Guia Para a Elaboração do Relatório de Avaliação Interna de Risco (RAIR)

BSM SUPERVISÃO DE MERCADOS

Dezembro/2024

Sumário

Apresentação

A BSM Supervisão de Mercados ("BSM") no exercício de suas funções de autorregulação dos mercados organizados administrados pela B3 S.A. – Brasil, Bolsa, Balcão ("B3") divulga o presente Guia, com o objetivo de orientar os Participantes quanto à forma e ao conteúdo a serem observados na elaboração do Relatório de Avaliação Interna de Risco ("Relatório de Avaliação Interna de Risco", "RAIR", ou, simplesmente "Relatório") de Lavagem de Dinheiro e Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa ("LD/FTP"), nos termos da Resolução CVM nº 50/2021 ("RCVM 50") e do Roteiro do Programa de Qualificação Operacional ("PQO").

O presente Guia reflete exclusivamente melhores práticas e seu conteúdo, sob nenhuma hipótese, vincula discussões sobre o tema no âmbito da autorregulação da BSM.

As orientações nele contidas não devem ser interpretadas de forma a contrariar, mitigar ou se opor a nenhum normativo presente na legislação, regulação e autorregulação aplicáveis ou, ainda, às decisões do Colegiado da CVM e do Conselho de Autorregulação da BSM, servindo apenas para informar melhores práticas aos Participantes dos mercados administrados pela B3.

Desse modo, o presente Guia se apresenta como um material de auxílio e orientação ao Participante para a elaboração do RAIR e, dessa maneira, não constitui, de nenhuma forma, esgotamento das informações que devem ser apresentadas pelo Participante para atendimento da regulamentação vigente. Os exemplos presentes neste Guia são meramente ilustrativos e contêm dados fictícios, sendo elaborados para orientar a forma de apresentação das informações no RAIR, cabendo a cada Participante a definição do conteúdo do Relatório.

Os termos definidos estão de acordo com o Glossário da BSM[1] ou são definidos no presente Guia.

[1] Disponível em: https://www.bsmsupervisao.com.br/normativos-bsm.

1. Orientações quanto a forma do RAIR

1.1 Formalização do RAIR

O RAIR deve ser um documento escrito, no formato físico ou eletrônico, passível de verificação. Referido documento deve contar com a assinatura do Diretor Responsável pela RCVM 50 nomeado pelo Participante ("Diretor Responsável pela RCVM 50") e responsável por sua elaboração.

O RAIR deve ser mantido no Participante à disposição do regulador e autorregulador, não sendo, contudo, necessário seu envio, exceto quando solicitado.

O RAIR deve ser encaminhado formalmente, pelo Diretor Responsável pela RCVM 50, aos órgãos da alta administração do Participante, especificados na Política de PLD/FTP, até o último dia útil do mês de abril de cada ano.

O Diretor Responsável pela RCVM 50 deve manter o registro do encaminhamento do RAIR a todos os integrantes da alta administração. São exemplos de evidências do encaminhamento: (i) ata de reunião, com a respectiva data, que tenha como objeto a ciência do RAIR, assinada por todos os integrantes da alta administração; e (ii) e-mail de encaminhamento do RAIR a todos os integrantes da alta administração.

O Participante pode elaborar o RAIR de forma conjunta ao seu Relatório de Controles Internos (RCI), desde que o faça de forma organizada e em observância ao conteúdo estabelecido pela regulamentação vigente e às orientações específicas para o preenchimento de cada um dos relatórios, sobretudo àquelas elencadas no presente Guia e no Guia para a Elaboração do Relatório de Controles Internos ("Guia RCI").

1.2 Estrutura do RAIR

Cada Participante possui porte e modelo operacional com características e riscos específicos, que deverão ser considerados na elaboração do seu RAIR.

Por essa razão, a regulamentação em vigor não define uma estrutura fixa a ser observada pelo Participante para a elaboração do RAIR, que pode ser adaptada conforme as características e particularidades do Participante, desde que contemple o conteúdo mínimo

requerido pela RCVM 50 e pelo Roteiro do PQO, para os mercados de bolsa e balcão organizado, conforme aplicável.

Nesse sentido, é de responsabilidade do Diretor Responsável pela RCVM 50 estruturar o RAIR, visando contemplar as características e particularidades do Participante, de modo a compatibilizá-las com as exigências da regulamentação em vigor.

2. Conteúdo mínimo do RAIR

A elaboração do RAIR deve atender ao conteúdo e aspectos mínimos indicados a seguir, conforme estabelecido na RCVM 50 e no Roteiro do PQO, levando-se em consideração, no que for aplicável ao Participante, as diretrizes mencionadas neste Guia.

2.1 Descrição dos aspectos mínimos

O RAIR deve conter a descrição dos seguintes aspectos mínimos, entre outros.

2.1.1 Os produtos oferecidos, serviços prestados, respectivos canais de distribuição e ambientes de negociação e registro em que o Participante atue, segmentando-os, minimamente, em baixo, médio e alto risco de LD/FTP conforme Abordagem Baseada em Risco ("ABR") adotada pelo Participante.

Nesta avaliação, devem ser considerados todos os canais de distribuição do Participante, tais como mesa de operações, plataformas eletrônicas de negociação (ex. *Home Broker*), Assessor de Investimento, entre outros. Também devem ser considerados todos os ambientes de negociação e registro pelos quais o Participante atua, incluindo os sistemas de negociação e os sistemas de registro próprios e de terceiros utilizados pelo Participante.

a. Produtos e serviços: fatores e metodologia para apurar o risco inerente à base de produtos e serviços oferecidos pelo Participante e o resultado atribuído, que poderá ser avaliado, no mínimo, como risco baixo, médio ou alto.

Exemplo 1:

Classe	Produto / Serviço	Risco
Derivativos	Futuro de Moedas / Futuros de Ibovespa / Opção de Moedas / Opção de Ações ou Índices / Termo	Alto
Renda Variável	Ações, BDRs, ETF, Ofertas Públicas	
Balcão Organizado	Debêntures	Médio
Fundos Estruturados	Fundo de Investimento Estruturados (FIDC, FIP, FII)	
Títulos Não Financeiros	Certificado de Recebíveis do Agronegócio (CRA)	
Títulos Não Financeiros	Certificado de Recebíveis Imobiliário (CRI)	
Título Público	Letras do Tesouro Nacional (LTN)	Baixo
Título Público	Nota do Tesouro Nacional (NTN)	
Título Público	Letras Financeiras do Tesouro Nacional (LFT)	

O Participante também deverá descrever a metodologia utilizada para apuração do risco inerente aos produtos e serviços.

Exemplo 2:

• **Produtos e Serviços:** os fatores considerados para apurar o risco inerente à base de produtos e serviços foram: a quantidade de clientes operando cada produto e o volume operado por produto.

A análise de riscos identificou potenciais vulnerabilidades relacionadas a crimes financeiros, sugerindo um cenário de probabilidade moderada para eventos que possam comprometer a integridade operacional e reputacional da instituição. Os impactos contemplam dimensões financeiras, operacionais e de imagem.

Do ponto de vista financeiro, foram observadas variações nos indicadores de desempenho, que podem afetar marginalmente a estrutura de receitas da instituição. Também foi observada a possibilidade de interrupções temporárias nos fluxos de distribuição de produtos e serviços, capazes de impactar a cadeia de valor.

No âmbito reputacional, foram mapeados riscos de exposição midiática e potencial desgaste na percepção dos clientes, que podem impactar a credibilidade da instituição.

Adicionalmente, no contexto regulatório, foram mapeadas possibilidades de acionamentos formais, com eventuais aplicações de penalidades e sanções específicas na forma da legislação vigente.

Por esses fatores, o risco inerente atribuído aos produtos e serviços foi classificado como Médio.

b. Canais de distribuição: descrição da forma de relacionamento com os clientes, eventuais plataformas e canais utilizados e o resultado atribuído, que poderá ser avaliado, no mínimo, como risco baixo, médio ou alto.

Exemplo 3:

Canais de distribuição	
Baixo	Telefone, e-mail e internet, sendo distribuídos por meio de operadores celetistas devidamente certificados.
Médio	Filiais com colaboradores celetistas.
Alto	Assessores de Investimento.

O Participante também deverá descrever sua metodologia para apuração do risco inerente aos canais de distribuição.

Exemplo 4:

• **Canais de distribuição**: os canais de distribuição utilizados pela instituição incluem sistemas eletrônicos com conexão DMA, como *Home Broker*, e as Mesas de Operações. Esses canais seguem rigorosas regras de identificação prévia dos clientes e garantem a identificação das operações, abrangendo tanto o comitente quanto as características dos ativos negociados.

Os canais digitais apresentam maior risco de fraude e LD/FTP, devido à ausência de contato físico e ao acesso limitado a documentos originais. Medidas como a restrição na abertura de contas por procuradores são adotadas como forma de mitigar esses riscos.

Também devem ser considerados fatores externos como as diretrizes do GAFILAT, os resultados positivos do Brasil na avaliação do GAFI, bem como as orientações da CVM.

Mesmo com o uso crescente de meios digitais, a infraestrutura tecnológica e procedimentos robustos de Conheça Seu Cliente e antifraude atuam como mitigadores significativos desses riscos. Portanto, o risco inerente aos canais de distribuição utilizados pela instituição é considerado Médio.

c. Ambientes de negociação e registro: análise dos ambientes de negociação e registro em que o Participante atua, classificando-os, no mínimo, como risco baixo, médio ou alto.

Exemplo 5:

Ambientes de negociação e registro	
Baixo	Ativos negociados em mercado de bolsa.
Médio	Ativos negociados em mercado de balcão organizado.
Alto	Ativos negociados fora do ambiente de bolsa e em balcão organizado não liquidadas por CCP.

O Participante também deverá descrever sua metodologia para apuração do risco inerente aos ambientes de negociação e registro em que atua.

Exemplo 6:

• **Ambientes de negociação e registro:** Todas as operações realizadas por clientes da instituição ocorrem em ambientes de bolsa e balcão organizado, em que são negociados títulos, ativos financeiros e valores mobiliários.

A entrada e a saída de recursos são feitas exclusivamente por transferência eletrônica de mesma titularidade, conforme determina a regulamentação vigente. A instituição também dispõe de medidas de segurança, como duplo fator de autenticação para acesso à conta, fornecimento de informações apenas aos titulares, mediante identificação e por meio de área logada.

Desse modo, o perfil geral de risco para os ambientes de negociação e registro em que a instituição atua é considerado Médio.

2.1.2 A classificação dos clientes por grau de risco de LD/FTP, conforme ABR adotada pelo Participante, com segmentação, no mínimo, em baixo, médio e alto risco, levando em consideração, dentre outros fatores:

a. o tipo de cliente e sua natureza jurídica, sua atividade, sua localização geografia, os produtos, serviços, operações e canais de distribuições por ele utilizados, bem como outros parâmetros de risco adotados no relacionamento com seus clientes;

b. o relacionamento com outras pessoas previstas no art. 3º da RCVM 50, considerando, inclusive, as políticas de PLD/FTP de tais pessoas; e

c. a contraparte das operações realizadas em nome do cliente, no caso de operações realizadas em ambientes de registro.

Essa classificação permite uma ABR, em que os controles e monitoramentos são proporcionais ao nível de risco apresentado pelo cliente.

Exemplo 7:

Grau de risco de LD/FTP	Quantidade de clientes pessoas físicas	% pessoas físicas	Quantidade de clientes pessoas jurídicas	% pessoas jurídicas	Total
Alto	69.300	7%	300	3%	69.600
Médio	128.700	13%	700	7%	129.400
Alto	792.000	80%	9.000	90%	801.000
Total	**990.000**	**100%**	**10.000**	**100%**	**1.000.000**

O Participante também deverá descrever sua metodologia para apuração do risco inerente aos clientes.

Exemplo 8:

• **Clientes:** Para avaliar o risco inerente à base de clientes, foram considerados os seguintes aspectos:

i. status de Pessoa Exposta Politicamente (PEP) ou relacionada,

ii. informações no momento de início do relacionamento comercial e durante o ciclo de vida do relacionamento;

iii. localização geográfica (risco de fronteira);

iv. alertas positivos provenientes de transações suspeitas;

v. reportes ao COAF;

vi. encerramento de contas por fraude;

vii. encerramento por questões de PLD; e

viii. sancionados.

Essa combinação de fatores indica uma probabilidade moderada de envolvimento dos clientes em LD/FTP.

Dessa forma, o risco inerente à base de clientes, conforme os fatores de risco observados, é classificado como Médio.

Os riscos de LD/FTP inerentes às seguintes categorias de clientes devem considerar as suas respectivas peculiaridades e características, assim como ser objeto de tratamento específico dentro da Política de PLD/FTP e do processo periódico de avaliação interna de risco do Participante:

a. PEP, bem como com seus familiares, estreitos colaboradores e pessoas jurídicas de que participem, nos termos do Anexo A da RCVM 50; e

b. organizações sem fins lucrativos, nos termos da legislação específica.

São considerados estreitos colaboradores:

a. pessoas naturais que são conhecidas por terem sociedade ou propriedade conjunta em pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, que figurem como mandatárias, ainda que por instrumento particular, ou possuam qualquer outro tipo de estreita relação de conhecimento público com PEP; e

b. pessoas naturais que têm o controle de pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de PEP.

O risco da base de clientes pode ser apurado considerando fatores identificados durante o *onboarding* e o ciclo de vida do relacionamento, tais como a localização geográfica, os alertas identificados nas rotinas de monitoramento, comunicações ao Conselho de Controle de Atividades Financeiras ("COAF"), apurações relacionadas à LD/FTP. Essa avaliação deve resultar em atribuição de risco, no mínimo, baixo, médio ou alto, contemplando medidas reforçadas para clientes classificados em categorias de maior risco.

2.1.3 A análise das situações de risco de LD/FTP identificadas na avaliação interna de risco do Participante, considerando as respectivas ameaças, vulnerabilidades e consequências, podendo se relacionar com os desafios publicados na Avaliação Nacional de Riscos (ANR)[2], emitida pelo GTANR (Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa).

Nesse ponto, o RAIR deve descrever:

a. a periodicidade na identificação e manutenção de clientes PEP;

[2] Publicado em https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes.

Exemplo 9:

- **Procedimentos na identificação e manutenção de clientes PEP e relacionados**: os solicitantes devem declarar se são Pessoas Expostas Politicamente (PEP) durante o processo de abertura de conta. Independentemente da autodeclaração, é realizada verificação do CPF do solicitante em listas públicas e privadas. Caso seja confirmado que o solicitante cliente é PEP, é verificada a existência de mídias negativas relacionadas ao solicitante. Conforme a ABR, o solicitante é automaticamente aprovado se não houver mídia negativa. Caso contrário, se houver mídia negativa relevante do ponto de vista de LD/FTP, a equipe responsável avalia e decide pela aprovação ou rejeição do PEP.

  Esse procedimento é aplicado tanto a novos clientes quanto a clientes já existentes, utilizando-se os mesmos critérios para identificação de mídias negativas.

  Diariamente, são realizadas rotinas para atualizar a base de PEP, com o objetivo de identificar clientes que se tornaram PEP após a abertura da conta.

b. a avaliação de que todos seus clientes ativos possuem atribuição do risco do cliente, classificados, no mínimo, em baixo, médio e alto; e

Exemplo 10:

Grau de risco de LD/FTP	Total
Alto	69.600
Médio	129.400
Alto	801.000
Total	**1.000.000**

c. a existência ou não de clientes constituídos sob a forma de *trust* e, caso existam clientes na referida modalidade, a descrição das diligências para identificação dos componentes do *trust* e beneficiários finais.

Exemplo 11:

> **b. Clientes constituídos sob a forma de *trust***: os clientes INR constituídos sob a forma de *trust* demandam um procedimento diferenciado de monitoramento e gestão de riscos. A sistemática de acompanhamento prevê uma metodologia de avaliação customizada, caracterizada por procedimentos de análise mais rigorosos e sistemáticos.
>
> A estratégia de governança estabelecida para essa modalidade de cliente contempla um acompanhamento detalhado, com verificações periódicas e registro pormenorizado de operações, na forma da ABR da instituição.
>
> Mensalmente, são consolidados relatórios específicos que são apresentados ao comitê especializado da instituição, permitindo uma avaliação técnica das operações e a adoção de ações estratégicas.

2.1.4 Análise da atuação dos prepostos, Assessores de Investimento e prestadores de serviços relevantes contratados, bem como a descrição da governança e dos deveres associados à manutenção do cadastro simplificado de INR, nos termos do Anexo C da RCVM 50, quando aplicável.

São considerados serviços relevantes:

a. recepção e execução de ordens, com o objetivo de preservar o atendimento aos clientes;

b. liquidação junto às entidades administradoras de mercados organizados;

c. liquidação de seus clientes;

d. conciliação e atualização das posições de seus clientes; e

e. demais processos classificados como críticos pelo Participante em seu processo de análise e impacto de negócios.

Nesse ponto, o RAIR deve abordar as diretrizes elaboradas e seguidas em relação à atuação de prepostos, Assessores de Investimento, prestadores de serviços relevantes contratados e INR, fundamentadas nas políticas do Participante, com tabulação de matriz contendo o nível de risco atribuído.

Os critérios utilizados para definição de risco dos parceiros também devem estar descritos no RAIR, de modo que, após a aplicação da metodologia, todos os parceiros sejam classificados de acordo com o seu grau de risco.

Caso o Participante não possua vínculo com Assessores de Investimento, prestadores de serviços relevantes contratados ou INR, essa informação deve ser mencionada no RAIR.

Exemplo 12:

Nível de risco	Quantidade	Percentual
Alto	100	10%
Médio	700	70%
Baixo	200	20%
Total	**1.000**	**100%**

A matriz de risco de parceiros, empregada para a classificação em diferentes categorias de risco, leva em conta os seguintes critérios:

Tipo de serviço prestado ou produto oferecido			
Classe	**Fatores avaliados**	**Score**	**Atribuição de risco**
Categorias e subcategorias de serviços	Riscos de LD/FTP, reputacionais, regulatórios e de corrupção associados ao serviço prestado ou produto oferecido.	300	Alto
		200	Médio
		100	Baixo

Dados reputacionais				
Classe	**Fatores avaliados**	**Objeto de análise**	**Score**	**Atribuição de risco**
Listas Restritivas Internacionais	Proibido o relacionamento com pessoas naturais e jurídicas listadas em listas de sanções	OFAC, CSNU, UE, outras	700	Vetado
Listas Restritivas Nacionais/Sanções Nacionais/Mídias Negativas	Necessária validação quanto ao risco da restrição com o país demandante do *Screening*, para impedimentos e riscos	Qualquer resultado	300	Alto
PEP	Alto risco reputacional e regulatório, devido à maior exposição a crimes como corrupção, lavagem de dinheiro, financiamento do terrorismo e de proliferação de armas de destruição em massa e outras atividades financeiras ilícitas.	Qualquer resultado	200	Médio
Complexidade da Cadeia Societária	Complexidade na identificação do Beneficiário Final.	Estrutura societária	100	Baixo

Depois de aplicar a metodologia mencionada, todos os parceiros podem ser classificados com base na pontuação total obtida:

Score	Classificação de Risco	Resultado
110 a 130	Baixo	Aprovação e monitoramento
100 a 300	Médio	Aprovação e monitoramento, por meio de equipe especializada
301 a 699	Alto	Seguir a recomendação da equipe especializado
Acima de 700	Veto	Reprovar e reportar à equipe especializada

Também é atribuído um prazo específico para a renovação das informações, com o objetivo de reclassificar o risco associado, observando o intervalo máximo de 5 (cinco) anos, contados a partir da data do cadastro inicial ou da última atualização cadastral realizada:

Risco	Prazo
Baixo	60 meses
Médio	24 meses
Alto	12 meses

2.1.5 Informações de Monitoramento, Seleção, Análise e Comunicação de Operações e Situações Suspeitas.

O RAIR deve apresentar tabela relativa ao ano anterior, contendo:

a. o número consolidado das operações e situações atípicas detectadas, segregadas por hipótese;

b. o número de análises realizadas;

c. o número de comunicações de operações suspeitas reportadas para o COAF; e

d. a data do reporte da declaração negativa, se for o caso.

Referida Tabela deve apresentar todas as hipóteses aplicáveis descritas nos incisos e alíneas do art. 20 da RCVM 50 e seus respectivos números consolidados.

Exemplo 13:

Hipóteses (Art. 20, RCVM 50)	Situações Atípicas (Art. 6º, III, a, RCVM 50)	Quantidade de análises (Art. 6º, III, b, RCVM 50)	Comunicações (Art. 6º, III, c, RCVM 50)	Declaração negativa (Art. 6º, III, d, RCVM 50)
Situação prevista no inciso I, alínea 'a)'	132	132	112	DD/MM/AAAA
Situação prevista no inciso II, alínea 'c)'	240	240		
Situação prevista no inciso III, alínea 'b)'	128	128		
Situação prevista no inciso IV, alínea 'd)'	74	74		
Outras hipóteses acompanhadas de breve descrição da possível irregularidade (Inciso V)	13	13		
Total	**587**	**587**	**112**	

O Participante poderá também descrever incrementos e melhorias em sua rotina de monitoramento.

Exemplo 14:

O aumento observado nos indicadores reflete uma série de iniciativas implementadas pela instituição para melhorar os processos internos de monitoramento e identificação de operações e situações suspeitas. As revisões contínuas dos cenários de monitoramento, realizadas em parceria com a equipe de Governança de PLD/FTP, resultaram aprimoramento significativo da metodologia de ABR.

Esses aprimoramentos proporcionaram maior dinamismo e precisão nos procedimentos de Monitoramento, Seleção, Análise e Comunicação. Como consequência direta, foi observado uma maior acurácia na detecção e reporte operações suspeitas, elevando os patamares de segurança e conformidade regulatória.

2.1.6 Medidas adotadas para continuamente conhecer os clientes ativos, incluindo procedimentos de verificação, coleta, validação e atualização de informações cadastrais; funcionários e prestadores de serviços relevantes; bem como de identificação do beneficiário final.

O Participante deverá descrever a metodologia adotada em suas políticas internas para o tratamento e mitigação dos riscos identificados, a qual deve amparar os parâmetros estabelecidos na avaliação interna de risco, para continuamente conhecer:

a. os clientes, incluindo procedimentos de verificação, coleta, validação e atualização de informações cadastrais, bem como demais diligências aplicáveis; e

b. os funcionários e prestadores de serviços relevantes;

Exemplo 15:

• **Metodologia para Tratamento e Mitigação dos Riscos Identificados:** a instituição desenvolve uma metodologia abrangente para tratamento e mitigação de riscos, fundamentada em leis e normativos, definindo procedimentos internos rigorosos para análise de operações suspeitas e identificação de potenciais riscos legais, operacionais e reputacionais.

Na política de Política de PLD/FTP são estabelecidas diretrizes específicas que contemplam atualização periódica de cadastros, reclassificação de riscos de clientes, parceiros, prestadores de serviços e funcionários. A instituição realiza monitoramento contínuo em diversas listas de sanções, acompanha atividades financeiras, promove treinamentos internos e monitora possíveis conflitos de interesse. Existe foco especial em mecanismos de denúncia relacionados a qualquer envolvimento em atividades ilícitas.

No modelo de gestão de riscos, a primeira e segunda linhas de defesa possuem capacidade de identificar riscos e definir planos de ação para mitigá-los. Todas as vulnerabilidades são registradas em uma ferramenta interna e acompanhadas por comitês específicos. A depender da criticidade, os planos de ação possuem prazos menores ou maiores. Periodicamente, o status de cada plano de ação é reportado à gestão.

2.1.7 A apresentação, se for o caso, de recomendações visando mitigar os riscos identificados no exercício anterior que ainda não foram devidamente tratados, contendo:

a. possíveis alterações nas diretrizes previstas na política de PLD/FTP; e

b. aprimoramento das regras, procedimentos e controles internos referidos no art. 7º da RCVM 50, com o estabelecimento de cronograma de saneamento.

Exemplo 16:

a. alterações nas diretrizes previstas na Política de PLD/FTP

> **Mudanças nas Diretrizes da Política de PLD/FTP**: Em mm/aaaa, houve atualização da Política de PLD/FTP, que resultou mudança de diretrizes anteriormente seguidas, levando a alterações nas seções relacionadas à guarda e documentação de informações. Além disso, foi incorporado um dispositivo relacionado à identificação de beneficiários finais.

b. aprimoramento das regras, procedimentos e controles internos referidos no art. 7º da RCVM 50, com o estabelecimento de cronogramas de saneamento

Exemplo 17:

Processo avaliado	Descrição do teste	Risco	Plano de Ação	Área responsável	Prazo
Conheça seu cliente	Apuração de efetividade da captura e atualização dos dados cadastrais exigidos pela CVM Resolução nº 50	Alto	Descrição do plano de ação elaborado para mitigar o risco	Área e profissional responsável por sua implementação	Cumprimento da primeira etapa em dd/mm/aaaa e segunda etapa implementada em dd/mm/aaaa
Monitoramento, Seleção, Análise e Comunicação	Avaliação da matriz de alçadas internas, alinhada à ABR para o processo de Monitoramento Seleção Análise e Comunicação	Alto	Descrição do plano de ação elaborado para mitigar o risco	Área e profissional responsável por sua implementação	Implementação em dd/mm/aaaa
Infraestrutura	Melhorias em sistemas para guarda e backup de documentos exigidos pela regulação	Alto	Descrição do plano de ação elaborado para mitigar o risco	Área e profissional responsável por sua implementação	Implementação em dd/mm/aaaa

2.1.8 Indicação da efetividade das recomendações adotadas em relação ao relatório respectivamente anterior, de acordo com a metodologia de que trata o inciso II do art. 4º da RCVM 50, registrando de forma individualizada os resultados.

Exemplo 18:

Tema	Resultados identificados no ano anterior	Recomendação	Plano de Ação	Responsável	Prazo	Situação	Efetividade
Conheça seu cliente	Descrição sobre os resultados apurados no Relatório do ano anterior	Objetivo da alteração de procedimento e recomendação indicado	O que foi implementado, com indicação se parcial ou total	Área e profissional responsável	DD/MM/AAAA	Concluído	Efetivo
Conheça seu empregado	Descrição sobre os resultados apurados no Relatório do ano anterior	Objetivo da alteração de procedimento e recomendação indicado	O que foi implementado, com indicação se parcial ou total	Área e profissional responsável	DD/MM/AAAA	Concluído	Efetivo
Conheça seu Parceiro	Descrição sobre os resultados apurados no Relatório do ano anterior	Objetivo da alteração de procedimento e recomendação indicado	O que foi implementado, com indicação se parcial ou total	Área e profissional responsável	DD/MM/AAAA	Concluído	Efetivo

O Participante também deverá descrever os resultados dos planos de ação indicados:

Exemplo 19:

- **Resultados dos planos de ação:** conforme a avaliação realizada, foi constatado que todos os planos de ação concluídos em 2024, relativos ao relatório anterior, produziram todos os resultados esperados.

2.1.9 Em caso de uso de sistemas alternativos de cadastro, o RAIR deve conter a avaliação do sistema utilizado pelo Participante demonstrando sua adequação à norma, nível de confiabilidade na forma da metodologia elaborada e descrita em suas políticas, assim como o indicador de efetividade para o processo de identificação dos clientes (biometria, *bureaus*, coleta de imagens etc.).

No caso de utilização de *bureaus*, o Participante deve adotar diligências para validar as informações apresentadas pelos meios alternativos utilizados e incluir no RAIR o resultado da análise, completude e cruzamento das informações, mantendo, obrigatoriamente, a consulta e avaliação de todas as pessoas que constam nas bases públicas oficiais, tais como a Lista de PEP da CGU.

Exemplo 20:

a. **Descritivo do processo avaliado:** descrição do processo para apurar o nível de confiabilidade do sistema alternativo, na forma e parâmetros descritos nas políticas do Participante.
b. **Execução do teste:** descrição do teste executado para validação do processo cadastral e quais informações são avaliadas.
c. **Vulnerabilidade identificada:** descrição dos problemas que foram eventualmente detectados e o risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.
d. **Resultado:** conclusões extraídas dos testes aplicados e eventual detalhamento das divergências ou inconformidades, com informação estatística quanto à relevância e eventuais razões para divergências e inconformidades.

2.1.10 Em caso de uso de *bureaus*, o RAIR deve conter o teste de efetividade do sistema, armazenando as trilhas de auditoria com as validações que foram realizadas pelos *bureaus,* demonstrando, no mínimo, os dados que foram validados e o motivo da aprovação ou rejeição da informação no cadastro, além da data em que a validação foi realizada.

Exemplo 21:

a. **Descritivo do processo avaliado**: descrição do período em que a instituição utiliza esse processo, a forma as informações são disponibilizadas, armazenadas e atualizadas.

b. **Execução do teste**: descrição do teste executado para validação do processo cadastral e quais informações são avaliadas.

c. **Vulnerabilidade identificada**: descrição dos problemas que foram eventualmente detectados e qual o risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.

d. **Resultado**: conclusões extraídas dos testes dos processos aplicados e eventual detalhamento das divergências ou inconformidades, com informação estatística quanto à relevância e eventuais razões para divergências ou inconformidades.

f. Descrição sobre o armazenamento das trilhas utilizadas.

g. Data em que a validação foi realizada.

2.2 Indicadores Estatísticos de Monitoramento de Operações e Ofertas

O RAIR deve incluir e detalhar indicadores estatísticos que demonstrem a avaliação do Participante de que:

i. as análises dos alertas gerados no ano de referência foram realizadas no prazo estabelecido; e

ii. a comunicação ao COAF das situações atípicas do ano de referência ocorreu em até 24 (vinte e quatro) horas da identificação da atipicidade, caso seja aplicável.

O detalhamento dos indicadores pode ser demonstrado por meio de um índice de precisão dos alertas. Esse índice contribuirá para a avaliação da qualidade e eficácia das regras de monitoramento, por meio da proporção de alertas que resultaram reportes ao COAF, com abertura de números tabulados. É recomendável, ainda, que o Relatório traga o detalhe estatístico, mensal, dessa proporção de comunicações, análises e alertas.

Exemplo 22:

Referência	Número de alertas	Tempestividade do tratamento	Casos comunicados ao COAF	% casos tratados
Jan/AAAA	1.102	100%	62	100%
Fev/AAAA	932	99%	57	100%
Mar/AAAA	1.067	100%	60	100%
Abr/AAAA	1.234	98%	42	100%
Mai/AAAA	1.368	99%	68	100%
Jun/AAA	1.127	97%	51	100%
Jul/AAA	1.492	96%	74	100%
Ago/AAAA	1.573	99%	62	100%
Set/AAAA	1.649	98%	73	100%
Out/AAAA	1.782	96%	58	100%
Nov/AAAA	1.526	97%	46	100%
Dez/AAAA	1.409	97%	46	100%
Consolidado AAAA				
AAAA	15.904	98% dos casos tratados de forma tempestiva	721 comunicações ao COAF	100%

Exemplo 23:

a. **Processo:** diariamente é executado processo de monitoramento, seleção, análise e comunicação para fins de PLD/FTP. A instituição utiliza plataforma tecnológica especializada, que mapeia as operações dos clientes, identificando padrões atípicos, mediante algoritmos e códigos desenvolvidos pela equipe técnica.

   A seleção ocorre a partir da data da operação ou situação detectada, priorizando operações que apresentem características potencialmente fraudulentas ou suspeitas de LD/FTP.

   Durante a análise, que deve ser concluída no prazo de 45 dias, são examinadas, detalhadamente, informações sobre as transações, incluindo origem, destino, valor e contexto, para confirmar ou descartar a suspeita de LD/FTP. Caso sejam encontradas evidências suficientes, a comunicação ao COAF é feita em até 24 horas.

   Em cada área de atuação são conduzidos monitoramentos utilizando métricas relacionadas ao volume de alertas de operações selecionadas. Além disso, é realizado um acompanhamento diário da capacidade operacional dos analistas e uma avaliação da qualidade das análises operacionais por meio de controle de qualidade.

b. **Teste executado:** descrição do teste executado para verificação de efetividade dos alertas e das situações que geraram comunicações ao COAF.

c. **Vulnerabilidade identificada:** descrição dos problemas que foram detectados.

d. **Risco:** indicação do risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.

e. **Resultado:** conclusões extraídas por meio de indicadores de efetividade.

2.3 Indicadores de efetividade

Os indicadores de efetividade destinam a avaliar a eficácia das políticas, regras, controles e procedimentos internos do Participante e a sua capacidade de mitigar riscos de LD/FTP, de acordo com o seu modelo de negócio.

Desse modo, a avaliação de efetividade é o momento de o Participante avaliar onde falhou, onde não conseguiu mitigar adequadamente seus riscos e onde os processos não estão se mostrando efetivos, bem como de buscar correções e aprimoramentos por meio de planos de ação. É esperado que a alta administração tenha comprometimento com os resultados dessa avaliação e com o acompanhamento de eventuais planos de ação estabelecidos.

O Participante que utilize a mesma ABR para conglomerado financeiro, ou a ABR de terceiros, deverá descrever a metodologia utilizada, de modo que a ABR utilizada seja coerente aos processos e controles internos do Participante para assegurar o total cumprimento das obrigações regulatórias, refletindo também esse aspecto nos indicadores de efetividade.

Os indicadores de efetividade, nos termos definidos na Política de PLD/FTP do Participante, devem ser apresentados no RAIR de modo a contemplar as métricas e os critérios adotados para a análise de efetividade, incluindo a tempestividade das atividades de detecção, análise e comunicação de operações ou situações atípicas.

É recomendado que os resultados dos indicadores devem sejam apresentados com valores estatísticos, conjuntamente com uma conclusão quanto à efetividade, na forma da metodologia definida pelo Participante em sua Política de PLD/FTP.

Exemplo 24:

> Testes que resultem em efetividade superior a 50% podem ser considerados efetivos pelo Participante, ao passo que os testes que resultem em efetividade menor que 50% sejam classificados como inefetivos.
> Resultados ≥ 50%: **Processo Efetivo**.
> Resultados < 50%: **Processo inefetivo**.

Os exemplos descritos no presente Guia possuem caráter meramente ilustrativo, visando auxiliar o Participante em seu processo de Avaliação Interna de Risco, e desse modo não representa, de nenhuma forma, esgotamento das hipóteses de testes de efetividade, que devem ser realizados de forma criteriosa pelo Participante para cumprimento das diretrizes e sua Política de PLD/FTP a atendimento dos deveres da RCVM 50.

2.3.1 Avaliação da classificação de risco da base de clientes.

Descrição do teste realizado para avaliar o risco da integridade da base de clientes do Participante e seus respectivos resultados.

A integridade corresponde à preservação da precisão, consistência e confiabilidade das informações e sistemas, tanto no *onboarding* quanto ao longo do ciclo de vida do relacionamento com o cliente.

O teste deve, no mínimo, indicar se:

i. os clientes possuem uma classificação de risco; e

ii. essa classificação de risco foi atribuída de acordo com a metodologia de ABR do Participante.

Exemplo 25:

Clientes ativos	Clientes alto risco	Clientes médio risco	Clientes Baixo Risco	Clientes PEP	Clientes sem classificação de risco
10.000	50	2.300	7.623	27	0
%	0,5%	23%	76,2%	0,2%	0%

2.3.2 Avaliação dos indicadores de efetividade sobre atualização de cadastro de clientes inativos ou baixados na base do Participante e ativos na entidade administradora de mercado organizado em razão de posições na depositária.

O Participante deve detalhar a descrição do teste, avaliação e resultado para identificar a integridade da conciliação da base de dados cadastrais, em conformidade com os sistemas da B3, listando e apontando eventuais divergências e as respectivas justificativas.

O teste deve indicar se o status dos clientes (Ativo, Inativo, Suspenso, entre outros) registrado nos sistemas de cadastro da B3 está em conformidade com o sistema do Participante.

Para essa verificação, o Participante deve estar atento à definição de "Clientes Ativos" conforme descrito no art. 2º da Resolução CVM 50.

Clientes inativos no sistema do Participante devem estar cadastrados como inativos na B3, e assim por diante.

2.3.3 Avaliação dos indicadores de efetividade dos dados cadastrais de Bolsa e Balcão do mesmo cliente.

Exemplo 26:

a. **Processo:** descrever o processo cadastral e eventuais diferenças cadastrais para clientes que operam em mercado de bolsa e balcão organizado.

b. **Teste executado:** descrição do teste executado para validação dos dados cadastrais.

   O teste deve verificar se os dados cadastrais dos clientes presentes nos sistemas cadastrais de bolsa e de balcão organizado são iguais. Exceções são identificadas quando um mesmo cliente (CPF/CNPJ) possui dados cadastrais divergentes em ambos os sistemas.

   O teste é aplicável aos Participantes que atuam nos mercados de bolsa e de balcão organizado.

c. **Vulnerabilidade identificada:** quais problemas foram detectados.

d. **Risco:** qual risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.

e. **Resultados:** conclusões extraídas através de indicadores de efetividade.

Exemplo 27:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Dados cadastrais de Bolsa e Balcão do mesmo cliente	Descrição dos testes, metodologia, amostra selecionada	Descrição sobre o resultado dos testes e respectiva avaliação, demonstrando se os resultados estão em conformidade com as regras e procedimentos internos do Participante	Alto	Conclusões e eventuais planos de ação estabelecidos

2.3.4 Avaliação dos indicadores de efetividade quanto às diligências para identificação de Beneficiário Final: documentos que evidenciem a diligência para *Trusts*, Investidores Não Residentes, Organizações Sem Fins lucrativos, Fundos Exclusivos, Fundos Exclusivos no Exterior e Sociedade Por Ações.

O teste deve demonstrar quais foram as diligências adotadas para identificação dos beneficiários finais de toda a base de pessoas jurídicas dos clientes e se estão de acordo com o disposto na ABR do Participante.

Exemplo 28:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Identificação do beneficiário final	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões

2.3.5 Avaliação dos indicadores de efetividade do processo de monitoramento diferenciado conforme sua Política de PLD/FTP.

Exemplo 29:

Exemplos de clientes que podem demandar monitoramento diferenciado:

- Clientes classificados como de maior risco;
- Clientes que são Organizações Não Governamentais, Pessoas Expostas Politicamente ou Investidores Não Residentes com cadastro simplificado;
- Clientes presentes em listas restritivas;
- Clientes frequentemente identificados nos monitoramentos de PLD/FTP.

Para atender a esse requisito, o Participante deve definir o que constitui um monitoramento diferenciado em sua ABR e testar a efetividade desse monitoramento.

Exemplo 30:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Monitoramento diferenciado de clientes	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões

2.3.6 Avaliação dos indicadores de efetividade acerca da utilização de listas restritivas pelo Participante, em especial das listas do Conselho de Segurança das Nações Unidas ("CSNU") e do GAFI.

Nesse quesito, o Participante necessita se atentar para o cumprimento das obrigações relativas listas restritivas. Ao se tratar da lista do CSNU, é de cumprimento obrigatório o

bloqueio e indisponibilidade de bens, direitos e valores de clientes nela identificados. As listas do GAFI em relação a jurisdições que apresentam deficiências estratégicas em seus regimes de PLD/FTP, por sua vez, demandam monitoramento diferenciado para os clientes de jurisdições nela citadas.

O Participante deve considerar também a necessidade de elaboração de metodologia documentada em sua Política de PLD/FTP, para descrever a frequência no monitoramento sobre as listas restritivas, que devem ser consultadas de forma recorrente pelo Participante.

Destaca-se que o cumprimento dessa obrigação não deve ser submetido aos parâmetros de ABR.

Exemplo 31:

a. **Processo:** descrição do processo de verificação e diligências adotadas pelo Participante, bem como as listas restritivas incorporadas.
b. **Teste executado:** descrição dos testes executados para verificação da efetividade das diligências para utilização das listas restritivas.
c. **Vulnerabilidade identificada:** descrição dos problemas que foram detectados.
d. **Risco:** indicação do risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.
e. **Resultado:** conclusões extraídas por meio de indicadores de efetividade.

Exemplo 32:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Utilização de listas restritivas	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões

2.3.7 Avaliação dos indicadores de efetividade no monitoramento dos sinais de alerta previstos na RCVM 50.

Exemplo 33:

a. **Processo:** descrição do processo de monitoramento dos sinais de alerta previstos para atendimento do artigo 20 da RCVM 50.
b. **Teste executado:** descrição do teste executado para validação da efetividade do monitoramento, contemplando, no mínimo (i) adequação da calibragem dos parâmetros e das regras ao modelo operacional da instituição e (ii) verificação da suficiência de atendimento ao requisito.
c. **Vulnerabilidade identificada:** descrição dos problemas que foram detectados.
d. **Risco:** indicação do risco atribuído pela instituição, avaliado, no mínimo, em baixo, médio ou alto.
e. **Resultado:** conclusões extraídas por meio de indicadores de efetividade.

Exemplo 34:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Monitoramento dos sinais de alerta	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões

2.3.8 Avaliação dos indicadores de efetividade sobre Política de Conheça Seu Cliente, Monitoramento, Seleção de Atipicidades e Reportes Encaminhados ao COAF.

Exemplo 35:

a. **Processo:** descrição das diretrizes da Política de Conheça Seu Cliente, Monitoramento, Seleção de Atipicidades e Reportes Encaminhados ao COAF.

b. **Teste executado:** descrição do teste executado para validação da efetividade (i) dos processos estabelecidos na Política de Conheça seu Cliente, detalhando se, com base em uma amostra ou no universo completo, foram seguidos os critérios de Conheça seu Cliente para os clientes admitidos; (ii) do monitoramento, seleção de atipicidades e reportes feitos ao COAF, detalhando se o monitoramento está sendo eficaz na comunicação de situações atípicas detectadas.

É fundamental que o Participante verifique se a quantidade de alertas gerados e as análises realizadas e arquivadas estão condizentes com a realidade da instituição, ou seja, se não há um número excessivo de falsos positivos ou um número inexpressivo de análises.

c. **Vulnerabilidade identificada:** descrição dos problemas que foram detectados;

d. **Risco:** indicação do risco atribuído pela instituição, avaliado, no mínimo, em **baixo**, **médio** ou **alto**.

e. **Resultado:** conclusões extraídas por meio de indicadores de efetividade.

Exemplo 36:

Indicadores de efetividade				
Processo	**Teste executado**	**Vulnerabilidade identificada**	**Risco**	**Resultados**
Política de Conheça Seu Cliente	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões
Monitoramento	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões
Seção de Atipicidade	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões
Reportes encaminhados ao COAF	Descrição dos testes	Descrição sobre o que foi detectado	Alto	Conclusões

3. Aspectos gerais

O Participante, ao identificar a não aplicabilidade de algum item obrigatório da regulamentação vigente, não poderá apenas suprimir os tópicos e informações em seu RAIR, deverá explicar de forma detalhada e precisa a razão da inaplicabilidade.

Os testes de avaliação podem contemplar a referência a seus resultados, de forma sintética, no documento principal, sendo, contudo, recomendável a demonstração analítica anexa ao RAIR, contendo a apresentação de todas as informações.

Caso o Participante opte por referenciar outro documento que atenda aos requisitos mínimos, o RAIR deve incluir a indicação do nome do documento, versão, item e página em que a informação pode ser encontrada. Esse documento será considerado complementar ao RAIR e deve ser apresentado de forma conjunta sempre que solicitado.

O RAIR deve também indicar quais parâmetros foram utilizados para identificar, analisar, compreender e classificar os riscos. Deve também demonstrar que as amostras foram estatisticamente significativas, fazendo-se referência à descrição de metodologia e critérios para seleção de amostra e os testes aplicados, apontando o documento (nome e a versão) em que estão descritos.

Os testes de efetividade não devem se basear apenas nas diligências e procedimentos descritos pelo Participante. É necessário que os testes incluam amostras e/ou universos de análise com representatividade estatística e que comprovem a efetividade dos procedimentos e das diligências implementadas durante o período avaliado.

Todos os testes de efetividade contemplados no RAIR deverão ser armazenados pelo Participante e mantidos à disposição do regulador e autorregulador pelo prazo estabelecido na regulamentação em vigor, contendo, no mínimo:

a. procedimento realizado;
b. bases utilizadas; e
c. resultados.

Os exemplos trazidos neste Guia apresentam dados fictícios e são meramente ilustrativos, não representando, de nenhuma forma, esgotamento das informações que devem ser apresentadas pelo Participante.

A abordagem criteriosa visa não apenas o fiel cumprimento à regulação, mas principalmente o fortalecimento dos mecanismos de PLD/FTP no âmbito do mercado de capitais brasileiro.

BSM SUPERVISÃO DE MERCADOS

bsm@bsmsupervisao.com.br

bsmsupervisao.com.br