Agosto/2025

Trilha de Conhecimento

Controles Internos

BSM SUPERVISÃO DE MERCADOS

SUPERVISÃO DE MERCADOS

Sumário

1. Introdução

O dever de implementar controles internos

De acordo com o art. 4º da Resolução CVM nº 35/2021 ("**RCVM 35**"), as regras, os procedimentos e os controles internos devem ser escritos, passíveis de verificação e estar disponíveis para:

- a CVM,
- entidades administradoras de mercados organizados em que o intermediário seja autorizado a operar
- a entidade autorreguladora; para administradores, funcionários, operadores e demais prepostos do intermediário que desempenhem atividades de intermediação ou de suporte operacional; e
- assessores de investimento que prestem serviços ao intermediário e demais profissionais que mantenham, com o intermediário, contrato de prestação de serviços diretamente relacionados à atividade de intermediação ou de suporte operacional.

É considerado descumprimento da norma a inexistência ou a insuficiência de regras, de procedimentos e de controles, bem como sua não implementação ou a implementação inadequada para os fins previstos na norma. São evidências de implementação inadequada a reiterada ocorrência de falhas e a ausência de registro de aplicação de metodologia de forma consistente e passível de verificação.

A implementação de controles internos é essencial para a verificação do cumprimento adequado e eficaz da regulação.

Desde 2012, a internalização das recomendações do GAFI promoveu transformação no paradigma regulatório, inaugurando a **Abordagem Baseada em Risco (ABR)**. Na ABR, os próprios participantes de mercado são responsáveis pelo desenho de seus controles.

Os controles internos são a essência da operação segura e sustentável no mercado de capitais. Mais do que requisito regulatório, são componente estratégico para a integridade das instituições financeiras.

Pilar estratégico da integridade

Cabe a cada instituição identificar, avaliar, registar e mitigar os riscos de sua operação, considerando clientes, produtos, serviços, canais e fornecedores relevantes.

A criação de regras, procedimentos e controles internos, em conjunto com a **gestão de riscos**, transcende a noção de que são formalidades exigidas pela regulação ou meros *checklists* para evitar sanções.

Pelo contrário, trata-se de oportunidade para que os Participantes de mercado realizem diagnóstico aprofundado, corrijam rumos e promovam melhoria contínua de seus processos.

A implementação de sistema efetivo de controles demanda **investimento contínuo em pessoas**, processos e tecnologia, com envolvimento direto da alta administração e desenvolvimento de cultura organizacional orientada ao risco e à conformidade.

2. Noções gerais e definições

2.1. O que são controles internos?

Definição

Controles internos são processos formais definidos pelos órgãos de administração e executados por gestores e colaboradores para garantir o cumprimento dos objetivos institucionais. Esses processos fornecem segurança razoável quanto à eficiência operacional, à precisão dos relatórios e à conformidade com leis e políticas.

Objetivos

Na prática, os objetivos de controle interno são agrupados em:

- Objetivos operacionais: operações eficientes e eficazes (incluindo a salvaguarda de ativos).
- Objetivos de relatório: informações financeiras e gerenciais confiáveis e tempestivas.
- Objetivos de conformidade: aderência às leis, aos regulamentos e às políticas internas aplicáveis.

Elementos Fundamentais

Segundo o modelo COSO[1], amplamente adotado por instituições financeiras, a estrutura de controles internos baseia-se em cinco elementos fundamentais:

1. Ambiente de Controle: refere-se à cultura organizacional, ao comprometimento da alta administração e à definição clara de responsabilidades.
2. Avaliação de Riscos: identificação e análise dos riscos internos e externos que podem afetar o cumprimento dos objetivos da instituição.
3. Atividades de Controle: regras, políticas e procedimentos estabelecidos para mitigar os riscos identificados.
4. Informação e Comunicação: fluxo eficiente de informações relevantes entre as áreas da organização.
5. Monitoramento: avaliação contínua da eficácia dos controles, com eventuais ajustes.

Desse modo, controles internos, avaliação de riscos e políticas corporativas não são dimensões isoladas da integridade da organização, são componentes profundamente interligados do **sistema de governança único e coeso**.

A avaliação de riscos identifica as ameaças; as atividades de controle são as ações específicas tomadas para mitigar essas ameaças; e as políticas fornecem a estrutura formal que codifica e comunica essas ações.

Compreender esta relação dinâmica é crucial para projetar um sistema de controle que seja tanto eficaz quanto eficiente.

[1] COSO ou Committee of Sponsoring Organizations of the Treadway Commission, é uma organização americana privada sem fins lucrativos. Seu objetivo principal é fornecer liderança inovadora sobre três questões inter-relacionadas: Gestão de Riscos Corporativos (ERM), Controle Interno e Prevenção de Fraudes.

Tipos de controle interno

Os controles internos podem ser classificados com base em sua função e no momento de sua atuação em relação a potencial evento de risco. Este espectro inclui controles preventivos, detectivos e corretivos, que atuam em conjunto para formar defesa abrangente.

Controles preventivos

São medidas proativas destinadas a impedir que erros, irregularidades ou atos fraudulentos ocorram. Exemplos: segregação de funções, níveis de autorizações e aprovações, segurança dos ativos (incluindo controle de acesso e confidencialidade de dados).

Controles detectivos

São medidas reativas destinadas a encontrar erros ou irregularidades depois que já ocorreram, sendo essenciais para identificar quando os controles preventivos falharam. Exemplos: conciliações, revisão do desempenho operacional.

Controles corretivos

São as ações tomadas para resolver problemas identificados pelos controles detectivos.

Seu propósito não é apenas corrigir o erro imediato, mas também estabelecer procedimentos para prevenir sua recorrência. Isso inclui desenvolvimento e implementação de planos de remediação para tratar situações de controle identificadas.

A análise de causa raiz, realizada como parte dessa ação corretiva, fornece resposta crucial para redesenhar ou fortalecer os controles preventivos iniciais, completando assim o ciclo de melhoria contínua.

Controle interno x auditoria interna

O controle interno engloba o conjunto completo de sistemas, políticas, procedimentos e processos que são implementados e operados pela alta administração, gestores e equipe.

A auditoria interna fornece avaliação objetiva e independente do sistema de controle interno para auxiliar a alta administração e os gestores a monitorar e a avaliar sua adequação e eficácia.

Em essência, o controle interno é o sistema que está sendo avaliado, e a auditoria interna é o avaliador.

2.2. Melhores práticas: o que fazer?

ESTABELECER e comunicar incansavelmente o forte *"tone at the top"*. A liderança deve personificar e fazer cumprir a cultura de integridade e responsabilização.

IMPLEMENTAR estrutura de governança clara, como o modelo das Três Linhas de Defesa para definir papéis e garantir que a responsabilidade pelo risco seja compreendida e aceita pelas unidades de negócio.

CONDUZIR avaliações de risco regulares, abrangentes e prospectivas para garantir que os controles sejam direcionados com precisão às ameaças mais significativas, tanto atuais quanto emergentes.

INVESTIR continuamente em treinamento. Assegurar que cada colaborador entenda não apenas quais são suas responsabilidades de controle, mas os motivos pelos quais elas são importantes para a segurança e a integridade da instituição.

DOCUMENTAR e formalizar políticas e procedimentos e registrar a justificativa das principais decisões de controle, especialmente para processos de alto risco, mantendo a rastreabilidade das decisões.

UTILIZAR tecnologia e automação para melhorar a eficiência e a eficácia dos controles e garantir que os sistemas sejam submetidos a seus próprios processos rigorosos de governança e validação.

GARANTIR que controles sejam proativos, agreguem valor e tenham custo-benefício. O custo do controle não deve superar o benefício que ele proporciona.

2.3. Melhores práticas: o que NÃO fazer?

NÃO TRATAR os controles internos como mero exercício de conformidade para cumprir formalidades, ou como função que pertence exclusivamente aos departamentos de auditoria interna ou de compliance, pois é responsabilidade de todos.

NÃO VIOLAR o princípio da segregação de funções. Nunca permitir que um único indivíduo tenha controle de ponta a ponta sobre transação financeira crítica.

NÃO IMPLEMENTAR controles de forma isolada. Atividade de controle que não está claramente ligada à mitigação de risco específico e identificado é provavelmente ineficiente e desperdício.

NÃO NEGLIGENCIAR o monitoramento e o teste regular dos controles. Controle não testado é controle não confiável, e sua falha só será descoberta depois que o dano já tiver ocorrido.

NÃO CAIR na armadilha de acreditar que os controles fornecem segurança absoluta. Reconheça as limitações inerentes, como o conluio e a burla pela administração, e estabeleça controles detectivos compensatórios para mitigar esses riscos.

NÃO PERMITIR que as comunicações relacionadas ao negócio migrem para plataformas não monitoradas e “fora do canal”, como aplicativos de mensagens pessoais. Esta é uma área de grande fiscalização regulatória e representa falha de controle significativa.

NÃO SOBRECARREGAR o sistema com controles em excesso. Concentre-se nos controles-chave que abordam riscos mais significativos para evitar ineficiência e "fadiga de controle".

3. Regras, procedimentos e controles internos

3.1. Conteúdo mínimo

Conforme a RCVM 35, a entidade administradora de mercado em que o intermediário estiver autorizado a operar e a respectiva entidade autorreguladora devem estabelecer **conteúdo mínimo** das regras, dos procedimentos e dos controles internos que o Participante deve criar, e fiscalizá-las.

A BSM, em suas Normas de Supervisão e Notas de Orientação, estabelece conteúdos que o Participante deve considerar em suas regras, procedimentos e controles internos.

As **Regras e Parâmetros de Atuação (RPA)** ou **Normas e Parâmetros de Atuação (NPA)** estabelecem as diretrizes e os critérios para a atuação dos Participantes no mercado.

Esses documentos visam nortear a conformidade com as normas da CVM e da B3, protegendo os investidores e Participantes e contribuindo para a integridade e a eficiência do mercado.

Para além de um conteúdo mínimo, o Participante pode tratar em suas RPA/NPA de procedimentos e regras internas que afetam a forma como realiza a intermediação de operações para seus clientes.

3.1. Conteúdo mínimo (cont.)

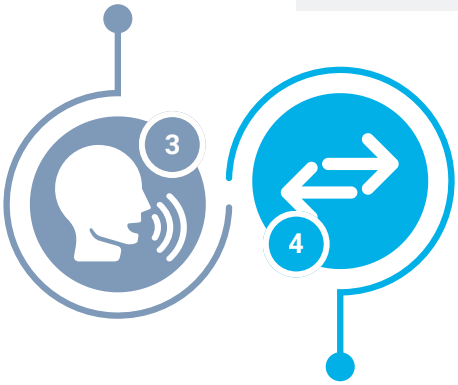
O conteúdo mínimo que as RPA/NPA devem abranger envolve:

Cadastro

Monitoramento de procedimentos de **KYC**

Ordens

1. Tipos de ordens aceitas
2. Horário de recebimento
3. Forma de emissão e recebimento — incluindo os serviços de mensagem instantânea aceitas;
4. Prazo de validade
5. Procedimento de recusa e cancelamento — inclusive aquelas recebidas por intermédio de *home broker* ou outras plataformas de negociação, e canais alternativos disponibilizados aos clientes;
6. Registro
7. Execução, não execução e confirmação de ordens
8. Sistema de gravação
9. Tratamento em caso de concorrência de ordens — devendo deixar clara a forma como as ordens de clientes terão prioridade sobre as operações de carteira própria e de pessoas vinculadas ao Participante, inclusive na oferta de serviço de *Facilitation*.



Operações

1. Política de Operações de Pessoas Vinculadas e de carteira própria;
2. Distribuição das operações, inclusive regras sobre brokerage[1] e repasse tripartite[2];
3. *Facilitation;*
4. RLP;
5. Liquidação de operações; e
6. Sistemática de reversão de operações lançadas na Conta Erro[3] e na Conta Erro Operacional[4].

Controle de risco

Custódia de ativos

Forma de **comunicação** aos clientes das alterações nas RPA/NPA

[1] **Brokerage:** é o modelo tradicional de repasse, no qual o cliente firma contrato diretamente com o Participante que executa as ordens.
[2] **Repasse Tripartite:** envolve três partes — o cliente, o assessor de investimentos (ou escritório vinculado) e o Participante. É comum quando o assessor atua como originador da ordem, mas a execução é feita por outro Participante.
[3] **Conta Erro:** conta automaticamente criada pela Câmara B3, para os Participantes de Negociação Plenos e Participantes de Liquidação, que recebem operações não alocadas para Comitentes na forma e no prazo estabelecido, em decorrência de erro operacional.
[4] **Conta Erro Operacional:** conta automaticamente criada pela Câmara B3 e utilizada pelos Participantes de Negociação Plenos e pelos Participantes de Liquidação para realocação de operações por motivo de erro operacional.

3.1. Conteúdo mínimo (cont.)

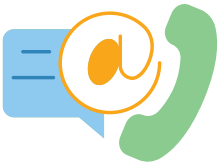
Para que as regras reflitam a realidade e particularidades do Participante, é preciso atentar para os critérios a seguir.

Natureza, porte, complexidade e estrutura

Perfil de Risco

Modelo de negócio

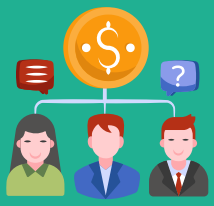
Volume operado



Canais de acesso oferecidos

Produtos e Serviços oferecidos

Complexidade das operações executadas



Tipos de clientes atendidos

3.2. Princípios da atuação do Participante

Os seguintes princípios devem nortear as RPN/NPA para a condução das atividades do Participante:

1) Probidade na condução das atividades;

2) Zelo pela integridade do mercado, inclusive quanto à seleção de clientes e à exigência de depósito de garantias;

3) Capacitação para desempenho das atividades;

4) Diligência no cumprimento de ordens e na especificação de clientes;

5) Diligência no controle das posições dos clientes na custódia, com a conciliação periódica entre:

- Ordens executadas;
- Posições constantes em extratos e demonstrativos de movimentação fornecidos pela entidade prestadora de serviços de custódia;
- Posições fornecidas pelas câmaras de compensação e liquidação;

6) Obrigação de apresentar, aos clientes, informações necessárias ao cumprimento de ordens;

7) Adoção de providências no sentido de evitar a realização de operações em situação de conflito de interesses e assegurar tratamento equitativo a seus comitentes; e

8) Suprir seus clientes, em tempo hábil, com a documentação das operações realizadas.

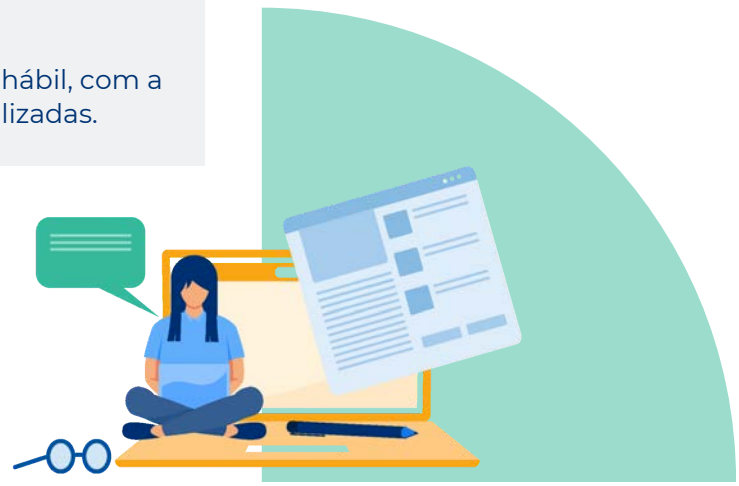
Formato e Publicidade

O conteúdo das RPA/NPA deve ser elaborado em linguagem clara, suscinta e de fácil entendimento pelo cliente, e utilizando de conceitos e termos em consonância com as normas de regulação e autorregulação em vigor, devendo ser mantida atualizada.

O intermediário deve divulgar, em sua página na rede mundial de computadores, antes do início de suas operações. Deve ser informada a data de início de sua vigência e seu conteúdo é parte integrante do contrato de intermediação do Participante com seu cliente.

Alterações devem ser comunicadas a todos os clientes antes da vigência do novo documento.

A BSM, em seus processos de supervisão e fiscalização, verifica se as RPA/NPA seguem os deveres estabelecidos pela CVM e as regras de autorregulação da B3 e da BSM.



4. Medidas disciplinares (*enforcement*)

Enforcement

Infrações às normas relativas a controles internos podem levar à adoção de medidas disciplinares em face do diretor responsável por conduta irregular (violação de deveres fiduciários) e falha em controles internos, sem prejuízo da responsabilidade de outros membros da alta administração, conforme o caso.

A governança dos controles internos é atribuição da alta administração da instituição, incluindo o conselho de administração e a diretoria executiva. Esses órgãos devem:

Dificuldades dos Participantes ao implementar seus controles internos

Integração de sistemas

Muitas instituições possuem sistemas fragmentados, o que dificulta a conciliação de dados, a rastreabilidade de processos e a geração de relatórios consistentes.

Falta de cultura de controle

Algumas instituições ainda tratam o tema como burocracia, sem a devida internalização da importância estratégica dos controles.

Definição inadequada de papéis e responsabilidades

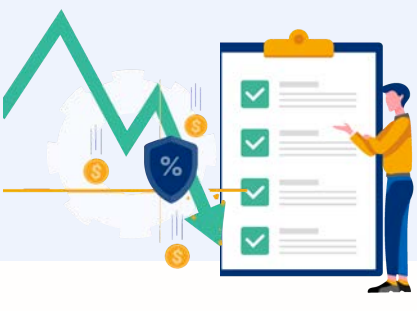
É comum a ausência de segregação adequada de funções, o que eleva o risco de fraudes e de falhas operacionais.

Falta de qualificação profissional

O dimensionamento da equipe responsável pelos controles internos, aliado à falta de capacitação, compromete a efetividade das atividades de monitoramento e auditoria.

Documentação insuficiente

Muitos participantes não mantêm registros adequados de seus processos, dificultando a demonstração de cumprimento das exigências regulatórias em caso de auditoria.



4.1. Conheça seus deveres

O **dever de diligência** dos integrantes da alta administração pode ser desdobrado em algumas dimensões:

- Dever de conhecer regras, processos, controles internos e seus indicadores de efetividade;
- Dever de se informar, monitorar alertas, desenhar e aprimorar rotinas de acompanhamento, avaliar denúncias;
- Dever de aferir o cumprimento de regras ao longo do tempo, segundo abordagem baseada em risco.

Nesse contexto, pode ser adotado o princípio **"Conheça seus Deveres" (*Know Your Duties* – KYD)**, inspirado na lógica do KYC e do KYT, para converter o dever abstrato de diligência em práticas concretas e verificáveis.

O primeiro passo consiste em **mapear todas as obrigações** legais, autorregulatórias e internas que recaem sobre o sistema de controles, associando a cada uma delas **indicador objetivo de cumprimento**, como prazo, frequência ou limiar de materialidade.

Concluída essa etapa, é indispensável passar à **análise de riscos**. A instituição precisa identificar, avaliar e classificar as ameaças inerentes à sua operação, levando em conta não apenas a exposição associada aos clientes, mas também aos produtos, serviços, canais de distribuição e prestadores de serviços relevantes. Essa avaliação fornece a base para a seleção das atividades de controle, que são as ações específicas desenhadas para mitigar as ameaças priorizadas.

As **políticas**, por sua vez, formalizam esses controles e asseguram que a lógica de mitigação seja comunicada e aplicada de forma consistente em toda a organização. Sem esse fluxo – **do risco à política** – o sistema de controles internos perde coerência e efetividade.

Depois, é essencial instituir **rotinas de monitoramento** que agreguem desvios de processo, falhas sistêmicas e denúncias recebidas, estabelecendo gatilhos claros para a adoção de medidas.

Nesse passo, é possível ver com maior nitidez a diferença entre controlar e monitorar.

Monitorar é medir um evento, o cumprimento da regra e seus efeitos.

Controlar é planejar essas medidas, analisá-las e tomar decisões.

4.1. Conheça seus deveres (cont.)

Em paralelo, deve haver ciclos contínuos de **testes de aderência e efetividade**, priorizando processos críticos ou historicamente frágeis, com amostras estatisticamente representativas e documentação minuciosa da metodologia, das situações identificadas e dos planos de ação.

Todas as **decisões** tomadas a partir desses **alertas** precisam ficar registradas de forma rastreável para fins de supervisão e fiscalização, inclusive quando forem delegadas a terceiros ou a sistemas automatizados.

O cumprimento diligente dessa função exige revisão periódica da **suficiência** de pessoas, de orçamento e de tecnologia, ajustando políticas e recursos sempre que houver mudanças regulatórias, de mercado ou de infraestrutura.

Por fim, os **relatórios** destinados à administração e às autoridades competentes devem apresentar não só as situações identificadas, mas também a evolução dos planos de ação e as justificativas para eventuais atrasos, permitindo demonstrar, de forma inequívoca, o comprometimento da instituição e dos seus diretos responsáveis com a integridade do sistema de controles internos.

4.2. Falha de controle (cont.)

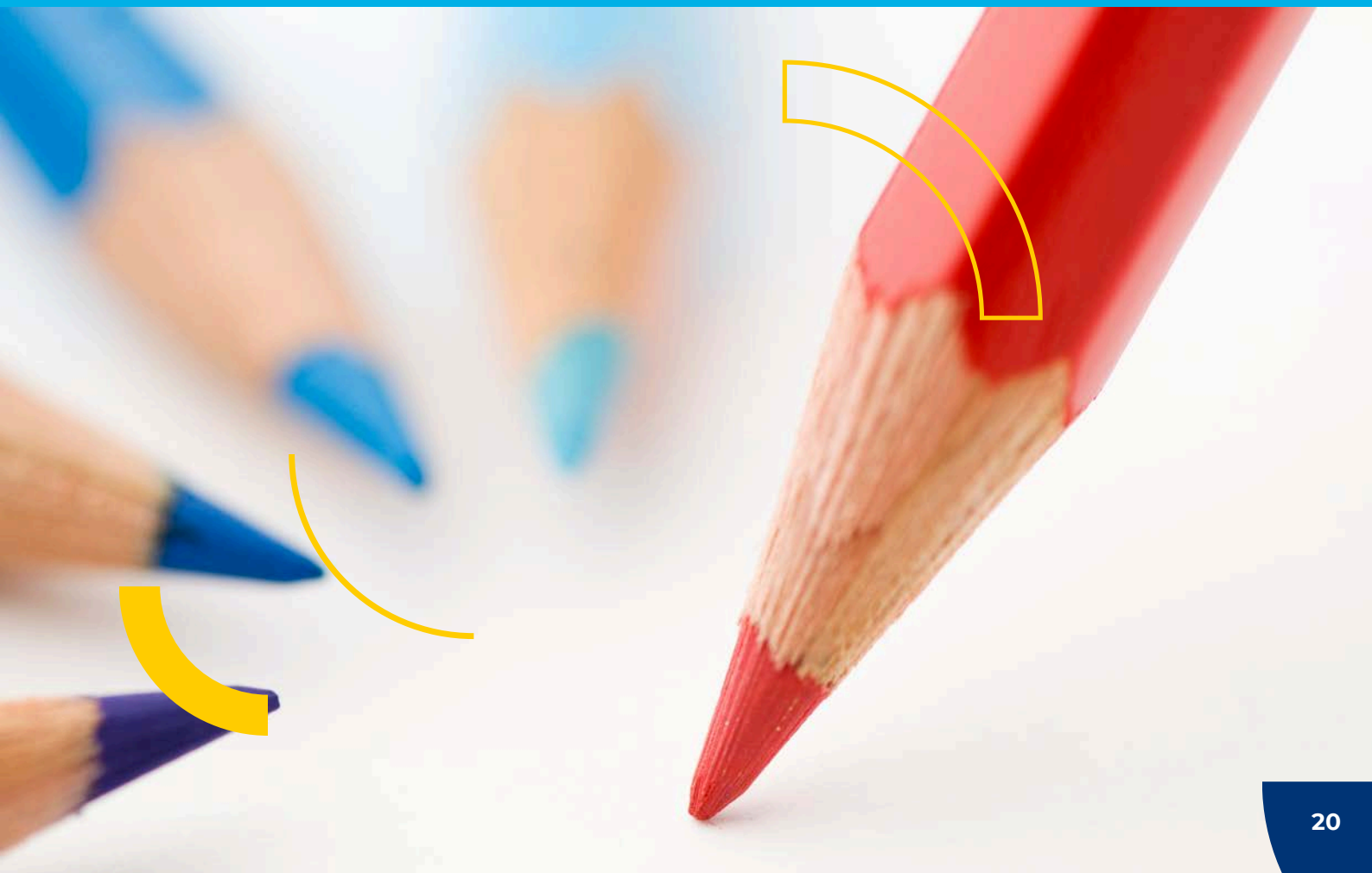
No contexto da regulação e da autorregulação, a **falha no controle interno** é a **incapacidade** de atingimento de seus **objetivos** regulatórios, isto é, de os processos definidos pela alta administração não serem aptos a fornecer **segurança razoável** quanto à conformidade com leis, regulamentos e políticas.

As falhas de controle podem ser analisadas em termos qualitativos e quantitativos.

Consequências

As falhas podem resultar em:

- Apontamentos em auditorias internas e externas;
- Planos de ação obrigatórios a serem estabelecidos e cumpridos;
- Abertura de processos administrativos disciplinares (PAD) ou sancionadores;
- Impactos reputacionais e operacionais; e/ou
- Riscos de penalidades financeiras e restrições de atuação no mercado.



4.2. Falha de controle

Aspectos quantitativos

A análise quantitativa das falhas em controles internos diz respeito à recorrência de situações e à gravidade de seu impacto.

Quantas vezes a mesma falha pode ser admitida? O elemento fundamental dessa definição é o conceito de **segurança razoável** (*reasonable assurance*). Não se espera que os sistemas de controles internos forneçam segurança absoluta.

Este é o reconhecimento pragmático das limitações inerentes de qualquer sistema de controle, as quais incluem potencial para erro humano devido ao descuido ou ao esgotamento, à burla por meio de conluio entre dois ou mais indivíduos, ao julgamento falho na tomada de decisões e à possibilidade de burla pela administração, na qual funcionários da alta administração ignoram intencionalmente os controles estabelecidos.

Compreender este conceito é vital para gerenciar expectativas das partes interessadas e ressaltar a necessidade de monitoramento e de melhoria contínuos em vez de abordagem do tipo "**implementar e esquecer**" (*set it and forget it*).

A extrapolação de **limite quantitativo de falhas em uma janela temporal** que pode deflagrar medida de *enforcement* deve levar em conta o risco do intermediário e impacto no mercado.

Aspectos qualitativos

Em sua dimensão qualitativa, falhas em controles internos abrangem implementação ausente ou inadequada em face dos riscos específicos do Participante.

São exemplos:

- Ausência de validação para atualização de dados declarados no cadastro.
- Incompatibilidade entre risco do negócio e complexidade de seu modelo e parâmetros de sensibilidade da política do Participante.
- Inexecução de mecanismos de liquidação compulsória.
- Incompatibilidade entre transferências de custódia e situação patrimonial e financeira.
- Ausência de critérios para operações de venda à descoberto.
- Ausência de critérios para verificar recomendações de produtos.

5. Abrangência

5.1. Negócios e controles internos

Há dois grandes grupos de controles internos: **negócios** e **tecnologia**. Deve ser levada em conta a realidade do intermediário na equação de risco, incluindo parâmetros como ativos sob custódia, quantidade de contas de clientes, produtos e serviços, canais de distribuição, exposição a mercados e jurisdições de maior risco, dentre outros.

Cadastro (art. 7° da RCVM 35), KYC, PLD/FTP e manutenção de dados

Deve haver procedimentos e controles para os processos de elaboração, manutenção e atualização do **cadastro** de clientes, conforme conteúdo mínimo determinado pela **RCVM 50**, abrangendo, quando aplicável, o cadastro simplificado, o cadastro de acesso e sistemas alternativos de cadastro.

Igualmente, deve haver procedimentos e controles para assegurar o cumprimento do dever de verificação da adequação dos produtos, serviços e operações ao perfil de investimento do cliente (***suitability***).

O cadastro de clientes mantido pelo intermediário deve ser **rastreável**, isto é, deve permitir a identificação da data e do conteúdo de todas as alterações e atualizações realizadas.

O intermediário deve garantir que os sistemas eletrônicos de cadastro contenham trilhas de auditoria íntegras e suficientes para assegurar o rastreamento das inclusões, alterações e exclusões, e que permitam identificar, no mínimo o usuário responsável, a data e horário da ocorrência do evento e se o evento se trata de inclusão, alteração ou exclusão.

Outros procedimentos e controles correlatos dizem respeito à PLD/FTP e guarda de arquivos:

Especificação de comitentes

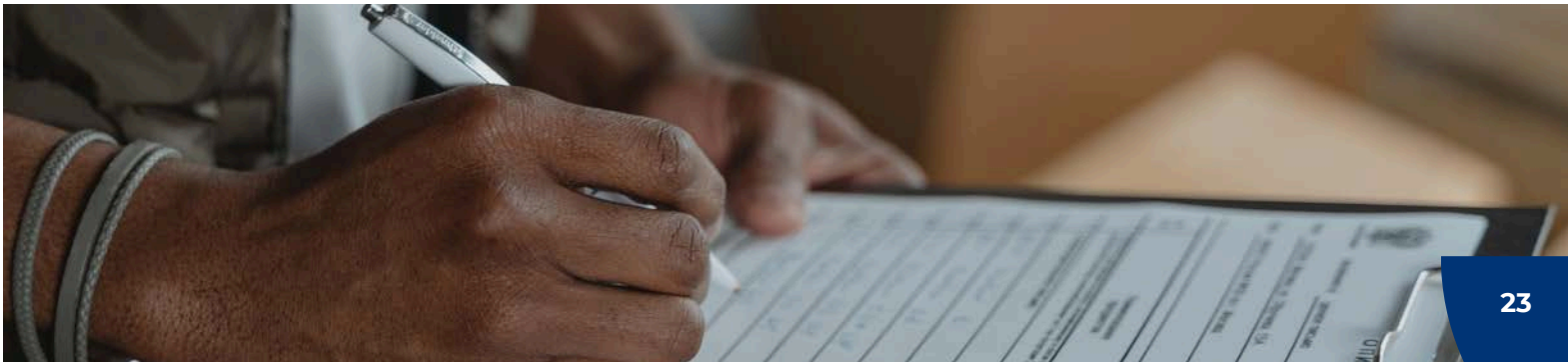
Procedimentos e controles para assegurar a identificação de comitentes finais nos prazos estabelecidos na regulamentação.

Pagamento e recebimento de valores

Procedimentos e controles para cumprimento das limitações às formas de pagamento e recebimento de valores do cliente.

Manutenção de arquivos

Procedimentos e controles para assegurar a manutenção e *backup* de documentos, informações, gravações, trilhas de auditoria e registros exigidos pelo prazo mínimo estabelecido na regulamentação.



5.1. Negócios e controles internos (cont.)

Procedimentos e controles relativos a ordens (art. 21 da RCVM 35)

O intermediário deve estabelecer regras, procedimentos e controles internos sobre a execução de ordens, de modo a permitir que obtenha as **melhores condições** disponíveis no mercado para a execução das ordens de seus clientes, atendendo o **dever de melhor execução**.

Também deve ser possível, a qualquer tempo, a **vinculação** entre a **ordem** transmitida, a respectiva **oferta** e o negócio realizado

Transmissão de ordens

Procedimentos e controles relacionados à transmissão e registro de ordens com identificação e validação do emissor, origem e forma de transmissão, horário do seu recebimento e as condições de sua execução.

Gravação de ordens

Procedimentos e controles relacionados à documentação de ordens transmitidas presencialmente e manutenção de sistema de gravação de todos os diálogos mantidos com clientes, inclusive por intermédio de prepostos previamente à sua execução.

Execução de ordens

Procedimentos e controles para vinculação entre a ordem transmitida, a oferta e o negócio realizado, cumprimento das condições estabelecidas pelo cliente e atendimento às regras de melhor execução.

Manutenção de arquivos e dados relativos a ordens

O intermediário deve arquivar os registros das ordens transmitidas pelos clientes e as condições em que foram executadas, independentemente de sua forma de transmissão e, ainda, adotar procedimentos específicos de arquivamento dos registros de dados e de voz relativos às ordens transmitidas que garantam:

- a confidencialidade, autenticidade, integridade e disponibilidade das informações;
- trilhas de auditoria íntegras e suficientes para assegurar o rastreamento das inclusões, alterações e exclusões; e
- a manutenção de cópias de segurança em ambiente distinto do destinado ao armazenamento das informações a que se refere o caput, em condições seguras de armazenamento, acesso e preservação.

Roteiro do PQO

O Participante deve monitorar as operações por ele intermediadas, com o propósito de assegurar que (i) sejam previamente ordenadas pelo Cliente; (ii) sejam executadas nas condições indicadas pelo Cliente ou nas melhores condições existentes; e (iii) não impliquem custos excessivos e inadequados ao Perfil de Investimento do Cliente.

5.1. Negócios e controles internos (cont.)

Conflitos de interesse e normas de conduta

Os procedimentos e controles relativos a conflitos de interesse e normas de conduta abrangem sua Política de Responsabilidade Socioambiental e os temas a seguir.

Atuação de pessoas vinculadas e carteira própria

Procedimentos e controles relacionados a operações de pessoas vinculadas e carteira própria do Participante.

Monitoramento de operações e ofertas

Procedimentos e controles para monitorar continuamente as operações e ofertas, de maneira a identificar e mitigar práticas irregulares.

Certificação de profissionais

Procedimentos e controles para monitoramento da existência e validade da certificação dos profissionais que atuarem nos mercados da B3.

Segregação de acessos e funções

Procedimentos e controles para assegurar a segregação das funções desempenhadas pelos integrantes do Participante, incluindo o acesso a dados e a informações sensíveis, de forma que seja evitado conflito de interesses.

O intermediário deve estabelecer regras, procedimentos e controles internos que sejam aptos a prevenir que os interesses dos clientes sejam prejudicados em decorrência de conflitos de interesses, devendo:

- Identificar quaisquer conflitos de interesses que possam surgir entre o intermediário, ou pessoas vinculadas a ele, e seus clientes, ou entre os clientes;
- Permitir que, diante de situação de conflito de interesses, o intermediário possa realizar a operação, em nome do cliente, com independência; e
- Estabelecer mecanismos para informar ao cliente que o intermediário e as pessoas a ele vinculadas estão agindo em conflito de interesses e as fontes desse conflito, antes de efetuar a operação.

Repasse de operações (art. 26 da RCVM 35)

Os controles devem prever, ao menos, o conteúdo mínimo do contrato que estabelece o vínculo de repasse entre os intermediários e a forma de identificação e registro das operações decorrentes de repasses.

5.2. Tecnologia e controles internos

A descrição das regras, processos e controles implantados também deve abranger o monitoramento da infraestrutura de tecnologia da informação, conforme estabelece a RCVM 35, o Roteiro PQO e a Norma de Supervisão da BSM sobre Segurança da Informação no âmbito da Segregação de Funções, no que couber, tais como:

- Segurança da informação;
- Gerenciamento de acessos e senhas, incluindo a eficácia do processo de desligamento de funcionários detentores de quaisquer acessos a sistemas internos e externos que compõem a infraestrutura do Participante;
- Processo de continuidade de negócios;
- Sistemas críticos;
- Tratamento e controle de dados de clientes;
- Segurança cibernética;
- Registro das situações de indisponibilidade em sistemas que impactem as operações (sistemas de negociação) e a gravação das ordens de clientes; e
- Contratação de serviços relevantes prestados por terceiros.

Também devem ser examinada a **segregação lógica das funções** desempenhadas pelos integrantes do Participante, incluindo o acesso aos dados e informações sensíveis, de forma que seja evitado o conflito de interesses, bem como o gerenciamento de senhas e a identificação de sistemas sem trilhas de auditoria.

Dados e informações sensíveis (art. 42 da RCVM 35)

O intermediário deve considerar como **sensíveis**, no mínimo, os dados cadastrais e demais informações que permitem a identificação de clientes, suas operações e posições de custódia.

Adicionalmente, deve-se garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis, contemplando:

- As diretrizes para a identificação e classificação dos dados e informações sensíveis;
- Os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos.
- A proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso ou destruição não autorizados, vazamento ou adulteração;
- A concessão e administração de acessos individualizados a sistemas, bases de dados e redes; e
- Segregação de dados e controle de acesso, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações.

5.2. Tecnologia e controles internos(cont.)

Política de segurança cibernética e incidentes relevantes (arts. 45 e 46 da RCVM 35)

A política de segurança da informação do intermediário deve contemplar programa de segurança cibernética, abrangendo procedimentos e controles internos adotados para:

- Verificar a implementação, a aplicação e a eficácia das medidas adotadas para reduzir a vulnerabilidade da instituição contra-ataques cibernéticos; e
- Efetuar o monitoramento contínuo e a detecção de ataques cibernéticos em tempo hábil.

O Participante deve ter programas de conscientização e treinamento aos colaboradores, Prepostos e prestadores de serviço sobre segurança da informação e segurança cibernética, no mínimo, àqueles com acesso a dados de clientes.

Adicionalmente, o intermediário deve comunicar, tempestivamente, aos seus órgãos de administração e à CVM a ocorrência de incidentes de segurança cibernética relevantes.

O intermediário deve elaborar e enviar à CVM relatório final contendo no mínimo:

- Descrição do incidente e das medidas tomadas, informando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes; e
- Os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar ocorrência de incidentes de segurança cibernética, se for o caso.

Por fim, é preciso registrar as situações de indisponibilidade em sistemas que impactem as operações dos clientes (sistemas de negociação) e a gravação das ordens dos clientes.

5.2. Tecnologia e controles internos (cont.)

Política de segurança cibernética e incidentes relevantes (arts. 45 e 46 da RCVM 35)

No caso de serviços prestados por terceiros, o intermediário deve identificar e relacionar seus prestadores de serviços relevantes, avaliar os controles realizados por estes provedores e se certificar que os contratos de prestação de serviços assegurem:

- o cumprimento das exigências de manutenção de informações;
- o acesso da instituição aos dados e informações a serem processados ou armazenados pelo prestador de serviços; e
- a confidencialidade, integridade, disponibilidade e a recuperação dos dados e informações processados ou armazenados pelo prestador de serviços.

6. Testes dos controles internos

Testes e ABR

O paradigma da abordagem baseada em risco envolve ciclo de melhoria contínua. A instituição deve planejar seus controles, executá-los, checar sua eficácia de forma contínua e, agir para corrigir processos e controles ineficazes, buscando sempre aprimorá-los.

Para ilustrar a aplicação da abordagem baseada em risco, pode-se usar uma analogia com um diagnóstico médico. Ao chegar ao hospital, o paciente passa por triagem (identificação de riscos), é examinado pelo médico, que solicita exames (testes de efetividade) para analisar, compreender e classificar a enfermidade.

Com base no diagnóstico, o tratamento é prescrito (mitigação do risco). Se os sintomas persistirem (situação de não conformidade não foi resolvida), há retorno e reavaliação, similar ao endereçamento do problema para o relatório do ano seguinte.

Representatividade estatística

Ao realizar os testes dos processos e controles, o Participante deve demonstrar que as amostras foram representativas, fazendo-se referência à descrição de metodologia para a seleção de amostra. É necessário que os testes incluam amostras e/ou universos de análise, com representatividade estatística, que comprovem a efetividade dos procedimentos e das diligências implementadas durante o período avaliado.

Se todos os indicadores apresentarem nota máxima (100% de conformidade), isso gera suspeita e pode indicar que o teste é falho ou que algo está errado. Identificar processos e controles ineficazes e endereçá-los para tratamento é sinal de autocrítica e maturidade.

Tipos de testes

- **Testes de aderência:** se os controles estão sendo executados conforme o previsto;
- **Testes de eficiência e eficácia:** se os controles são eficazes para mitigar os riscos identificados;
- **Revisões** de políticas e procedimentos sempre que houver mudanças significativas no ambiente de negócios ou no arcabouço regulatório.

Os controles internos devem ter sua efetividade testada continuamente. A definição do escopo dos testes deve considerar a criticidade e materialidade de cada processo para o perfil da instituição. Processos com histórico de falhas ou que passaram por mudanças recentes podem exigir testes mais diferenciados.

Os testes devem ser conduzidos pela área responsável (segunda linha de defesa), não pela auditoria (terceira linha). A **segunda linha de defesa** é composta por funções que fornecem conhecimento especializado, suporte, monitoramento e desafio às atividades de gerenciamento de riscos da primeira linha. Esta linha ajuda a estabelecer as políticas, as estruturas e as ferramentas abrangentes que a primeira linha utiliza para gerenciar seus riscos. Ela atua como uma verificação crucial sobre os esforços da primeira linha, garantindo que os controles sejam adequadamente projetados e estejam operando conforme o planejado.

Conjunto mínimo

Nesse contexto, podemos considerar o conjunto mínimo de processos e controles que devem ser avaliados:

- as atividades de cadastro de clientes;
- transmissão e execução de ordens, especificação de comitentes;
- operações com pessoas vinculadas;
- repasse de operações
- pagamento e recebimento de valores;
- normas de conduta e manutenção de arquivos, abrangendo tanto a atuação do intermediário no mercado de bolsa quanto no mercado de balcão organizado;
- monitoramento da infraestrutura de tecnologia da informação; e
- programa de segurança cibernética.

Exemplos

Amostra ineficaz

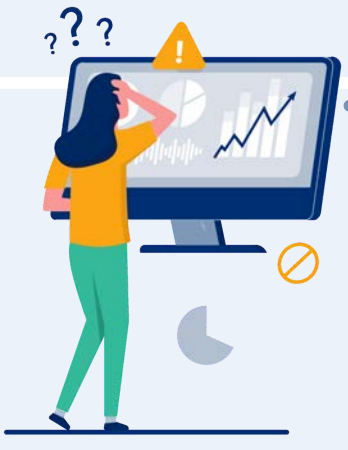
Participante com milhares de clientes testou apenas dois cadastros "porque eram 100 % da amostra selecionada". Conclusão regulatória: teste inválido, metodologia inadequada.

Comunicações duplicadas

Alguns participantes anexaram ao RCI comunicações enviadas ao COAF, sem indicar relação com infrações da competência CVM previstas no art. 14 da RCVM 35. Isso expõe dados sensíveis e não satisfaz o comando normativo.

Uso de *bureau*

Mencionar que o fornecedor "é líder mundial" não basta. Devem ser apresentados testes de aderência, falsos positivos e mitigadores adicionais quando o *bureau* não valida campos críticos (p. ex., endereço).



7. Relatório de Controles Internos

7.1. Objetivos e diretrizes de elaboração

A supervisão e fiscalização do mercado de capitais brasileiro, conduzida pela CVM e pela BSM, tem se pautado cada vez mais pelo diálogo e pela orientação como principais ferramentas para aprimoramento das práticas dos Participantes.

Nesse contexto, a elaboração do Relatório de Controles Internos ("**RCI**"), previsto na RCVM 35, e do Relatório de Avaliação Interna de Riscos ("**RAIR**"), focado em PLD/FTP, conforme a RCVM 50, representa pilar de governança e integridade.

Embora não exista formato rígido, o RCI completo e eficaz deve seguir **narrativa lógica**, que pode ser iniciada pela jornada do cliente, e conter elementos essenciais.

O Participante deve elaborar o RCI com o objetivo de articular a visão da Instituição em relação à gestão e ao controle de risco operacional, sua estrutura de controles internos, bem como apresentar as considerações pertinentes em relação ao ano anterior. Sua elaboração deve se atentar nos princípios e conceitos estabelecidos na governança da instituição.

A estrutura deve incluir a **descrição dos controles**, das **linhas de defesa** e, em seguida, detalhar os **processos avaliados**. Para cada processo a metodologia de teste deve ser claramente exposta, justificando o universo analisado e os critérios de amostragem. A descrição do teste precisa ser robusta o suficiente para que o leitor externo compreenda sua concepção e sua capacidade de avaliar o processo.

É fundamental que o relatório apresente **conclusões sobre os testes e detalhe os apontamentos**. A ausência total de resultado dos testes que necessitem de aprimoramento no processo ou no controle é forte indício de que o controle em si pode ser falho.

Os **planos de ação** para corrigir as deficiências – sejam elas identificadas internamente ou por meio de fiscalizações da CVM ou da BSM – devem ser explicitados, com cronogramas e justificativas para eventuais ajustes.
Se o processo listado na regulação ou no Roteiro PQO não for aplicável à instituição, isso deve ser expressamente mencionado e justificado no relatório.

A base normativa para a elaboração do RCI encontra-se no art. 5º da RCVM 35 e no Roteiro PQO.

Devem ser consultados também o Guia para a Elaboração do Relatório de Controles Internos (RCI) e o Guia para Elaboração do Relatório de Avaliação Interna de Risco (RAIR), elaborados pela BSM.

7.1. Objetivos e diretrizes de elaboração (cont.)

O caminho para a elaboração do RCI envolve:

Antecipação

Iniciar a elaboração do relatório muito antes do prazo final, tratando-o como projeto contínuo ao longo do ano.

Profundidade

Abandonar a superficialidade e relatos genéricos em favor de análises detalhadas, com metodologias claras e testes robustos.

Transparência

Não ter receio de apontar as próprias deficiências. Identificar um problema é o primeiro passo para resolvê-lo e demonstra uma cultura de autocrítica e melhoria contínua.

Integração

Garantir que os processos e as informações conversem entre si. O cadastro alimenta o suitability, que impacta o monitoramento de PLD/FTP. Os relatórios devem refletir essa integração.

Para que o Relatório Anual de Controles Internos cumpra integralmente as exigências da RCVM 35 e do Roteiro PQO da B3, a alta administração deve entender o documento como a consolidação de quatro grandes vertentes de informação:

1	O **retrato atualizado do ambiente** de controles: os controles implantados, seus tipos e atividades e operações abrangidas.
2	A **demonstração da eficácia** desses controles: metodologia de testes (incluindo critério de amostragem e parâmetros de atipicidade), detalhamento da realização e conclusões quanto à eficiência e eficácia dos testes realizados.
3	As **não conformidades** identificadas pela própria instituição, pelos seus reguladores e autorreguladores no ano de referência, juntamente com recomendações, planos de ação e cronogramas de saneamento para correção.
4	A **responsabilização da alta administração** pelos avanços ou pelos atrasos do ciclo de melhoria contínua: • Avaliação de riscos para o intermediário em relação aos seus controles internos e quanto à sua vulnerabilidade a ataques cibernéticos. • Manifestação do diretor responsável pelo RCVM 35 quanto ao cumprimento das normas e ao tratamento das deficiências encontradas ao longo do tempo – tanto atualmente como em comparação com exercícios anteriores – e à adequação do plano de continuidade de negócios.

7.2. Retrato atualizado do ambiente de controle

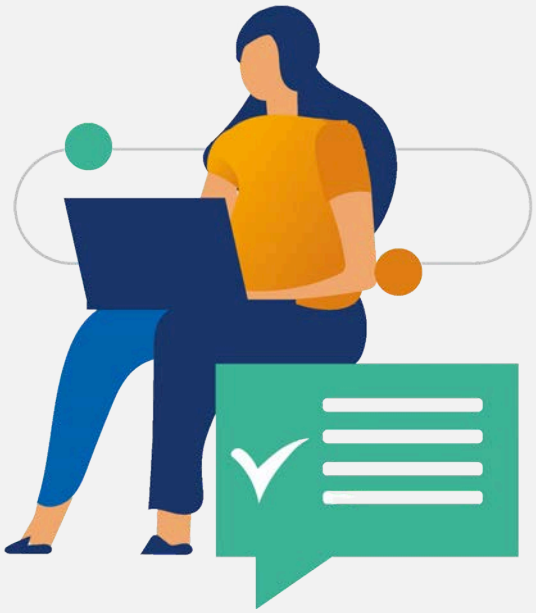
O ponto de partida é a descrição clara do arcabouço de controles já implantado. É necessário explicar quais tipos de controles estão em vigor, quais processos e controles eles alcançam e de que forma se aplicam tanto ao mercado de bolsa quanto ao mercado de balcão organizado.

Os blocos temáticos relativos a **negócios** incluem, por exemplo:

- Cadastro, KYC/KYT, PLD/FTP e identificação de beneficiário final;
- Suitability e recomendação de produtos;
- Recepção, execução e confirmação de ordens, incluindo gravação e melhores práticas de execução;
- Monitoramento de mercado e prevenção a práticas abusivas;
- Movimentação de recursos (pagamentos e recebimentos);
- Custódia, liquidação, e controle de posições;
- Operações de pessoas vinculadas e carteira própria;
- Repasse de operações;
- Atuação de assessores de investimento, operadores e terceiros relevantes;
- Certificação e capacitação de profissionais;
- Gestão de riscos; e
- Política de responsabilidade socioambiental e demais requisitos ESG.

Já os blocos temáticos relativos à **tecnologia** incluem, por exemplo:

- Segurança da informação, acesso, senhas e backups;
- Segregação lógica e acesso a dados sensíveis;
- Preservação de trilhas de auditoria;
- Programa de segurança cibernética;
- Continuidade de negócios e testes de contingência;
- Disponibilidade de sistemas críticos, inclusive de gravação de ordens; e
- Contratação de serviços relevantes prestados por terceiros.



7.2. Retrato atualizado do ambiente de controle (cont.)

Testes e eficácia dos controles

No RCI, deve ser apresentada metodologia usada para executar testes ao longo do ano. O diretor de controles internos deve explicar os critérios de materialidade, as matrizes de risco, os mecanismos de monitoramento, os parâmetros adotados para definir anomalias e as técnicas de amostragem probabilística ou direcionada.

Então, devem ser reunidos os resultados dos testes e as conclusões sobre eficiência e eficácia dos controles, tanto na primeira linha (unidades de negócio) quanto nas ações de defesa complementares.

Também é necessário apresentar a periodicidade dos testes, a competência das equipes envolvidas (inclusive quando houver terceirização) e a segregação entre quem executa e quem revisa os controles, atendendo ao princípio das três linhas de defesa.

Caso algum processo não se aplique à realidade do intermediário, a ausência deve ser justificada com fundamentação de risco.

Deficiências e não conformidades

Na sequência, o relatório deve relacionar todas as situações de não conformidades identificadas pela instituição, pelos auditores internos e externos, pela CVM, B3 ou BSM no exercício de referência. Para cada deficiência, devem constar a causa-raiz, a materialidade do risco, a ação corretiva, o responsável, o cronograma e os marcos já cumpridos.

O texto deve demonstrar a eficácia das correções implementadas e explicar eventuais atrasos, mudanças de escopo ou reincidências, indicando providências adicionais planejadas.

Devem ser explicitados os motivos que ocasionaram não cumprimento dos planos de ação estabelecidos em relatórios anteriores, tais como atraso, mudança de plano de ação ou outras situações, bem como os próximos passos definidos pelo Participante.

A exposição transparente desses pontos comprova maturidade e promove credibilidade junto aos reguladores.

7.2. Retrato atualizado do ambiente de controle (cont.)

Responsabilização dos órgãos de administração

Toda a narrativa do RCI converge para a manifestação do diretor responsável pela norma, que deve avaliar a evolução global da instituição no cumprimento das normas, comentar a adequação dos recursos humanos e tecnológicos, estimar a vulnerabilidade cibernética residual e opinar sobre a suficiência do plano de continuidade de negócios.

O órgão de administração precisa endossar o relatório de forma substancial, reafirmando compromisso com cultura de controle e com planejamento das ações contratadas.

7.3. Estrutura do RCI

Pelo exposto, uma estrutura sugerida para o RCI é apresentada a seguir.

1 **Sumário Executivo**	Principais riscos, situações críticas, planos de ação estratégicos e mensagem da administração.
Governança e Escopo 2	Identificação do diretor responsável, organograma das linhas de defesa, processos cobertos (bolsa e balcão), abrangência geográfica e normativa.
Ambiente de Controles 3	Descrição integrada dos controles implantados por macroprocesso, correlacionados aos riscos mitigados.
Metodologia de Avaliação 4	Critérios de materialidade, matriz de risco, parâmetros de monitoramento, técnicas de amostragem, frequência dos testes, responsáveis e segregação de funções.
Resultados dos Testes 5	Análise narrativa e conclusões de eficiência e eficácia por bloco temático (suitability, ordens, cadastro & PLD/FTP, riscos, custódia e liquidação, pessoas vinculadas, segregação, monitoramento de mercado, terceiros & certificações, segurança da informação & cibernética, continuidade, ESG, manutenção de arquivos).
Deficiências e Planos de Ação 6	Tabela ou narrativa contendo todas as não conformidades do período, status de planos de ação novos e antigos, eficácia das medidas, causas de atraso e próximos passos.
Parecer conclusivo 7	Elaboração do Relatório pelo Diretor de Controles Internos, Manifestação do Diretor Responsável pela RCVM 35 e Encaminhamento aos Órgãos de Administração - adequação do sistema, suficiência de recursos, avaliação do plano de continuidade e compromissos da alta direção.
Anexos Técnicos 8	Matrizes de risco–controle, evidências de testes, métricas de desempenho, glossário e referências normativas.

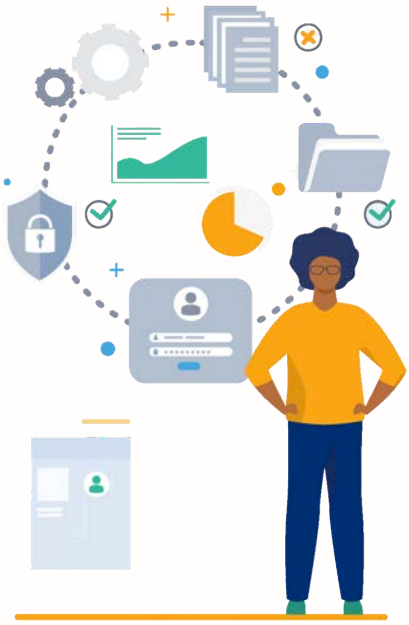
8. Considerações finais

Compromisso

A implementação de controles internos eficazes vai além do cumprimento formal de obrigações normativas. Trata-se de processo contínuo que demanda alinhamento entre os riscos assumidos pela instituição, estrutura de governança, controles projetados e resultados efetivamente alcançados.

A alta administração desempenha papel central nesse processo, sendo responsável por garantir que os controles estejam devidamente implementados, testados e documentados com base em abordagem baseada em risco e com foco em melhoria contínua. A supervisão, a responsabilização e a transparência são condições essenciais para fortalecer a cultura de integridade e de conformidade.

A elaboração do Relatório de Controles Internos deve refletir esse compromisso. Quando bem estruturado, o RCI funciona não apenas como prestação de contas regulatória, mas como instrumento de gestão que evidencia fortalezas e fragilidades do sistema, orienta decisões estratégicas e reforça credibilidade institucional junto aos reguladores e ao mercado.



Outras fontes importantes

Manual de Procedimentos Operacionais da B3

Roteiro do PQO da B3/BSM

Guia para a Elaboração do Relatório de Controles Internos (RCI)

Guia para Elaboração do Relatório de Avaliação Interna de Risco (RAIR)

Nota de Orientação BSM-17/2024 – Conteúdo e a disponibilização das Regras e Parâmetros de Atuação ou Normas e Parâmetros de Atuação

Norma de Supervisão da BSM sobre Segurança da Informação no âmbito de Segregação de Funções (BSM 03/2014)

Visite nosso site
www.bsmsupervisao.com.br

bsm
SUPERVISÃO DE MERCADOS