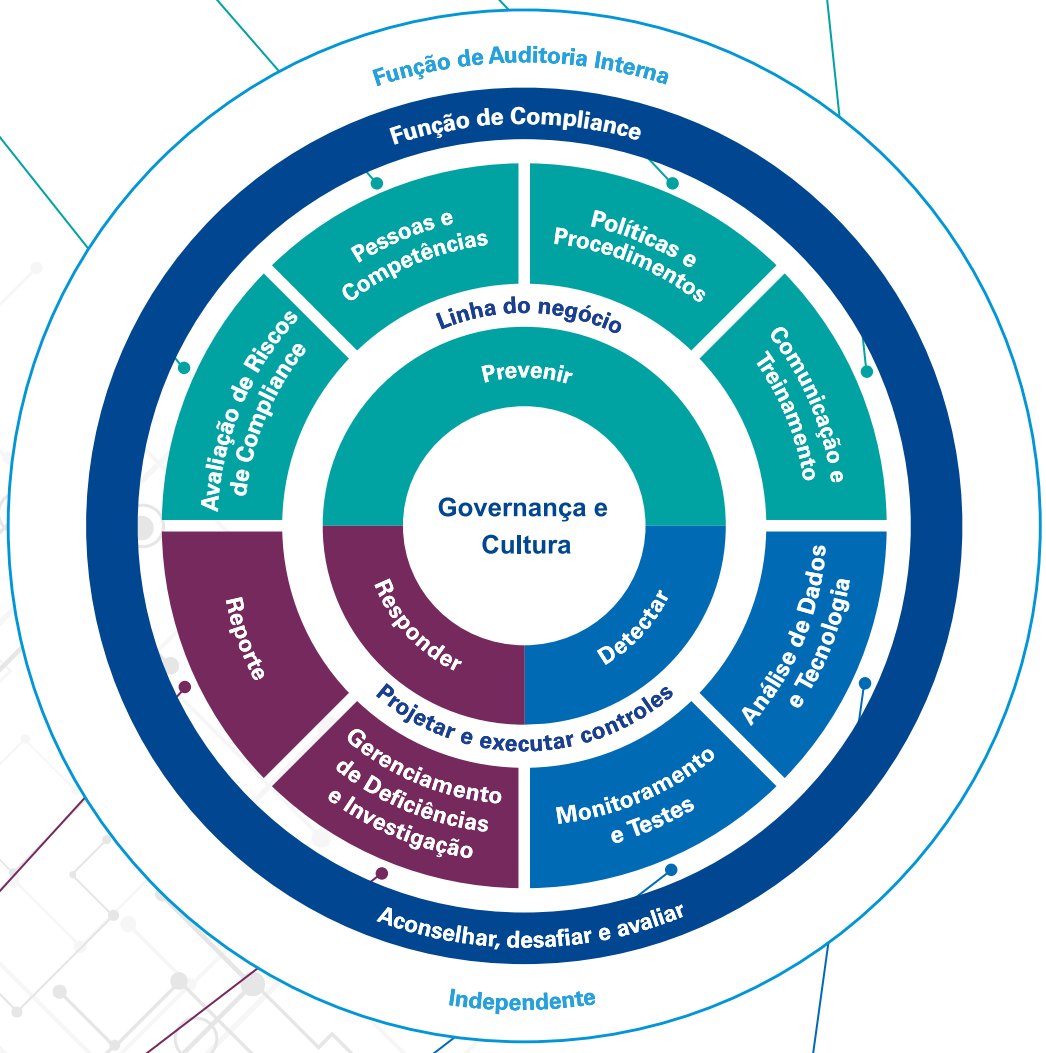
Veja a metodologia a seguir:

- Inventário das regulamentações
- Categorizar riscos inerentes de *compliance*
- Avaliar o risco residual

- Papéis e responsabilidades
- Gestão de desempenho, incentivos e remuneração
- Medidas disciplinares

- Missão, visão e valores
- Políticas e procedimentos corporativos (por exemplo: Código de Conduta)
- Políticas e procedimentos que incorporem os requerimentos de *compliance*
- Gerenciamento de políticas e procedimentos
- Gestão de mudança regulatória

- Comunicações e treinamentos regulares e frequentes
- Treinamento baseado em riscos (incluindo treinamento de novos admitidos, treinamento adaptado às responsabilidades e papéis de trabalho e treinamentos *ad hoc*)
- Reforço da cultura e comprometimento de *compliance*
- Treinamentos atualizados para refletir mudanças regulatórias
- Participação de terceiros em Programas de Treinamento



- Comunicação periódica ao Conselho de Administração e à Diretoria (Por exemplo: reuniões, relatórios, prestação de contas etc.)
- Relatório de riscos regulatórios e de *Compliance*
- Manutenção de dados

- Protocolos de relatos
- Responder a investigações/ inspeções dos governos
- Plano de respostas e processos estabelecido para investigações de não conformidades

- Monitoramento e rastreamento das mudanças regulatórias
- Testes transacionais, processos e controles
- Gestão de *compliance* de terceiros e colaboradores (Por exemplo: *due diligence* e gestão)
- Linha Ética / Canal de Denúncias com abrangência interna e externa (Por exemplo: profissionais, fornecedores, clientes etc.)
- Avaliação periódica do Programa de Compliance

- Tecnologia para suportar o Programa de Compliance (linha direta, investigações, inquéritos regulamentares, testes, registros de treinamento, monitoramento, emissão de relatórios, gestão de mudanças regulatórias etc.)
- Medidas de Prevenção:
  - Indicadores-chave de risco (KRIs) Indicadores-chave de Performance (KPIs)
  - Análise da Causa-raiz & Tendências
- Relatórios consolidados das atividades de *compliance*

A importância da cultura de *compliance* e o "tom" na alta e média Gerência contribuem significativamente no processo de implementação e manutenção de um Programa de Compliance efetivo e eficiente, além de ajudar as empresas a minimizar situações de desvio de conduta e reduzir o impacto dos eventuais problemas de *compliance*. Independentemente da maturidade da estrutura de *compliance* de uma empresa, os CCOs reconhecem que suas empresas precisam melhorar para promover a percepção do valor de *compliance* por meio de uma maior efetividade, eficiência e sustentabilidade. Para cada elemento do programa, as empresas devem determinar a situação desejada usando uma escala de 1 ("sem infraestrutura") a 5 ("alta *performance*").

Conforme as empresas avançam, elas tendem a se concentrar mais na prevenção e detecção e menos na resposta, o que lhes permite passar a ver a área de Compliance como um investimento e obter economias significativas. As empresas mais avançadas também migram para uma maior centralização e integração do programa. Para a maioria das empresas, a jornada rumo à conformidade será uma evolução e alinhamento contínuos entre os requisitos e expectativas regulatórias e o perfil de risco, cultura, objetivos estratégicos e financeiros e modelos de negócios e operacionais da empresa. Para algumas, o tamanho da jornada pode depender dos recursos financeiros ou da percepção da necessidade de evoluir. Para outras, uma transformação ampla pode ser necessária simplesmente para cumprir as exigências regulatórias. Além disso, a jornada rumo à conformidade muitas vezes varia dependendo da empresa, sua história, estrutura legada, experiências anteriores, da indústria, atividades de negócios e objetivos futuros. No entanto, a jornada representa uma oportunidade para todas as empresas integrarem ainda mais os requisitos de *compliance* de uma forma sustentável e identificar novas maneiras de avaliar a efetividade e aumentar a eficiência.

Avaliando a efetividade e eficiência do Programa de Compliance

Os CCOs de todas as indústrias estão focados em avaliar e aumentar a sua efetividade de *compliance* em resposta às exigências e expectativas regulatórias.

Isto inclui assegurar que eles tenham uma cultura robusta de *compliance* incorporada em toda a empresa e que sejam capazes de demonstrar aos seus Conselhos e reguladores que entendem e podem gerenciar seus riscos de *compliance*. Além disso, os CCOs em empresas com programas mais maduros também estão atentos à necessidade de melhorar a efetividade e a eficiência dos seus programas.

Embora muitos CCOs estejam começando a perceber o valor do seu investimento em *compliance* por meio deste foco na efetividade, eles muitas vezes têm dificuldades no que tange à maneira de avaliá-lo. Muitos utilizam métricas internas para obter informações sobre a efetividade de seus programas.

Além disso, os líderes de *compliance* reconhecem os limites das estatísticas unidimensionais, como *feedback* dos clientes e órgãos regulatórios ou multas decrescentes. Embora essas métricas forneçam algumas informações, elas geralmente não aumentam a conscientização de uma empresa sobre a efetividade real de *compliance*.

Como resposta, os CCOs estão cada vez mais buscando métricas multidimensionais que associam o desempenho operacional com *compliance* e métricas que podem fornecer um entendimento mais profundo da efetividade de *compliance* da empresa. As métricas multidimensionais, por exemplo, podem possibilitar que uma empresa entenda melhor as causas dos problemas relacionados com retenção, engajamento e atitude; o tempo necessário para fechar as questões de auditoria e o número de questões repetidas; e a satisfação ou reclamações do cliente no âmbito das unidades de negócios. Estas métricas também fornecem informações sobre a efetividade do Programa de Compliance. Além disso, os líderes estão buscando dados e análises e outras medidas preditivas e utilizando indícios da ciência comportamental para avaliar tendências de *compliance* e melhorar seu entendimento dos riscos emergentes e potencial má conduta.

Exemplos dessas métricas de vanguarda podem incluir uma "taxa de cliques", que mede o número de funcionários que leram uma política específica, ou rastrear más condutas de funcionários como um indicador de condutas futuras potencialmente mais graves.

Além disso, determinadas métricas levantadas de pesquisas com funcionários, avaliações culturais ou grupos focais podem demonstrar como o Programa de Compliance é implementado em uma empresa e destacar a solidez do seu desenho e execução. As avaliações, por exemplo, também podem fornecer *insights* sobre questões culturais em toda a empresa ou descumprimentos que não seriam necessariamente capturados pelas outras métricas. Embora não haja nenhuma definição universalmente aceita do que torna um Programa de Compliance efetivo e não exista uma métrica para avaliar a efetividade, as bases de um Programa de Compliance efetivo são um desejo e execução robustos, respostas oportunas e proativas para as questões de *compliance* e preparação para as mudanças regulatórias.

- **Desenho e execução**
  O desenho e execução são a base de um Programa de Compliance efetivo. Isso é demonstrado quando o programa funciona conforme o planejado e os problemas recorrentes diminuem ao longo do tempo. Para avaliar o desenho e execução, muitos líderes de Compliance analisam os seus principais indicadores de risco (KRI) ano a ano ou em pesquisas com funcionários selecionados. Eles normalmente também consideram a estrutura e as orientações de controles internos do Committee of Sponsoring Organizations (COSO) e comparam o seu programa com as boas práticas internacionais. Os órgãos regulatórios em determinadas indústrias desenvolveram orientações específicas do setor.

- **Resposta oportuna às questões**
  Embora a má conduta, *gaps* e outros problemas ainda possam ocorrer, independentemente da força do Programa de Compliance de uma empresa, a maneira como

ela responde reflete sua efetividade de *compliance*. Uma parte crítica desta resposta é a capacidade de implementar um processo sustentável para autoidentificar e autorreportar más condutas potenciais ou supostas más condutas aos órgãos reguladores antes do escrutínio regulamentar. Além disso, as empresas devem ter processos para receber e solucionar problemas mais amplos, incluindo reclamações dos consumidores.

- **Preparação para mudanças regulatórias**
  A preparação para a mudanças regulatórias requer que as empresas antecipem as mudanças regulatórias e respondam rapidamente a elas para assegurar sua conformidade. Isso inclui revisões da sua infraestrutura e abordagens internas.

Além da efetividade, as empresas com os esforços de *compliance* mais maduros muitas vezes percebem que a próxima etapa na sua jornada de *compliance* — e algo fundamental para obter um retorno sobre o seu investimento — é tornar o Programa de Compliance mais eficiente e sustentável. Um Programa de Compliance efetivo pode abordar muitas exigências regulatórias de uma empresa por meio de um conjunto comum de controles que podem exigir novos controles automatizados em toda a empresa para substituir controles múltiplos ou compensatórios nas unidades de negócios. Isso pode ser especialmente importante para empresas descentralizadas e empresas que atuam em várias jurisdições regulatórias e enfrentam desafios crescentes para monitorar e gerenciar as mudanças regulatórias. Além disso, um Programa de Compliance sustentável exige que os CCOs demonstrem efetividade ao longo do ciclo e submetam este programa a avaliações regulares e frequentes por meio de auditorias independentes ao negócio.

Identificando melhorias de *compliance*

Embora muitas empresas entendam a necessidade de avançar continuamente na sua jornada de *compliance*, há várias ações que os líderes de *compliance* podem tomar imediatamente para uma maior agilidade e gerenciamento de *compliance* proativo, reforçando a efetividade e eficiência do seu Programa de Compliance:

- Analisar a visão "estratégica" de *compliance*.
- Realizar uma avaliação de riscos empresariais.
- Ajudar a assegurar as três linhas de defesa efetivas.
- Avaliar a "Cultura de Compliance" da empresa.
- Avaliar a tecnologia atual.
- Atender mudanças regulatórias.

Percebendo o valor de *compliance*

Enxergar o *compliance* como um investimento, e não simplesmente como um custo, pode ajudar a mensurar o seu retorno durante melhorias de *compliance* contínuas, levando a empresa a uma maior efetividade e eficiência nos seus esforços de *compliance*. As empresas podem fazer isso considerando o valor do negócio e operacional — além do valor de *compliance* — que este investimento oferece.

Por exemplo, embora o investimento em tecnologia, mudanças culturais ou avaliações estratégicas do programa sejam um custo real, ele pode resultar em uma melhoria significativa de processos, melhorias de controle e melhores experiências dos clientes. Embora isso possa ser difícil de quantificar, tem um grande impacto. Para muitas empresas, a jornada de desenvolvimento de *compliance*, daquilo que tem sido para aquilo que precisa ser, pode ser uma grande tarefa. As empresas consideram desafiador enfrentar todos os impactos significativos na estrutura organizacional, processos e tecnologia com os quais as pessoas estão acostumadas a trabalhar. Convencer ou alinhar as pessoas na jornada de *compliance* pode encontrar resistência, uma vez que os funcionários questionam porque as mudanças são necessárias e o valor desses ajustes. Além disso, a migração de dados ou integração de sistemas é um processo complexo com custos significativos. A cultura da própria empresa também pode ser um obstáculo, uma vez que é difícil alinhar unidades de negócios distintas em muitas empresas.

No entanto, o Processo de Compliance é contínuo e requer uma supervisão e melhoria contínuas. Conforme as empresas são pressionadas para se tornarem mais ágeis e econômicas como resposta às condições de mercado, os líderes também devem aumentar a sua agilidade de *compliance*, adaptabilidade, eficiência e sustentabilidade.

Esta jornada deve tornar a área de Compliance parte da equipe de negócio que considera sistemas, produtos e mudanças nos negócios. Persistir nesta jornada pode ajudar as empresas a permanecer à frente das mudanças regulatórias e se adaptar a um ambiente de negócios complexo.

Ao tomar as ações necessárias para aperfeiçoar continuamente o Programa de *Compliance*, os CCOs estarão em uma melhor posição para tornar sua abordagem de *compliance* mais estratégica e obter uma maior efetividade e uma maior eficiência.

Metodologia da Pesquisa

A Pesquisa sobre a Maturidade do Compliance no Brasil foi conduzida por meio de uma **plataforma Web**

e concluída no **2º semestre de 2016**

contemplando **27 perguntas** com foco nos **8 elementos** da Metodologia de *Compliance* da KPMG e considerou os níveis de maturidade das empresas no Programa de Compliance.

Perfil das Empresas e Respondentes

Perfil das empresas

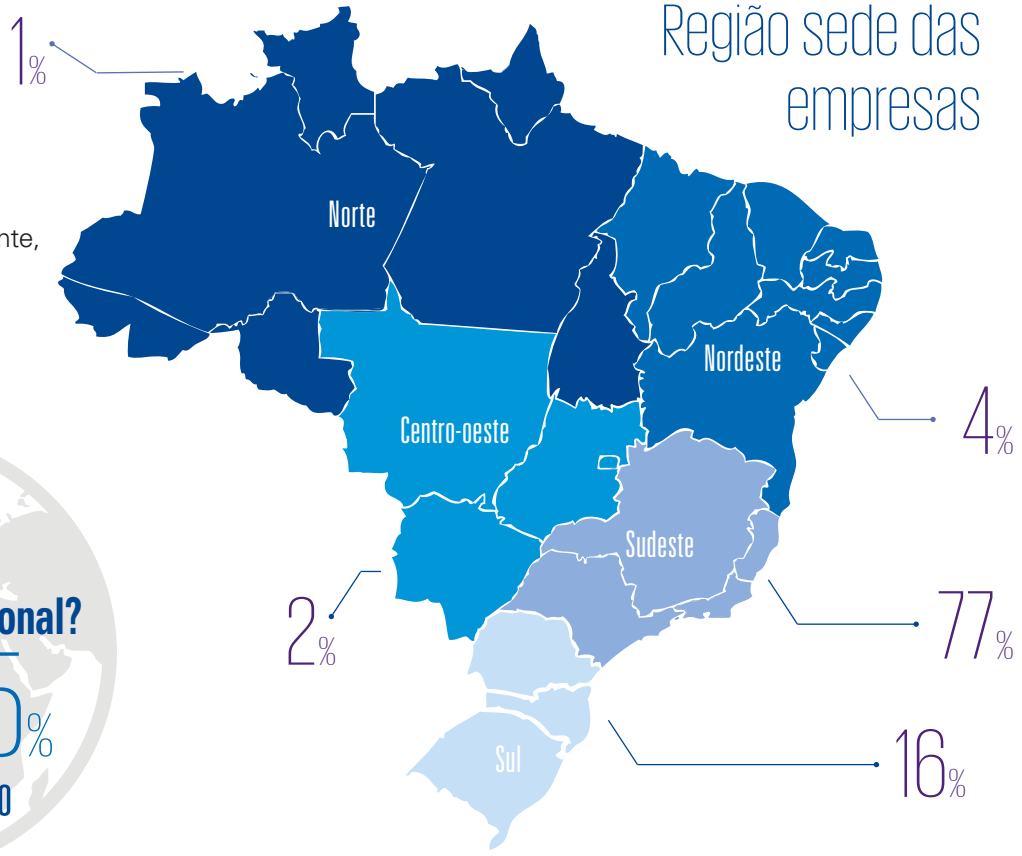
A Pesquisa sobre Maturidade do Compliance no Brasil teve a participação de, aproximadamente, 250 empresas de diferentes regiões e com diferentes estruturas, conforme gráficos apresentados a seguir:

Empresa Multinacional?

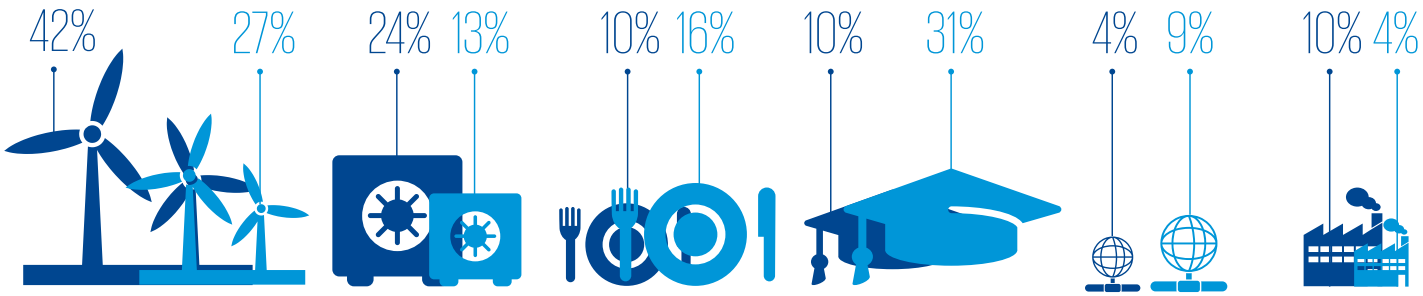
45% sim

55% não

Região sede das empresas



Segmento das empresas



IM
Industrial Markets (Industrial Manufacturing, Life Science & Pharmaceuticals, Energy & Natural Resources)

FS
Financial Services (Banking, Insurance, Real Estate, Investment Management)

CM
Consumer Markets (Food & Drink, Consumer Products, Retail, Agribusiness)

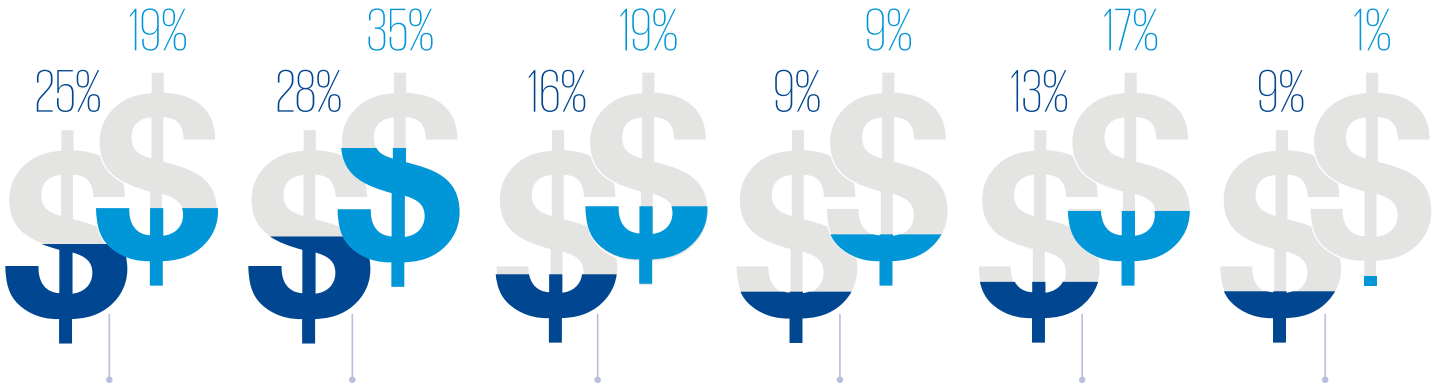
GI
Government & Infrastructure (Healthcare & Education, Government & Infrastructure, Sports)

TMT
Technology, Media & Telecommunications, Communications (Telco) Media, Technology & Software

OTHERS

2015 ***2016***

Receita operacional bruta das empresas



Acima de R$ 5 bilhões

De R$ 1 bilhão a R$ 5 bilhões

De R$ 301 milhões a R$ 1 bilhão

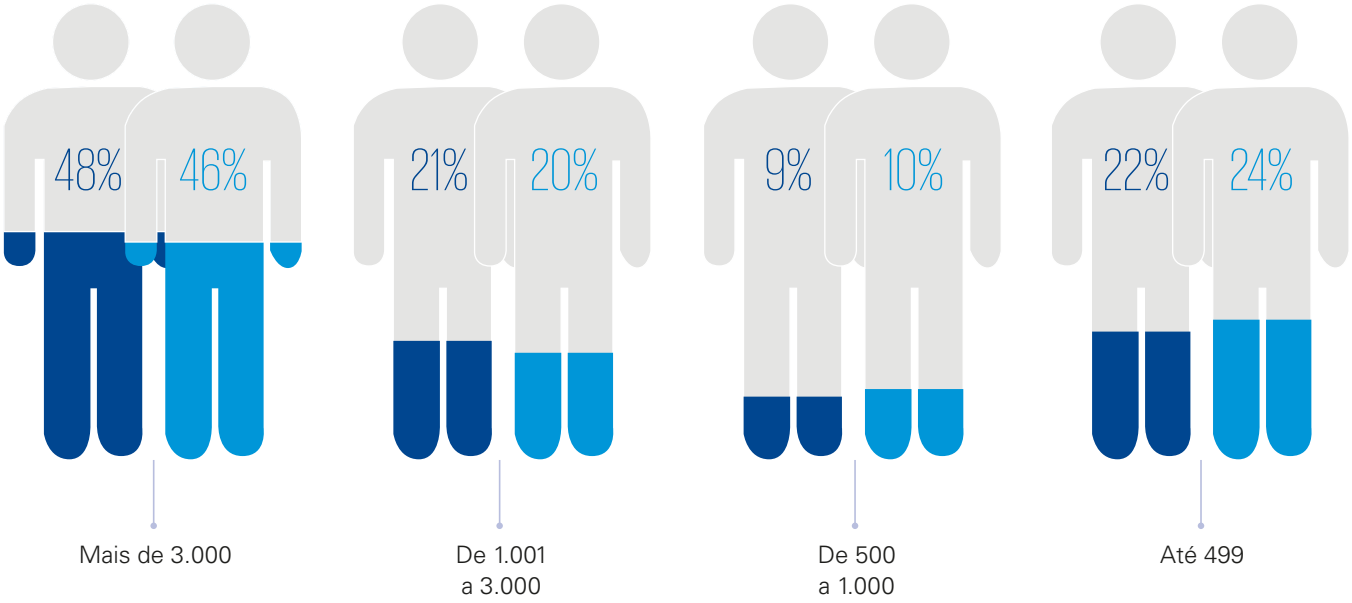
De R$ 91 milhões a R$ 300 milhões

Até R$ 90 milhões

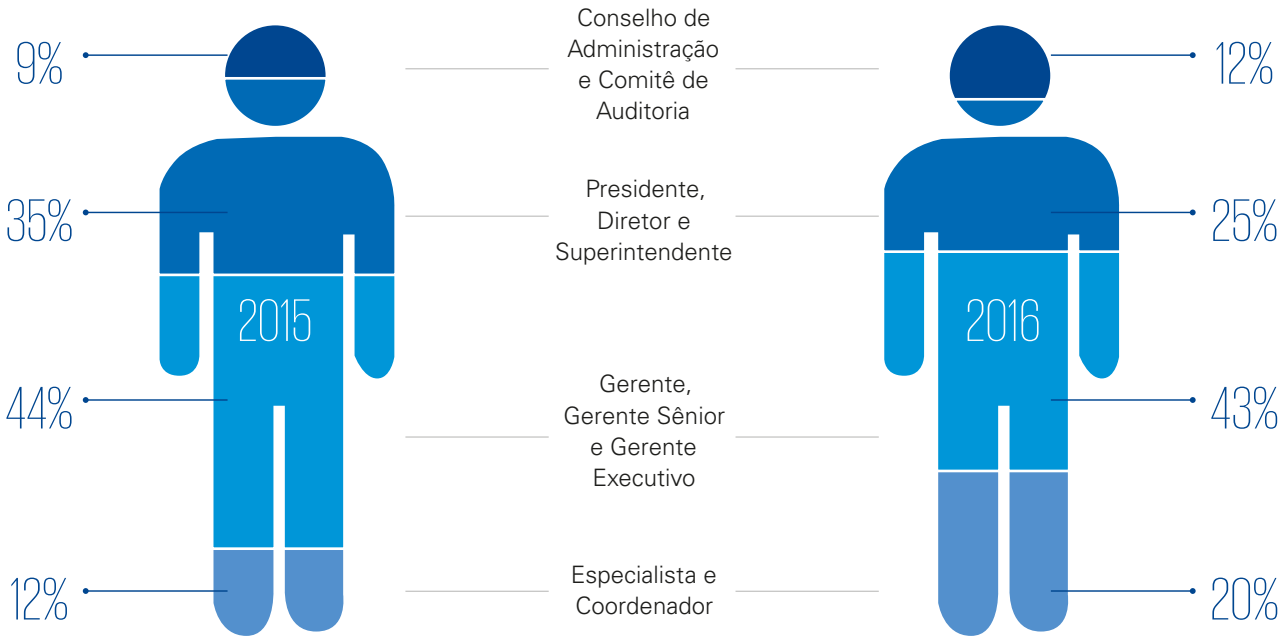
Informação não divulgada

2015 ***2016***

Quantidade de profissionais das empresas



Perfil dos respondentes



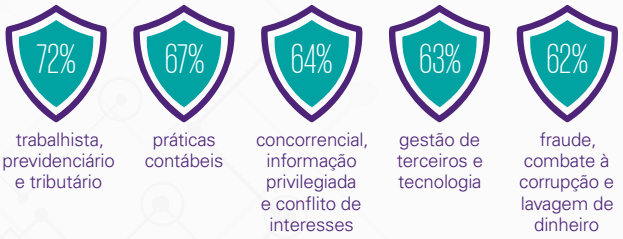
Sumário Executivo

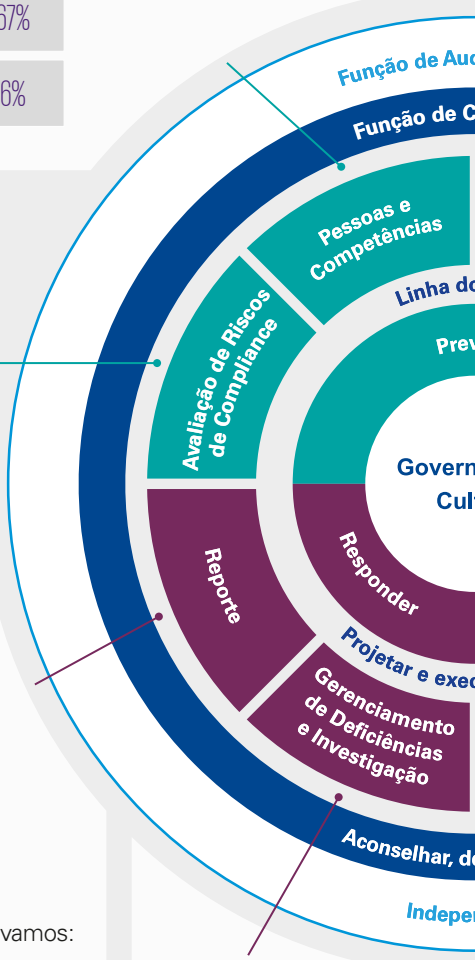
- Estrutura dedicada aos temas de *compliance* com recursos, autonomia e independência para exercer suas funções é considerada uma boa prática de governança. No entanto, as empresas:

- As responsabilidades de *compliance* mais relevantes destacadas pelos respondentes foram:

- Apesar de ser fundamental identificar e monitorar os riscos de *compliance* para estabelecer um programa eficiente de *compliance*, apenas 58% das empresas afirmaram possuir mecanismos de gestão de riscos de *compliance*, enquanto que 42% informaram desconhecê-los.

- Os riscos de *compliance* mais relevantes destacados pelos respondentes foram:





- O reporte aos níveis adequados demonstram a importância do *compliance* e o Tone at the Top, além de permitir a supervisão da estratégia de *compliance*. No entanto, **34%** dos respondentes afirmaram não possuir reporte regular e frequente à Alta Administração.

- Ao questionarmos quanto à frequência do reporte da área de Compliance à Administração, observamos:

- É fundamental atuar para prevenir, detectar e responder aos riscos de *compliance* que possam impactar a imagem e reputação da empresa. Conforme constatado na pesquisa, **37%** afirmaram não possuírem mecanismos de gestão de deficiências e investigação.

- Ao indagarmos sobre a quantidade de registros identificados pela Linha Ética / Canal de Denúncia nos últimos **12 meses**, foram apresentados os seguintes cenários:

- Cenário ainda mais crítico ao constatarmos que **12%** das empresas declararam não possuir o canal de denúncias implementado e **12%** não monitoram o volume de relatos.

- Os padrões de conduta ética e as diretrizes de como a empresa espera que os seus negócios sejam conduzidos, são, geralmente, documentados por meio de políticas e procedimentos e disseminados aos profissionais e partes interessadas (por exemplo, terceiros). Esta pesquisa constatou que:

72% das empresas possuem suas políticas formalizadas

64% envolvem o *compliance* no processo de revisão e aprovação

No entanto, ainda **17%** das empresas informaram não ter atualizado seus respectivos Códigos de Ética e Conduta

24% das empresas, adicionalmente, afirmaram que os Programas de Compliance ainda não estão implementados de forma eficiente

35% das empresas afirmaram não possuir diretrizes sobre as medidas disciplinares aplicadas em casos de desvios

- Investimentos em comunicações e treinamentos contribuem para o fortalecimento da cultura de *compliance*.

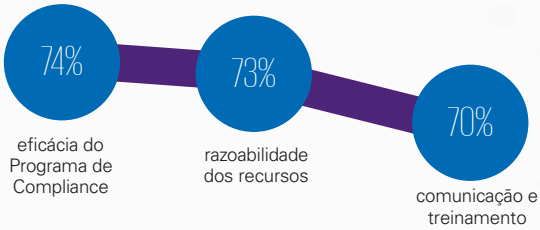
A pesquisa constatou que **43%** das empresas não possuem investimentos razoáveis.

- Os treinamentos e comunicações mais relevantes destacados pelos respondentes foram:

70% conflito de interesses e informação privilegiada, relacionamento com agentes públicos e ética e conduta incluindo terceiros. Foi observada, ainda, a baixa aderência aos treinamentos.

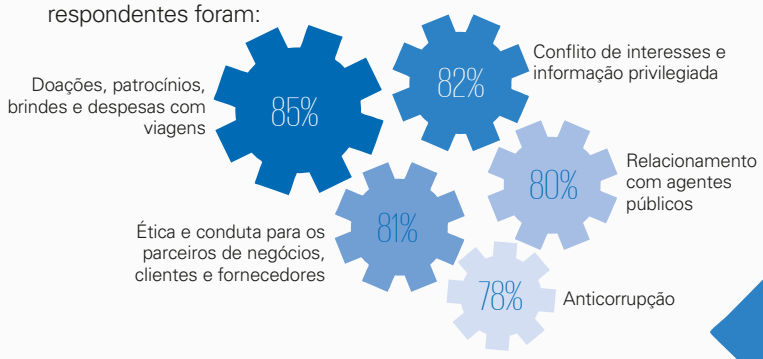
- Para apoiar o negócio perante complexo e dinâmico ambiente regulatório e suportar a implementação de um Programa de Compliance efetivo, é indispensável a utilização de uma plataforma de tecnologia integrada. Observou-se que **42%** das empresas não possuem sistemas para monitorar a efetividade do Programa de Compliance.

- Os indicadores de *compliance* mais relevantes destacados pelos respondentes foram:



- Monitorar a implementação das oportunidades de melhorias identificadas ao longo do processo contribui na melhoria contínua e no aperfeiçoamento do Programa de Compliance. No entanto, apenas **56%** das empresas possuem mecanismos de monitoramento e testes e apenas **64%** monitoram a implementação dos planos de ação identificados.

- As fragilidades de *compliance* mais relevantes destacadas pelos respondentes foram:



Nível de maturidade

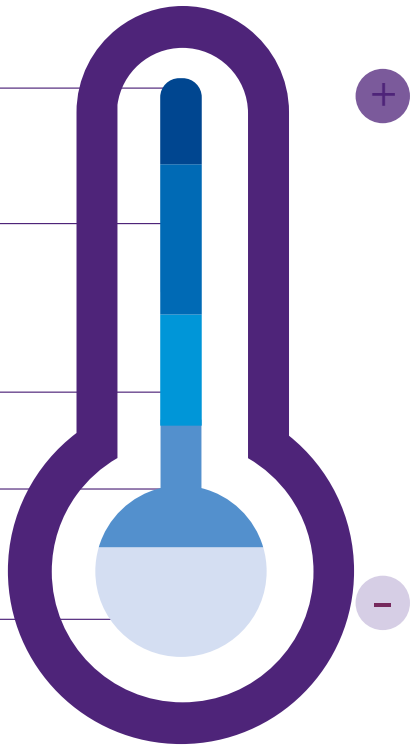
Alta *performance*
Líder reconhecido nas capacidades, nas atividades e na cultura de *compliance*, levando a benefícios tangíveis e estratégicos.

Função de integração
Função de Compliance integrada com Jurídico, Assuntos Regulatórios, Riscos e outros grupos que suportam investigação, consultoria, treinamento e desenvolvimento de uma cultura de *compliance*.

Função de monitoramento
Programa de Ética e Compliance monitorado por um grupo independente.

Infraestrutura mínima
Programa de Ética e Compliance enfatizado no Código de Ética e Conduta proposto por meio das políticas, dos processos e dos procedimentos.

Sem infraestrutura
Programa de Ética e Compliance não está enfatizado, tampouco implementado.



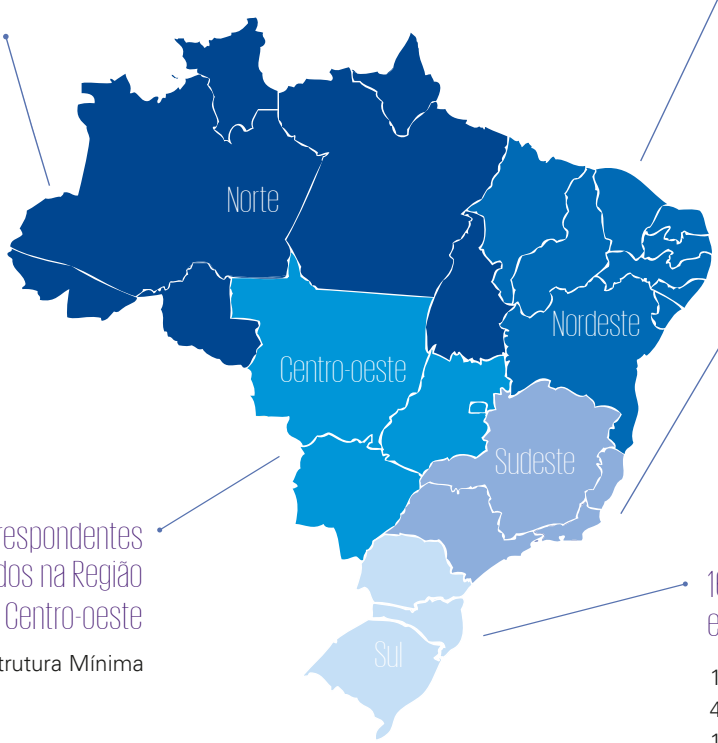
Maturidade do compliance por região

1% do total de respondentes está situado na Região Norte

100% Função de Integração

4% do total de respondentes estão situados na Região Nordeste

20% Infraestrutura Mínima
40% Função de Monitoramento
40% Função de Integração



77% do total de respondentes estão situados na Região Sudeste

8% Sem Infraestrutura
33% Infraestrutura Mínima
18% Função de Monitoramento
27% Função de Integração
14% Alta Performance

2% do total de respondentes estão situados na Região Centro-oeste

100% Infraestrutura Mínima

16% do total de respondentes estão situados na Região Sul

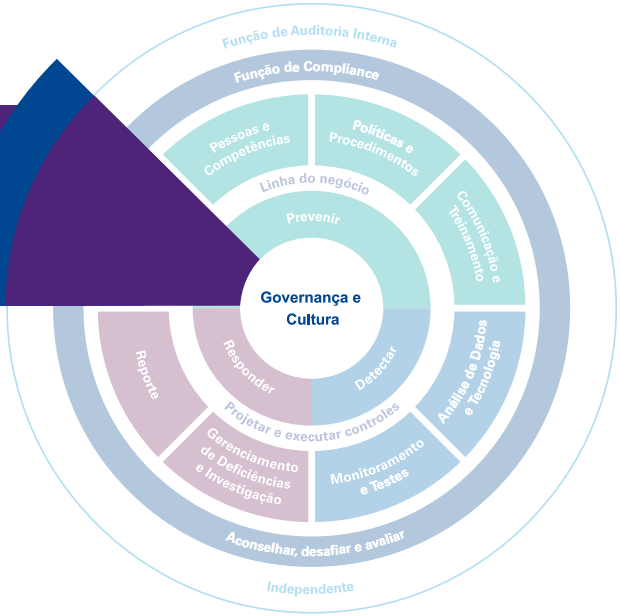
10% Sem Infraestrutura
40% Infraestrutura Mínima
15% Função de Monitoramento
35% Função de Integração

Maturidade do compliance

	2015	2016	2016 por segmento					
			Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Sem Infraestrutura	12%	8%	5%	6%	8%	6%	17%	20%
Infraestrutura Mínima	34%	34%	50%	12%	37%	35%	25%	40%
Função de Monitoramento	19%	18%	15%	17%	20%	18%	17%	20%
Função de Integração	23%	29%	25%	47%	20%	32%	33%	20%
Alta Performance	12%	11%	5%	18%	15%	9%	8%	0%

Resultado Detalhado do perfil de Compliance no Brasil

Governança e Cultura



Questões a considerar

- O Programa de Compliance está estruturado de forma adequada ao tamanho e à complexidade do negócio?
- Qual deve ser o estágio de Maturidade do Compliance para contribuir de forma efetiva ao objetivo estratégico?
- Como assegurar que as alterações promovidas serão sustentáveis?
- O Conselho de Administração e executivos seniores patrocinam a implementação do Programa de Compliance?

Prevenir

- Avaliação de Riscos de Compliance.
- Pessoas e Competências.
- Políticas e Procedimentos.
- Comunicação e Treinamento.

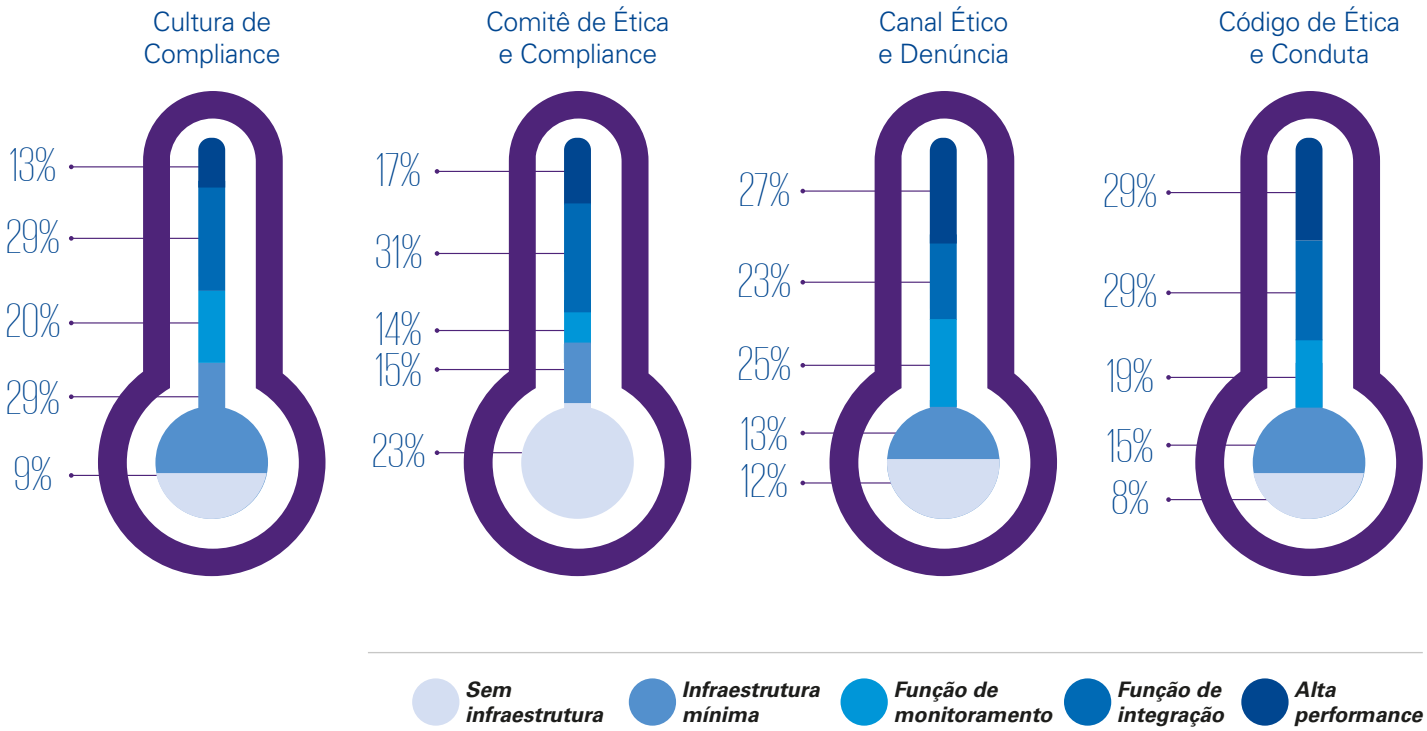
Detectar

- Tecnologia e Análise de Dados.
- Monitoramento e Testes.

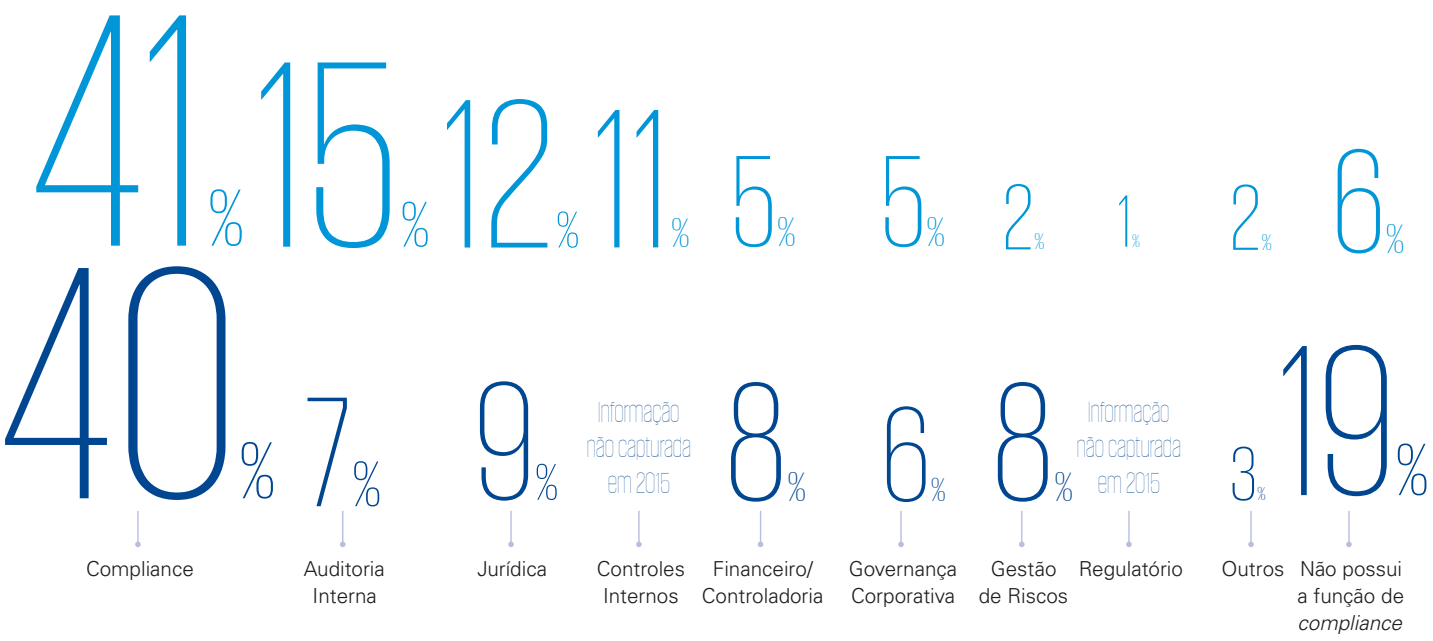
Responder

- Gerenciamento de Deficiências e Investigações.
- Reporte.

Nível de maturidade dos temas abaixo nas empresas

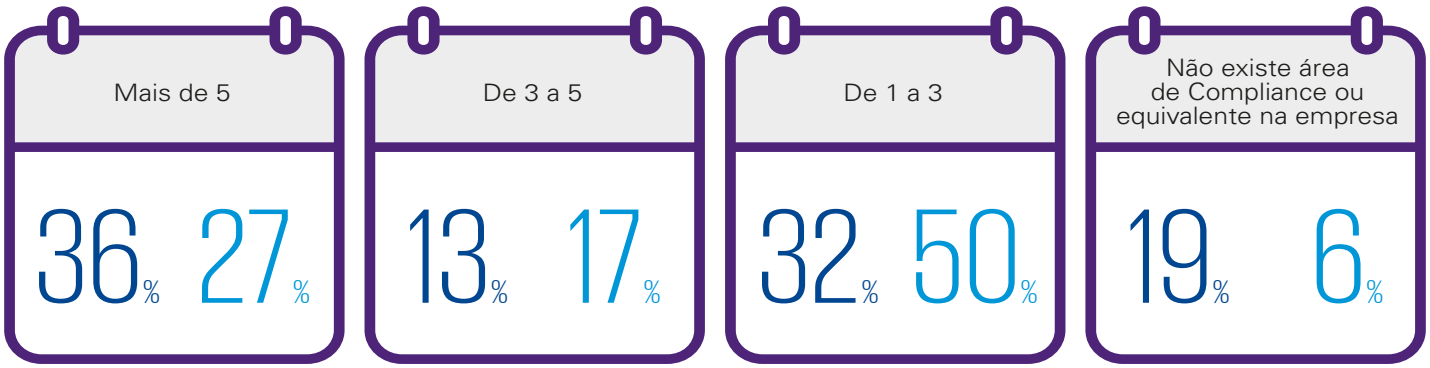


A função de compliance é predominantemente executada pelas seguintes áreas/departamentos:



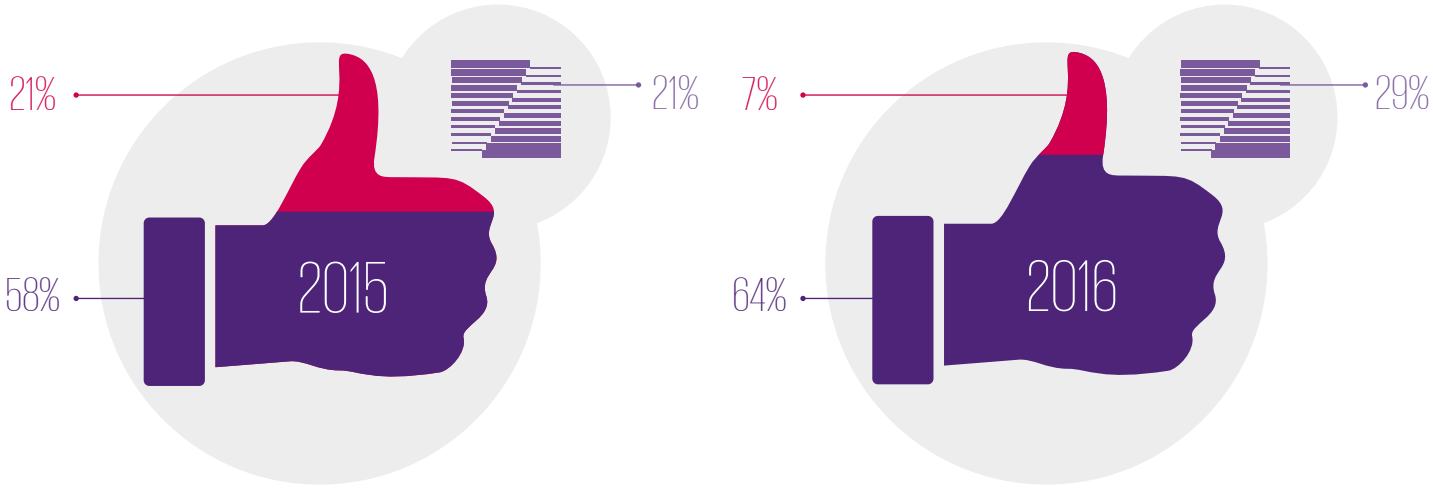
2015 2016

Há quantos anos a área de Compliance ou equivalente existe na empresa?



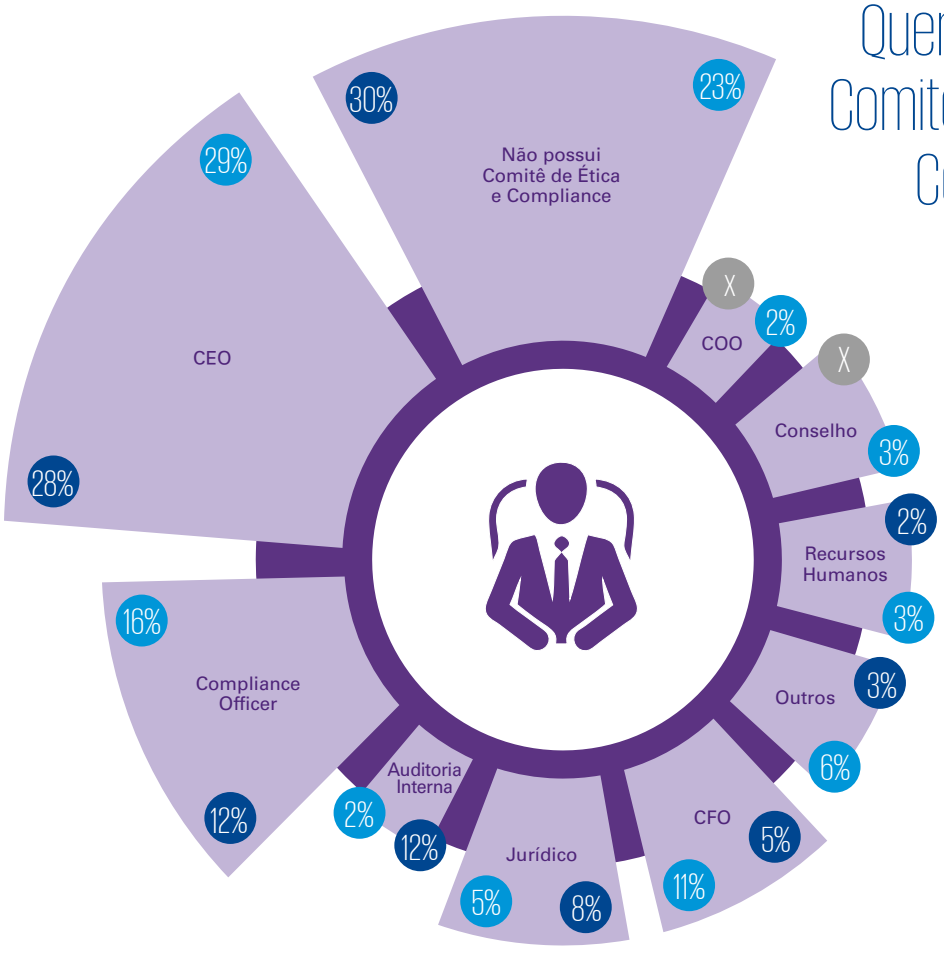
2015 2016

Os executivos seniores reforçam, periodicamente, que a governança e a cultura de *compliance* são essenciais para o sucesso da estratégia da empresa (Tone at the Top and/or middle)?



Não **Sim** ***O conceito de* compliance *não é uniforme na empresa***

Quem preside o Comitê de Ética e Compliance?



2015 **2016** **X** ***informações não foram capturadas em 2015***

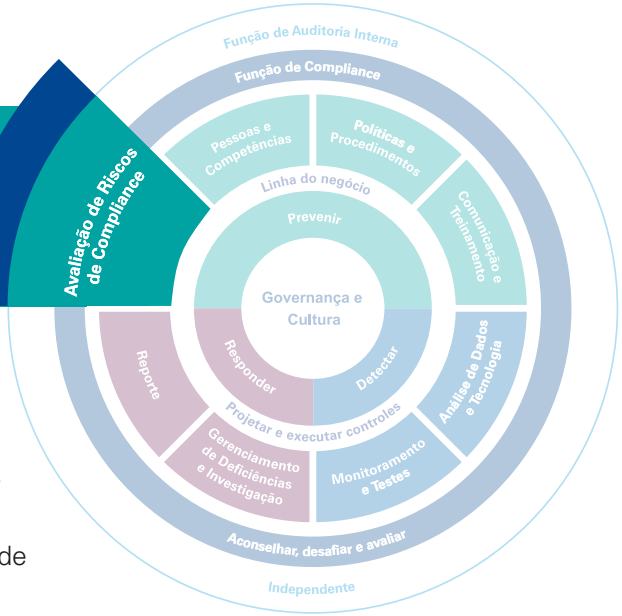
Orçamento anual da área de Compliance

	2015	2016	2016 por segmento: Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Acima de R$ 5 milhões	1%	4%	5%	0%	5%	3%	8%	0%
De R$ 2 milhões a R$ 5 milhões	1%	5%	0%	0%	5%	9%	9%	0%
De R$ 1 milhão a R$ 1,9 milhões	10%	7%	10%	6%	8%	9%	0%	0%
De R$ 501 mil a R$ 999 mil	8%	14%	10%	35%	15%	12%	0%	0%
Até R$ 500 mil	33%	35%	25%	35%	40%	41%	33%	0%
Esta informação não é monitorada	16%	20%	30%	6%	22%	12%	42%	20%
Desconheço esta informação	31%	15%	20%	18%	5%	14%	8%	80%

Principais desafios destacados pela área de Compliance

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Elaborar, aprovar e divulgar políticas e procedimentos	72%	75%	17%	13%	35%	26%	5%	4%
Executar investigações e diligências	53%	73%	17%	15%	32%	27%	6%	3%
Identificar, avaliar e monitorar os aspectos de *compliance* e regulatório aplicáveis ao negócio	76%	70%	18%	14%	28%	31%	7%	2%
Justificar o custo com não conformidades	52%	68%	14%	16%	29%	26%	11%	4%
Divulgar os canais de comunicação (Canal de Denúncia ou Linha Ética)	54%	68%	14%	11%	30%	32%	9%	4%
Capacitar o público interno e externo	78%	68%	15%	14%	26%	29%	11%	5%
Integrar a área de Compliance com as demais áreas de negócios	69%	66%	14%	13%	28%	32%	10%	3%
Desenvolver a matriz de vulnerabilidade dos riscos e indicadores-chave	72%	66%	14%	13%	32%	29%	8%	4%
Obter o patrocínio dos executivos seniores, do Comitê e do Conselho de Administração	62%	60%	16%	14%	29%	28%	10%	3%
Garantir a independência da área de Compliance	61%	61%	14%	15%	31%	28%	7%	5%

Avaliação de Riscos de Compliance



Questões a considerar

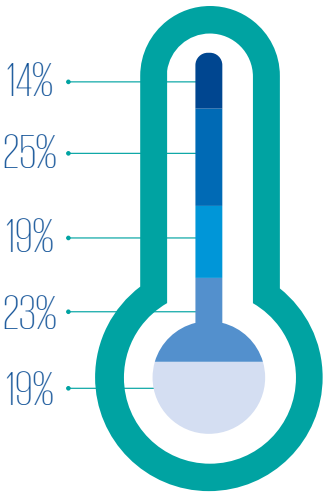
- Existe informação de qualidade de dados e infraestrutura tecnológica para identificar, medir e monitorar os riscos em todos os processos, linhas de negócio e entidades legais?
- Quais ferramentas e metodologias são utilizadas para a avaliação de riscos e qual é o processo para o gerenciamento destes riscos?
- A empresa priorizou os riscos identificados com base na probabilidade potencial e consequência de riscos, incluindo fraude, má conduta e outras exigências regulatórias (isto é, a análise de risco "inerente")?
- A empresa priorizou os riscos identificados com base em uma avaliação da efetividade dos controles para mitigar esses riscos (isto é, análise de "mitigação de controles")?
- A empresa realizou uma avaliação para determinar onde os riscos de *compliance* são relevantes (por exemplo, pelas unidades de negócio, funções de trabalho, geografia)?
- Como a empresa identifica e se mantém atualizada com a nova legislação e requisitos regulatórios?

Prevenção

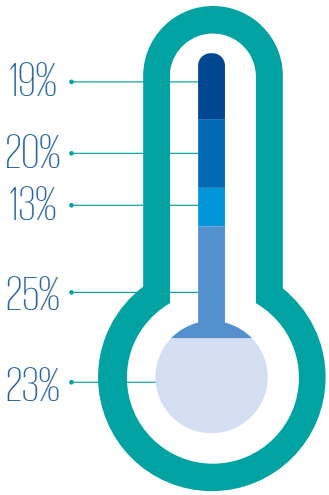
- Inventário de regulamentações.
- Categorizar riscos inerentes de *compliance*.
- Avaliar o risco residual.

Nível de maturidade dos temas abaixo nas empresas

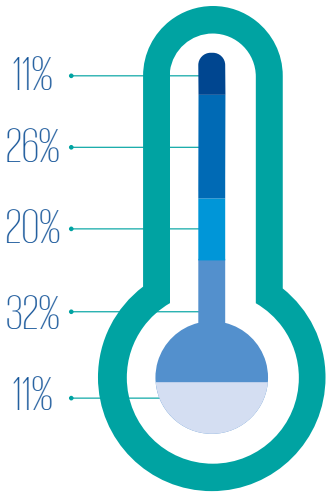
Matriz de Riscos de Compliance



Envolvimento do Compliance em Decisões Estratégicas



Entendimento dos Riscos de Compliance pelas Áreas

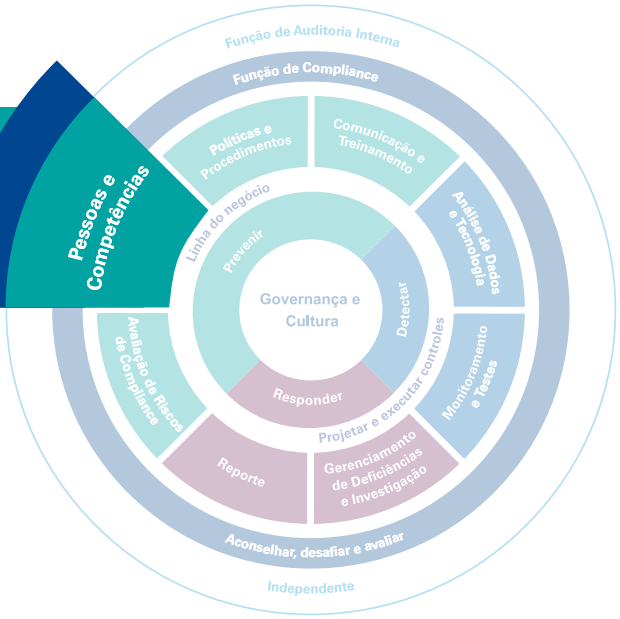


Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

Principais riscos de *compliance*

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Trabalhistas, segurança do trabalho, previdenciários e tributário	73%	72%	17%	9%	31%	29%	10%	4%
Práticas contábeis (nacionais e internacionais)	63%	67%	17%	10%	26%	33%	8%	6%
Concorrencial, informação privilegiada e conflito de interesses	65%	64%	16%	14%	33%	27%	5%	5%
Gestão de terceiros/Contratos	66%	63%	13%	15%	30%	30%	7%	5%
Tecnologia	65%	63%	11%	16%	28%	31%	10%	4%
Fraude, combate à corrupção e lavagem de dinheiro	68%	62%	15%	12%	32%	30%	7%	4%
Sustentabilidade (meio ambiente)	48%	59%	11%	16%	36%	26%	8%	3%
Políticas, processos e procedimentos (incluindo o Código de Ética e Conduta)	66%	56%	15%	15%	34%	23%	9%	4%
Regulatório	69%	55%	12%	17%	30%	26%	9%	6%
Propriedade intelectual	37%	53%	15%	16%	31%	28%	7%	3%

Pessoas e Competências



Questões a considerar

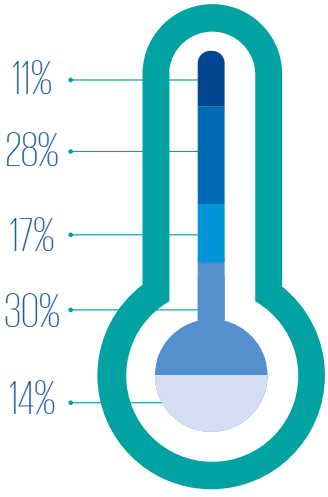
- Existem normas claras que orientam os profissionais quanto às suas responsabilidades?
- A estrutura de remuneração está alinhada com a sua governança e cultura de *compliance*?
- A estrutura organizacional mantém a independência entre suas três linhas de defesa?
- Como são estabelecidos e reforçados os papéis de *compliance*? Como é delegada a responsabilidade pelo *compliance* e seus riscos?
- A empresa possui os profissionais capacitados nas três linhas de defesa e para atender aos requisitos de *compliance*?
- Como são utilizadas as métricas operacionais de *compliance* para ajudar na efetividade do *compliance*?
- Como melhorar o conjunto de habilidades e conhecimentos de sua equipe de *compliance*?

Prevenção

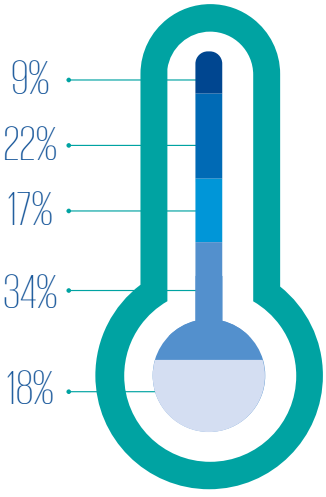
- Papéis e responsabilidades.
- Gestão de desempenho, incentivos e remuneração.
- Medidas disciplinares.

Nível de maturidade dos temas abaixo nas empresas

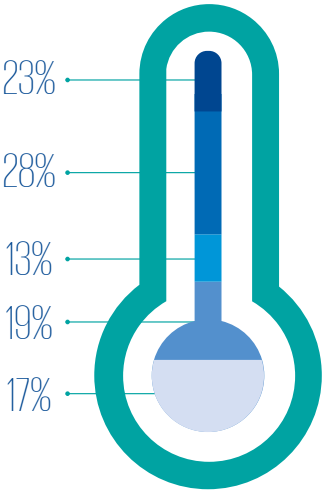
Estrutura da área de Compliance



Recursos alocados para funções de compliance



Autoridade, independência e responsabilidade de compliance

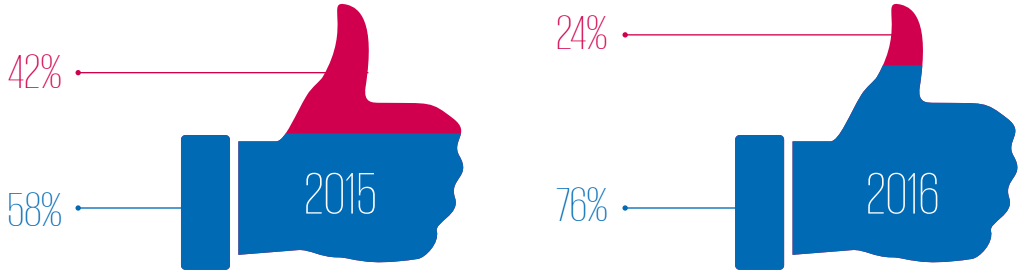


Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

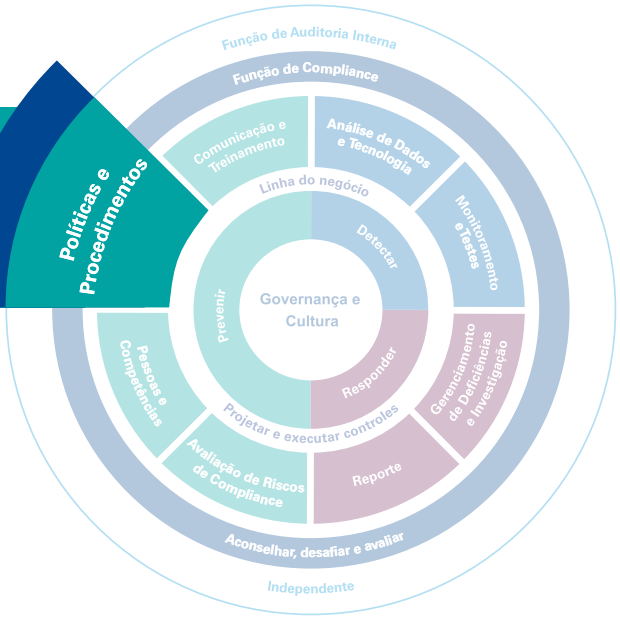
Principais responsabilidades da área de Compliance

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Realizar a manutenção e a capacitação de valor e cultura de *compliance* por meio de treinamentos internos e externos	78%	72%	16%	12%	27%	32%	9%	4%
Operacionalizar para a construção, a elaboração, a aprovação e a divulgação de políticas e procedimentos	76%	62%	15%	13%	28%	32%	9%	3%
Manter uma linha de reporte eficaz para a Alta Administração	71%	63%	17%	14%	28%	28%	7%	6%
Monitorar os indicadores-chave de *compliance*	70%	67%	15%	19%	24%	30%	7%	5%
Monitorar, testar e reportar a Política, o Programa de Ética e os riscos Regulatórios e de Compliance	69%	56%	19%	15%	24%	31%	7%	4%
Gerenciar Compliance Help Desk/ Canal de Denúncias	63%	57%	14%	16%	32%	29%	7%	2%
Executar investigações e diligências de parceiros de negócio	61%	65%	14%	14%	27%	28%	11%	6%
Atuar em processos de aprovação de novos produtos, serviços e mercados	50%	66%	13%	17%	35%	24%	6%	5%
Realizar a comunicação com os agentes reguladores	49%	59%	11%	16%	29%	29%	9%	6%
Revisar as contingências, as multas e os passivos gerados por não conformidades	49%	54%	16%	17%	32%	25%	6%	4%

Incentivos e ações disciplinares são aplicados para promover e reforçar o comprometimento e as responsabilidades dos profissionais?



Políticas e Procedimentos



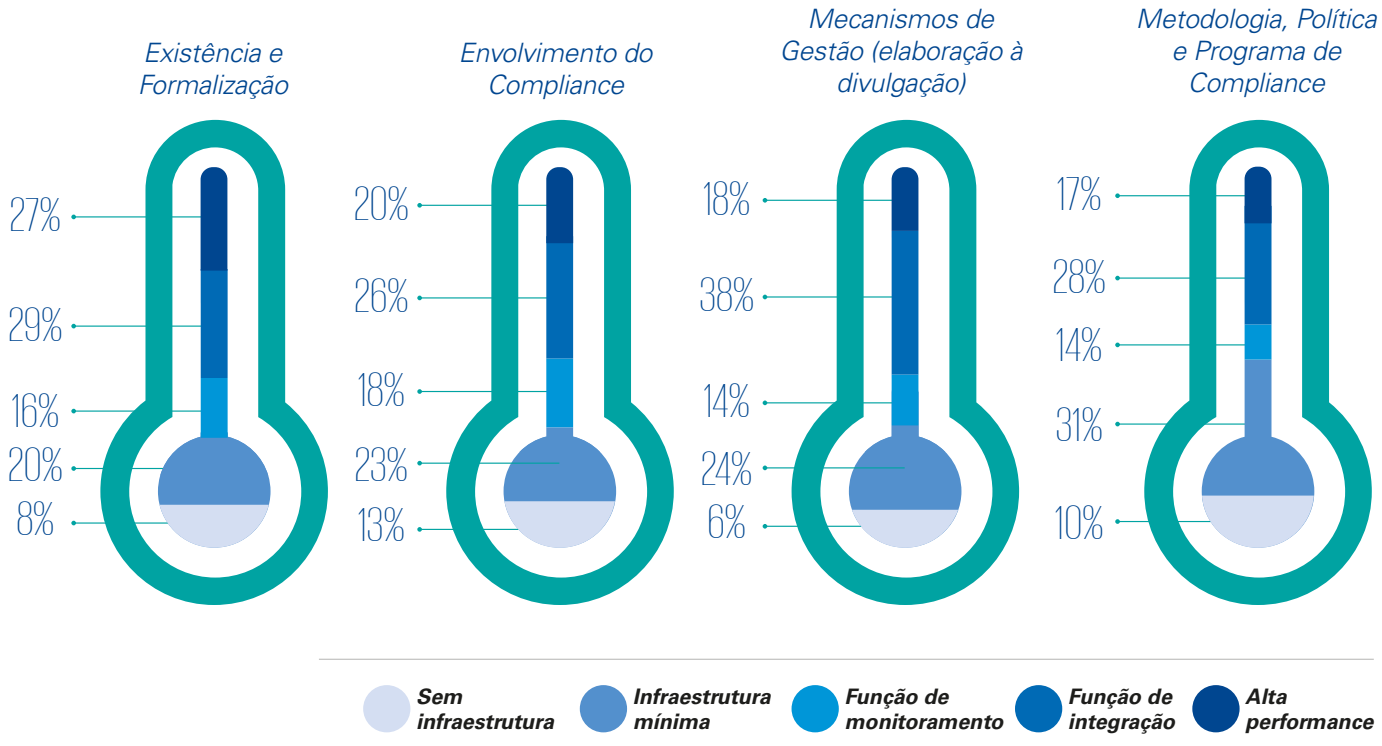
Questões a considerar

- Como o seu Código de Conduta repercute em seus profissionais e partes interessadas (como assegurar que o código é efetivo)?
- Como são administradas a manutenção e a atualização de políticas e procedimentos?
- Já foram inventariadas as obrigações de *compliance*? Caso tenham sido inventariadas, foram feitas de forma centralizada? Como são mapeadas as obrigações para as políticas e os procedimentos existentes?
- Os requisitos aplicáveis de *compliance* são incorporados em políticas e procedimentos específicos ou são incorporados às políticas e aos procedimentos operacionais?
- Quão consistentes são os seus procedimentos de *compliance* em toda a empresa?

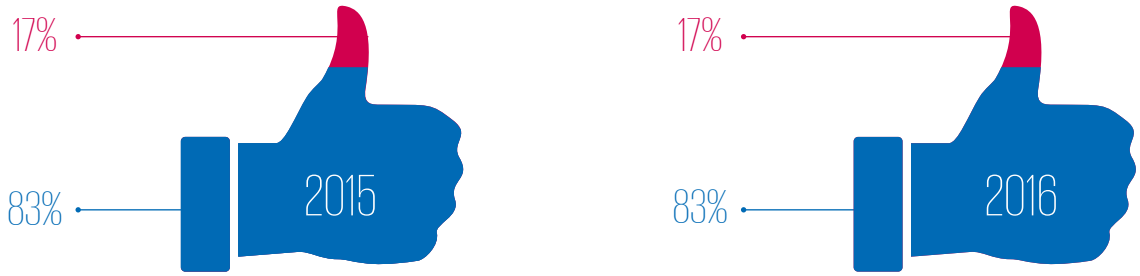
Prevenção

- Missão, Visão e Valores.
- Políticas e procedimentos corporativos (Por exemplo: Código de Conduta).
- Políticas e procedimentos que incorporem os requerimentos de *compliance*.
- Gerenciamento de políticas e procedimentos.
- Gestão de mudanças regulatórias.

Nível de maturidade dos temas abaixo nas empresas

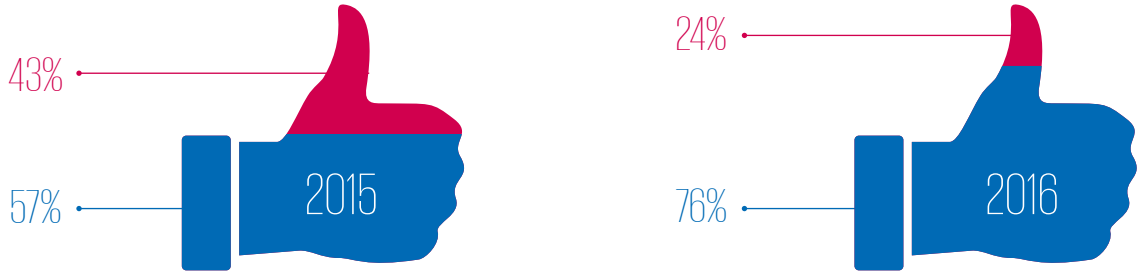


O Código de Ética e Conduta da empresa faz referência aos aspectos regulatórios e de compliance, por exemplo: Lei Anticorrupção, lavagem de dinheiro, conflitos de interesse etc.?



Sim ***Não***

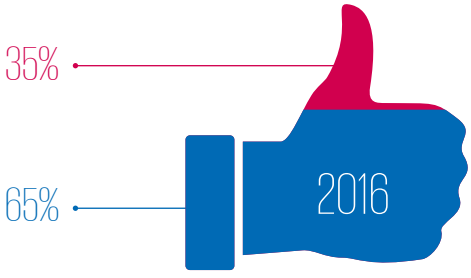
A Política e o Programa de Ética e Compliance estão implementados de forma eficiente na empresa com o objetivo de identificar condutas inadequadas, assegurando a prevenção e investigação?



sim ***A empresa não possui Política e Programa de Ética e Compliance***

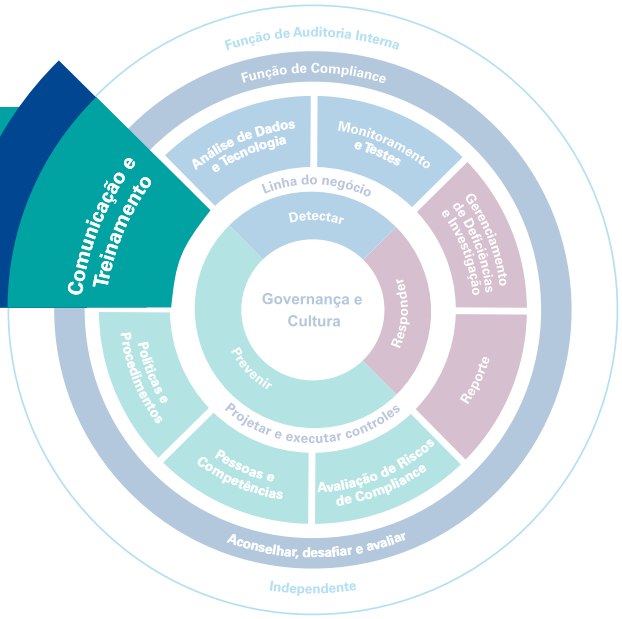
Incentivos e ações disciplinares estão formalizados em políticas e procedimentos e disponíveis para consulta?

Informação não capturada em 2015



Sim ***Não***

Comunicação e Treinamento



Questões a considerar

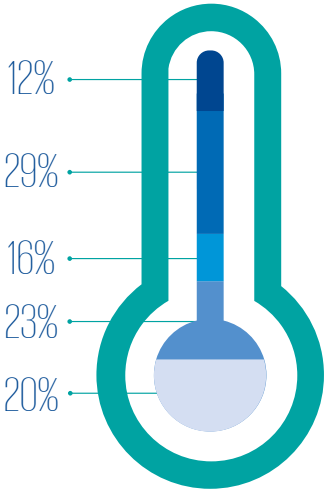
- Quão satisfatórios são os Programas de Treinamento e de Comunicação de Compliance?
- Quais mudanças foram feitas no Programa de Treinamento nos últimos anos? Quais foram os direcionadores?
- A empresa possui um plano formalizado de comunicação? Como o plano foi desenvolvido e implementado? É baseado em riscos? Quando foi a última vez que o plano foi revisto?
- Como a empresa comunica os padrões de ética e *compliance* aos profissionais? Os treinamentos abordam os canais de comunicação, procurando aconselhar e orientar sobre o papel dos profissionais na gestão dos riscos de *compliance*?
- A empresa utiliza métodos mistos de aprendizagem e de comunicação (Por exemplo: presenciais, Web Based, *newsletter*, vídeo e pôster)?
- Como é utilizada a comunicação interna para construir a cultura de *compliance*? Quão efetiva é a abordagem?
- Qual é o papel dos executivos e da Alta Administração ao se comunicar e reforçar padrões organizacionais?
- Quais métricas são consideradas para avaliar o impacto e a efetividade do seu Programa de Treinamento e Comunicação de Compliance?

Prevenção

- Comunicações e treinamentos regulares e frequentes.
- Treinamento baseado em riscos (incluindo treinamento de novos admitidos, treinamento adaptado às responsabilidades e papéis de trabalho e treinamentos *ad hoc*).
- Reforço da cultura e comprometimento de *compliance*.
- Treinamentos atualizados para refletir mudanças regulatórias.
- Participação de terceiros em Programas de Treinamento.

Nível de maturidade do tema abaixo nas empresas

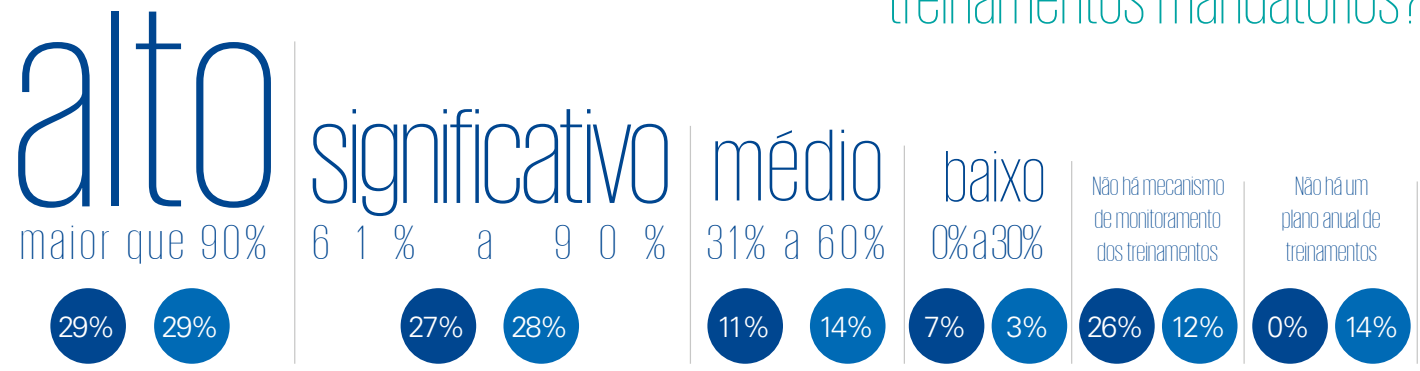
Treinamentos de Temas de Compliance



Principais treinamentos aplicados pela empresa

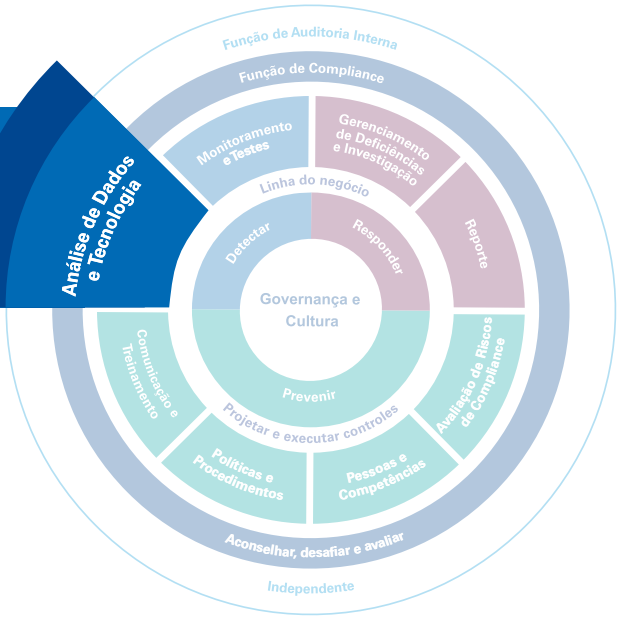
	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Conflito de interesses e informação privilegiada	74%	70%	17%	12%	28%	29%	10%	4%
Relacionamento com agentes públicos	68%	70%	18%	12%	30%	26%	9%	5%
Ética e Conduta para os parceiros de negócios, clientes e fornecedores	75%	70%	18%	16%	25%	27%	10%	4%
Doações, patrocínios, brindes e despesas com viagens	79%	67%	16%	15%	27%	27%	12%	3%
Ética e Conduta para os profissionais	74%	59%	20%	13%	24%	28%	12%	3%
Compliance	61%	59%	19%	12%	28%	27%	9%	5%
Anticorrupção	72%	59%	16%	12%	28%	31%	9%	4%
Facilitação de pagamentos	59%	57%	16%	15%	32%	22%	12%	3%
Antiterrorismo	39%	56%	10%	15%	35%	24%	11%	5%
Lavagem de dinheiro	50%	55%	11%	10%	35%	30%	11%	3%

Qual é o grau de conformidade dos profissionais em relação aos treinamentos mandatórios?



2015 2016

Análise de Dados e Tecnologia



Questões a considerar

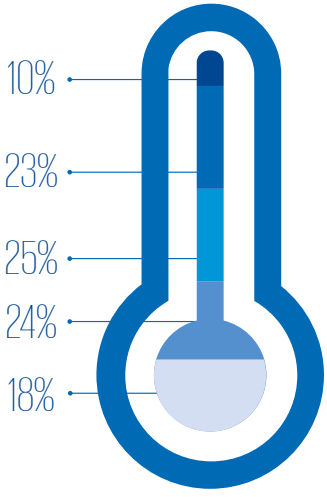
- A atual infraestrutura de tecnologia suporta o seu Programa de Compliance e permite a você identificar, medir e monitorar os riscos através das linhas de negócios em tempo real?
- Você possui ambas as qualidades dos dados (integridade e precisão) necessárias para apoiar o Programa de Compliance?
- Há a extração de dados, testes e análise frequentes?
- Você tem validado sua infraestrutura de *compliance*?
- As alçadas e métricas em relação a *compliance* estão bem definidas e baseadas em riscos? Há análise preventiva para identificar os riscos emergentes?
- A sua tecnologia, quanto à identificação de possíveis problemas ("alertas"), permite uma análise da causa-raiz e tempo de resposta mais eficiente?
- O trabalho digital ajudaria a maximizar suas habilidades analíticas?

Detecção

- Tecnologia para suportar o Programa de Compliance (linha direta, investigações, inquéritos regulamentares, testes, registros de treinamento, monitoramento, emissão de relatórios, gestão de mudanças regulatórias etc.).
- Medidas de Prevenção:
  - Indicadores-chave de risco (KRIs). Indicadores-chave de Performance (KPIs).
  - Análise da Causa-raiz & Tendências.
- Relatórios consolidados das atividades de *compliance*.

Nível de maturidade do tema abaixo nas empresas

Análise de Dados e Tecnologia

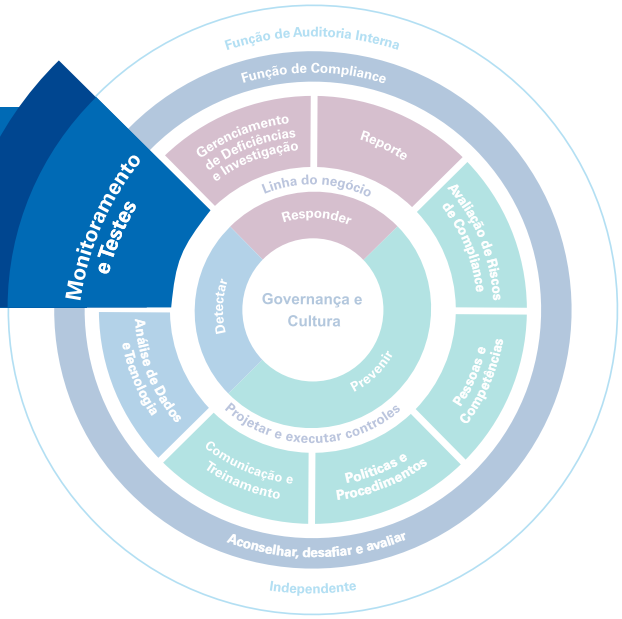


Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

Principais indicadores de monitoramento reportados aos executivos seniores

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Eficácia do Programa de Compliance	80%	74%	12%	16%	31%	27%	9%	5%
Análise dos recursos disponíveis *versus* necessidade do Programa de Compliance	65%	73%	15%	15%	33%	21%	11%	5%
Atualizações no processo de comunicação de assuntos Éticos e Compliance	78%	71%	15%	14%	27%	27%	11%	6%
Percentual de aderência aos treinamentos mandatórios	68%	70%	13%	11%	29%	33%	9%	5%
Alocação de recursos (*budget* x real) e análise comparativa com a Indústria	68%	70%	15%	16%	31%	25%	9%	4%
Overview do Plano de Ética e Compliance proposto para o próximo período	63%	66%	17%	14%	31%	25%	7%	6%
Resultado e evolução das investigações (Procedentes e Não Procedentes)	72%	66%	17%	13%	26%	29%	11%	4%
Relação de Riscos, Controles e Planos de Ação mitigatórios	71%	63%	14%	14%	26%	30%	11%	5%
Não possui indicadores-chave reportados à Administração	51%	60%	13%	13%	35%	26%	8%	5%
Atualização dos eventos regulatórios que podem afetar as operações do negócio	70%	59%	12%	12%	31%	27%	12%	6%

Monitoramento e Testes



Questões a considerar

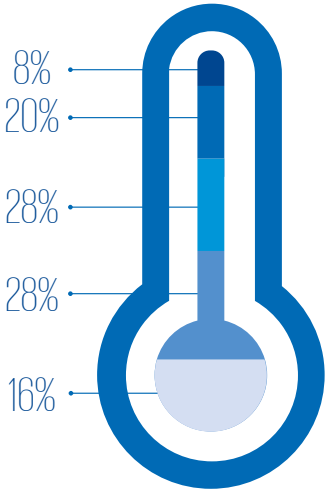
- Há tecnologia e infraestrutura para monitorar os riscos em todos os processos e entidades legais?
- Qual é o papel e a responsabilidade de cada linha de defesa para testes e monitoramento? A abordagem é centralizada ou descentralizada? Todos os *gaps* chegam a conhecimento na cobertura dos testes, nas três linhas de defesa?
- Como são priorizados os riscos para testes de *compliance* e monitoramento? Como estão os esforços ligados à avaliação de riscos de *compliance*?
- Como é avaliada a efetividade dos esforços de monitoramento e teste?
- O que está sendo relatado ao Conselho e outras partes interessadas sobre o seu monitoramento, testes e resultados?
- Como são endereçados os resultados negativos? É realizada uma análise de causa-raiz? Os testes são repetidos para verificar a correção ou melhoria dos resultados negativos?
- Como as relações de terceiros são monitoradas, considerando riscos de *compliance* e regulatórios?

Detecção

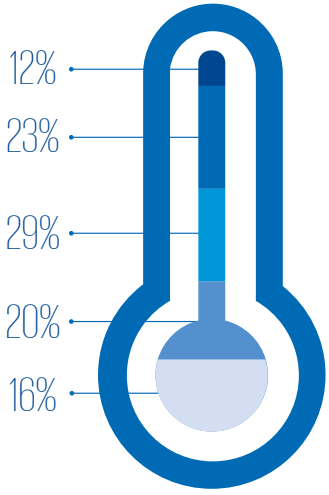
- Monitoramento e rastreamento das mudanças regulatórias.
- Testes transacionais, processos e controles.
- Gestão de *compliance* de terceiros e colaboradores (Por exemplo: *due diligence* e gestão).
- Linha Ética / Canal de Denúncias com abrangência interna e externa (Por exemplo: profissionais, fornecedores, clientes etc.).
- Avaliação periódica do Programa de Compliance.

Nível de maturidade dos temas abaixo nas empresas

Monitoramento e testes de aderência, incluindo gestão de mudanças regulatórias



Monitoramento dos planos de ação e principais fragilidades

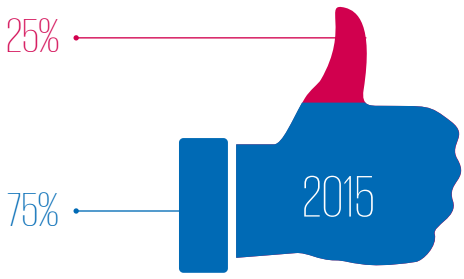


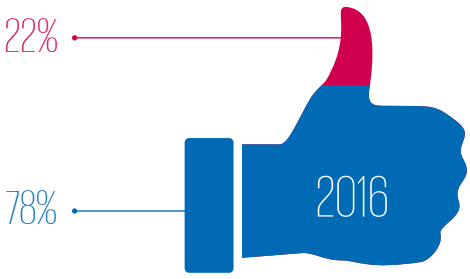
Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

Principais registros na Linha Ética/Canal de Denúncia

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Doações, patrocínios, brindes e despesas com viagens	94%	85%	16%	15%	31%	27%	7%	4%
Conflito de interesses e informação privilegiada	81%	82%	15%	13%	34%	26%	8%	4%
Ética e Conduta para os parceiros de negócios, clientes e fornecedores	83%	81%	17%	14%	30%	27%	7%	5%
Relacionamento com agentes públicos	71%	80%	17%	13%	32%	28%	6%	4%
Anticorrupção	69%	78%	11%	16%	31%	28%	9%	5%
Facilitação de pagamentos	76%	77%	14%	12%	34%	27%	9%	4%
Compliance	83%	76%	16%	13%	34%	24%	7%	6%
Ética e Conduta aos profissionais	79%	69%	14%	15%	30%	28%	9%	4%
Lavagem de dinheiro	54%	64%	13%	16%	34%	23%	9%	5%
Antiterrorismo	42%	60%	12%	16%	35%	22%	5%	10%

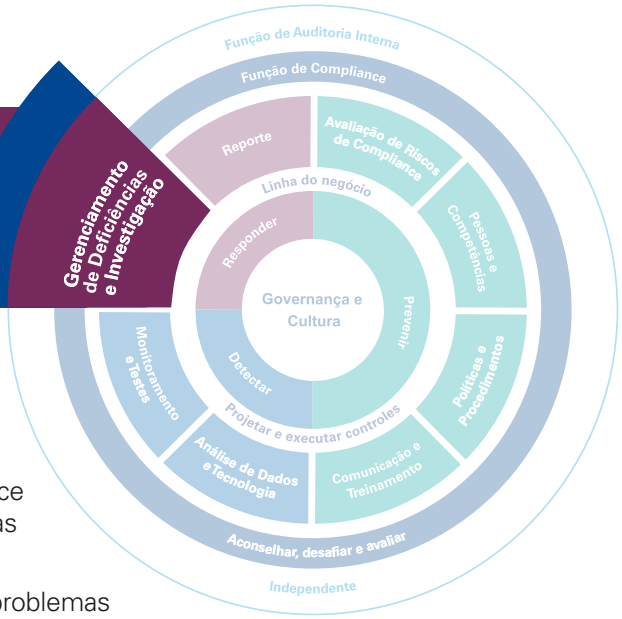
O C-Level ("Chiefs" - CEO, CFO, COO etc.), o Conselho de Administração e/ou o Comitê de Auditoria estão informados apropriadamente sobre o conteúdo e a operacionalização da Política e do Programa de Ética e Compliance?





Sim Não

Gerenciamento de Deficiências e Investigação



Questões a considerar

- O atual reporte do "Estágio de Compliance" é robusto com temas-chave de *compliance*, Avaliação de Programa de Compliance e métricas de riscos emergentes que incluem padrões, tendências e riscos de terceiros?
- Como são inventariados, priorizados, remediados e relatados os problemas de *compliance*? Existem normas de gestão claras para as investigações, exames e inspeções?

Investigações

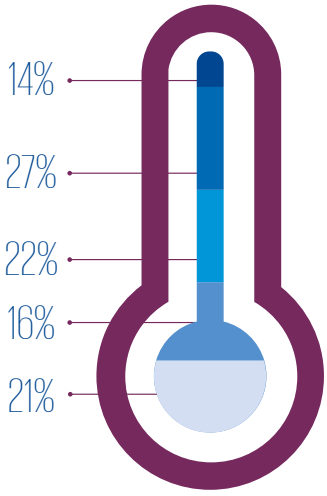
- Como é determinada a composição da sua equipe de investigação e como é atribuída a responsabilidade por investigações dentro de sua empresa?
- Quando são escaladas investigações para o seu Conselho de Administração e Comitê de Auditoria?
- Foram desenvolvidos fluxos de decisão que orientam o processo de investigação? Existem métricas regulares de relatórios vigentes de fácil compreensão, incluindo para o Conselho de Administração, para avaliar a efetividade da investigação? As métricas de investigação são utilizadas para informar e priorizar melhorias no Programa de Compliance?

Responder

- Protocolos de relatos.
- Responder a investigações/ inspeções dos governos.
- Plano de respostas e processos estabelecidos para investigações de não conformidades.

Nível de maturidade do tema abaixo nas empresas

Investigação e Due Diligence

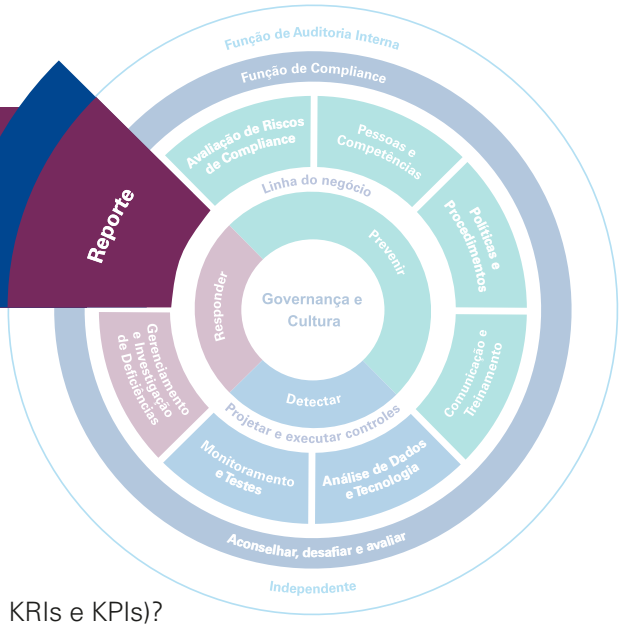


Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

Quantidade de registros identificados pela Linha Ética / Canal de Denúncia nos últimos 12 meses

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Menor que 20	30%	31%	20%	59%	28%	32%	33%	0%
De 20 a 50	8%	12%	5%	12%	10%	18%	17%	0%
De 51 a 100	5%	11%	10%	0%	15%	15%	8%	0%
Mais de 100	10%	22%	30%	12%	28%	21%	0%	40%
Não existe Compliance Help Desk / Canal de Denúncias implementado	18%	12%	20%	12%	10%	0%	33%	20%
Não tenho conhecimento	29%	12%	15%	5%	9%	14%	9%	40%

Reporte



Questões a considerar

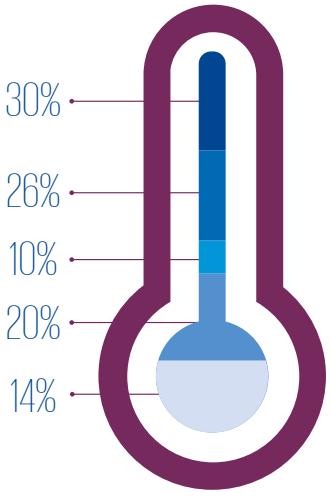
- Existe informação de qualidade de dados e infraestrutura de tecnologia para identificar, medir e reportar os riscos atuais e emergentes de toda a empresa em *compliance* com os requisitos regulatórios?
- As métricas de *compliance* são concebidas para satisfazer a comunicação das obrigações das regulamentações (Por exemplo: KRIs e KPIs)?
- Os recursos dedicados para sustentar o escopo necessário e a frequência dos relatórios de *compliance* são suficientes?
- Há protocolos de comunicação interna para o Conselho, comitês e gerentes seniores (frequência, escopo e os tipos de riscos)?
- Como é avaliada a efetividade e o impacto do seu relatório interno para as partes interessadas?
- As atividades e os dados reportáveis estão prontamente disponíveis mediante pedido dos reguladores?
- Como o Conselho vê a qualidade e robustez do seu relatório? Existem melhorias que estão procurando? Se sim, você pode endereçar essas melhorias? Quais são as limitações?
- Como as leis de privacidade globais / regulações impactam na sua capacidade de reportar?
- Quais protocolos e processos vigentes existem para gerir as suas responsabilidades de manutenção de registros?

Responder

- Comunicação periódica com o Conselho e a Administração (Por exemplo: reuniões, relatórios, prestação de contas etc.).
- Relatório de riscos regulatórios e de *compliance*.
- Manutenção de dados.

Nível de maturidade do tema abaixo nas empresas

Reporte regular e frequente à Alta Administração



Sem infraestrutura ***Infraestrutura mínima*** ***Função de monitoramento*** ***Função de integração*** ***Alta performance***

A quem a área de Compliance se reporta?

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
CEO	27%	26%	9%	15%	43%	15%	12%	6%
CFO	12%	18%	17%	13%	22%	39%	0%	9%
Chief Compliance Officer (Global ou Regional)	0%*	15%	5%	11%	16%	42%	21%	5%
Comitê de Auditoria	13%	12%	27%	13%	33%	27%	0%	0%
Conselho de Administração	10%	10%	15%	8%	62%	15%	0%	0%
Jurídico	4%	7%	45%	0%	0%	33%	22%	0%
Comitê de Ética e Compliance	2%	6%	13%	12%	50%	25%	0%	0%
Recursos Humanos	1%	0%	0%	0%	0%	0%	0%	0%
Conselho Fiscal	1%	1%	0%	100%	0%	0%	0%	0%
Gestão de Riscos	0%*	2%	0%	50%	0%	50%	0%	0%
Outras	10%	3%	0%	50%	50%	0%	0%	0%

**** Informação não capturada em 2015***

Qual é a frequência do reporte da área de Compliance à Administração?

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Anual	3%	6%	14%	0%	14%	43%	29%	0%
Semestral	9%	7%	22%	45%	33%	0%	0%	0%
Trimestral	21%	26%	9%	6%	33%	43%	6%	3%
Bimestral	10%	9%	9%	9%	55%	27%	0%	0%
Mensal	25%	23%	17%	14%	35%	28%	3%	3%
Quando solicitado	20%	20%	19%	19%	27%	15%	16%	4%
Não há comunicação entre a área de Compliance e a Administração	12%	9%	25%	7%	17%	17%	17%	17%

No último ano, qual foi o total de multas, sanções e penalidades pagas aos órgãos reguladores federais, estaduais e municipais?

	2015	2016	Consumer Markets	Financial Services	Government & Infrastructure	Industrial Markets	Technology, Media & Telecommunications	Outros
Até R$ 100.000	20%	29%	5%	24%	38%	14%	16%	3%
De R$ 101.000 a R$ 500.000	7%	8%	20%	30%	10%	40%	0%	0%
De R$ 501.000 a R$ 1MM	2%	5%	17%	16%	0%	33%	17%	17%
De R$ 1MM a R$ 5MM	4%	2%	0%	0%	34%	33%	33%	0%
Mais de R$ 5MM	5%	5%	43%	14%	29%	14%	0%	0%
Desconheço esta informação	57%	41%	15%	3%	33%	37%	6%	6%
Esta informação não é monitorada	5%	10%	31%	8%	38%	15%	8%	0%

Fale com o nosso time

Emerson Melo
Risk Consulting
Regulatory Compliance Brasil
Sócio-diretor
Tel.: +55 (11) 3940-4526
emersonmelo@kpmg.com.br

Fernando Lage
Risk Consulting
Sócio - Regiões Minas Gerais, Sul e Centro-Oeste
Tel.: +55 (31) 2128-5700
flage@kpmg.com.br

Bernardo Lemos
Risk Consulting
Sócio-diretor - Rio de Janeiro
Tel.: +55 (21) 3515-9335
blemos@kpmg.com.br

Alex Lopes
Risk Consulting
Sócio-diretor - Nordeste
Tel.: +55 (85) 3307-5125
alexlopes@kpmg.com.br

www.kpmg.com.br

/kpmgbrasil

Projeto gráfico e diagramação: Gaudí Creative Thinking