Manual de Controles Internos

Relacionado à política 1-P-000017

Taxonomia: 10. Governança corporativa e estrutura

Owner/Responsável: Diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos / Head of C&ORC Wealth Management Latin America and UBS Group Brazil

Por que temos esse documento?
Esse documento serve como material de orientação sobre algumas das funções e atividades de controles internos desempenhadas no âmbito da UBS Brasil Administradora de Valores Mobiliários Ltda., bem como para atendimento à regra prevista no Artigo 16, III, da Resolução 21, de 25 de fevereiro de 2021, da Comissão de Valores Mobiliários

Applicability / Aplicação

Roles / papéis	- Divisional and Group functional Risk Management / Gerentes de risco de divisão, e de funções do Grupo - C&ORC Controllers - Todos os integrantes de C&ORC
Business Division / Group Function / Divisão de Negócios / Função do Grupo	Wealth Management
Business Area / Área do Negócio	Todas
Legal Entity / Entidade jurídica	UBS Brasil Administradora de Valores Mobiliários Ltda.
Location / Localização	Brasil

Este manual é sujeito à aprovação do Conselho de Administração da UBS Administradora com manifestação prévia do Brazilian Risk Control Committee (BRCC), e deverá ser revisado anualmente ou a qualquer momento quando necessário.

Sumário

1. Resumo

Este documento indica os controles internos adotados, para o cumprimento da Resolução 21, de 25 de fevereiro de 2021, da Comissão de Valores Mobiliários (Res. 21, de 2021), e do Código de Administração de Recurso de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), pela UBS Brasil Administradora de Valores Mobiliários Ltda. (UBS Administradora), pessoa jurídica responsável no Brasil pela área de Wealth Managament (gestão de patrimônio) do UBS.

Este documento faz menção a regras e procedimentos aplicáveis à UBS Administradora independentemente se foram editados por ela ou se pelo Grupo UBS, o qual ela integra.

2. Escopo

O sistema de controles internos aplicável à UBS Administradora consiste em diversas estruturas políticas, e guias (conjuntamente chamados de "políticas") que são continuamente atualizados pelos seus owners e acompanhados pela área de governança da UBS Administradora e/ou do Grupo UBS. Todas essas políticas passam por revisões periódicas, quando podem ser implementadas modificações e/ou melhorias.

Esta Manual não se propõe a expor de forma exauriente regras e procedimentos da UBS Administradora e/ou do Grupo UBS. Ao contrário, visa compilar algumas das principais políticas, fazendo a elas referências, mas sem trazê-las na íntegra. O conteúdo completo das políticas pode ser encontrado na intranet no endereço goto/polo e, no caso de políticas específicas da UBS Administradora, em goto/brasil.

O mesmo vale para os controles internos executados com periodicidade mínima anual pela UBS Administradora. Ao final deste manual são expostos os códigos, nomes e descrição dos controles considerados por Compliance & Operational Risk Controls (C&ORC, ou em tradução livre, Controles de Compliance & Risco Operacional) como regulatórios à luz da Res. 21, de 2021. Assim, é importante notar que outros controles são regularmente executados pela UBS Administradora, ou por outras entidades do Grupo UBS mas com escopo na UBS Administradora. Ressalta-se, como será explicado adiante, que todos os controles mencionados neste manual são classificados internamente KPC (Key Procedural Control, ou

Controles-chave de processos, em tradução livre) ou PC (Procedural Control, ou Processo de Controle, em tradução livre).

3. Modelo das três linhas de defesa

3.1. Primeira linha de defesa (First line of defense – 1st LOD)

A chamada primeira linha de defesa no gerenciamento eficaz de riscos e controles abriga equipes que ajudam a proteger o Grupo UBS de forma direta. Partindo da Alta Administração, passa pelos controles da gerência e por medidas de controle interno. No que se refere aos negócios de gestão de patrimônio, são envolvidas nas atividades da primeira linha de defesa: a área de Investimentos, a área Comercial, a área de Business Risk Organization (BRO), entre outras.

A área de Investimentos tem como principais atribuições:

a. Discussões de cenários de mercado para tomadas de decisões estratégicas e táticas de investimentos;

b. Avaliação de ativos para inclusão em universo monitorado;

c. Avaliação, diligência e aprovação de ativos a serem investidos e o devido monitoramento;

d. Implementação das decisões de investimentos tomadas em fóruns / comitês;

e. Reuniões com clientes para alinhamento das decisões de investimento tomadas nos portfolios;

f. Desenvolvimento de novos produtos.

A área Comercial tem como principais atribuições a atuação dos Client Advisors (CAs, ou assessores dos clientes, em tradução livre) na prospecção e atendimento aos clientes, e gestão dos portfolios. À área de BRO (Business Risk Organization), por sua vez, cabem as seguintes atividades:

a. Identificar e comunicar riscos operacionais;

b. Monitorar e controlar riscos aos quais os fundos e carteiras administradas estão expostos (Portfolio Health Checks);

c. Identificação de deficiências de controles;

d. Desenhar, implementar e executar controles e controles chaves (KPCs – "Key Procedural Controls");

e. Avaliar periodicamente os controles em relação a desenho e efetividade por meio de avaliações específicas ("KPC Assessment");

f. Implementar ações para mitigar e corrigir as deficiências identificadas;

g. Conduzir avaliação anual de adequação de apetite a risco (RCSA – "Risk Control Self-Assessment").

3.2. Segunda linha de defesa (Second line of defense – 2nd LOD)

Na segunda linha de defesa estão as funções de risco, conformidade, controle e fiscalização para auxiliar no desenvolvimento e monitoramento dos controles da primeira linha de defesa.

A gestão de riscos considera a identificação de falhas na execução de tarefas, a estimativa das perdas financeiras resultantes dessas falhas, a relevância de cada falha e de cada perda em relação ao total, a integração das mensurações de risco e a flexibilização para a alocação de capital.

No que se refere aos negócios de gestão de patrimônio (Wealth Management), em linha com os princípios de governança corporativa e as normas da Comissão de Valores Mobiliários, a UBS Administradora possui uma área dedicada à implementação e cumprimento de regras, políticas, procedimentos e controles internos (Compliance) e à gestão e monitoramento do risco operacional denominada C&ORC, com políticas claramente definidas e divulgadas a todas as entidades do Grupo UBS, apoiada em processos e ferramentas implementados de acordo com a natureza e a complexidade dos produtos, serviços e atividades ligados aos serviços de gestão de patrimônio, com os objetivos de executar cada uma das etapas relativas ao ciclo de gestão de riscos: identificação, mensuração, avaliação, monitoramento, reporte, controle e mitigação. Suas principais atribuições são:

a. Garantir que todos os riscos sejam compreendidos, atribuídos a responsáveis e geridos de acordo com o apetite ao risco da organização;

b. Revisar, questionar e monitorar, de maneira independente, a efetividade da gestão, da avaliação, da mensuração e do controle de risco e prover questionamentos independentes às atividades de negócio que assumem risco;

c. Prover uma checagem independente e objetiva para averiguar se a gestão está adequadamente gerindo riscos materiais provenientes das atividades de negócio

d. Desafiar as áreas da 1ª linha de defesa acerca de potenciais riscos operacionais e/ou deficiências em controles;

e. Verificar se os riscos operacionais existentes e/ou discutidos em outras localidades tem aplicabilidade no UBS Brasil;

f. Revisar e opinar sobre as avaliações conduzidas pela 1ª linha de defesa;

g. Revisar e avaliar a efetividade das ações implementadas pela 1ª linha de defesa para mitigar e corrigir deficiências identificadas.

Adicionalmente, como parte integrante da 2ª linha de defesa, há a área de "Risk Control" (controle de riscos, em tradução livre), coordenada pelo diretor responsável pela gestão de riscos denominado "Chief Risk Officer". Essa área coordena a execução dos planos de ação para problemas identificados e gestão dos riscos primários associados à UBS Administradora e reporta-se ao Comitê de Risco & Controle do UBS Brasil (BRCC).

Cabe também à área de Risk Control assegurar a gestão integrada de todos os riscos da UBS Administradora, proporcionalmente à natureza e complexidade de suas operações, bem como pela adequação do perfil de risco da instituição ao seu apetite e aos seus objetivos estratégicos. Para esse fim, a área de Risk Control conta com o suporte das primeiras linhas de defesa, bem como as demais áreas que compõem a da 2ª linha de defesa.

3.3. Terceira linha de defesa (Third line of defense – 3rd LOD)

A auditoria interna (Group Internal Audit – GIA) provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. A terceira linha tem como

objetivo uma avaliação independente da gestão dos riscos, controles e governança da organização. O resultado é a comunicação e efetivação das oportunidades de melhoria identificadas. GIA, regularmente, informa partes interessadas relevantes, tais como agências reguladoras, autorreguladoras, e auditorias externas, sobre como a instituição está gerenciando e mitigando seus riscos. O responsável pelo GIA globalmente está subordinado ao presidente global do Grupo UBS ("CEO Global") e ao Comitê de Auditoria global.

4. Políticas

O Grupo UBS, e consequentemente a UBS Administradora, são regidos por inúmeras políticas globais, guias e regras (coletivamente chamadas "políticas"). Em sua maioria, estão disponíveis na intranet em (goto/polo), mas há, ainda, políticas específicas, aplicáveis somente à UBS Administradora, as quais estão disponíveis na intranet em goto/brasil.

A estrutura base de controles internos, por sua vez, está disponível em goto/orf ou goto/nfrf, onde é possível verificar a estrutura de risco operacional do Grupo, bem como as principais políticas, sobre o tema de controles internos e risco operacional, que regem o Grupo e, portanto, a UBS Administradora.

O conhecimento de certas políticas deve ser afirmado, periodicamente, por cada um dos colaboradores por meio de uma declaração on-line específica de conhecimento da regra realizada em sítio próprio na intranet (goto/aol). Cada perfil de colaborador obriga o indivíduo a conhecer, e por consequência a afirmar, o conhecimento de uma série de políticas por meio do sistema Affirmation On-Line (afirmação on-line).

Para fins deste manual de controles internos, destacam-se as políticas mencionadas na Res. 21, de 2021, e algumas outras cuja existência é imposta por meio de outras regras da Comissão de Valores Mobiliários, as quais serão destacadas ao final deste capítulo. No âmbito da Res. 21, de 2021, está prevista a divulgação, na internet, do código de ética, da política de gestão de risco, política de negociação de valores mobiliários, manual de precificação dos ativos das carteiras e política de rateio e divisão de ordens aplicáveis a administradora. Essas políticas são mantidas atualizadas e disponíveis, pela UBS Administradora em https://www.ubs.com/global/pt/legal/country/brazil/ubs-administradora.html.

Além disso, a mesma resolução prevê a manutenção de manuais escritos sobre segregação de atividades e sobre confidencialidade, os quais não precisam estar disponíveis na rede mundial de computadores. Quanto às regras sobre segregação de atividades, cabe dizer que as áreas da UBS Administradora possuem níveis de barreiras de acordo com informação e acesso (de dados), são segregadas (ou não) a partir da validação do Head (chefe) da área e submetida a aprovação de C&ORC.

As empresas também possuem, como regra, equipes distintas, inclusive no que se refere às funções de suporte ao negócio. Porém, são compartilhadas com outras empresas do Grupo UBS áreas administrativas como: Tecnologia da Informação, Recursos Humanos, segurança, manutenção, contas a pagar e receber, contabilidade, comunicação, governança corporativa, entre outras atividades que zelam pelo funcionamento da estrutura funcional da UBS Administradora.

Ainda sobre o tema da segregação de atividades, cada um dos sistemas, bem como os diretórios possuem um responsável (owner) pela concessão de acesso e revisão deste. O responsável deve avaliar, de acordo com a atividade desenvolvida, se o funcionário deve ou não possuir acesso a certo sistema e a adequação de seu perfil. Ademais, os acessos possuem prazo de vencimento, no qual é revisto a necessidade de mantê-lo. Isso é regido pela política Information Barriers (ou, em tradução livre, barreiras da Informação - 1-P-004686). O Grupo UBS conta, ainda, com página específica relacionada ao tema em sua intranet (goto/ibss) e mais de quarenta testes globais previstos na política Information Barriers.

Além disso a política Information Barriers tem como objetivo prevenir a divulgação não autorizada de informações privilegiadas e o uso indevido dessas informações. Barreiras de informação internas são estabelecidas para que informações privilegiadas sejam comunicadas tão somente aos funcionários do Grupo UBS que tenham necessidade legítima de conhecer ou ter acesso a estas informações.

Quantos às regras sobre confidencialidade os documentos da UBS Administradora devem ter a correta classificação da informação, o acesso às informações deve ser baseado no princípio de "need to know" (necessidade de conhecimento, em tradução livre) e os controles definidos em políticas devem ser seguidos por toda instituição, conforme política Cyber & Information Security Policy (ou, Política de segurança cibernética e da informação, em tradução livre, 1-P-000162).

Além disso, eventual vazamento de informações deve ser reportado na intranet da empresa (goto/incident) pelo colaborador que identificou a ocorrência. O goto/incident é uma ferramenta do CISO

– Chief Information Security Officer (ou, em tradução livre, Chefe de Segurança da Informação), em que todo incidente de segurança deve ser reportado, p.ex., perda de celular, extravio de documentos, endereçamento incorreto de e-mail, vazamento de dados etc. Caso haja vazamento de dados pessoais, o DPO local será acionado. Quando se trata de incidente sem dados pessoais, todo processo é conduzido pelo CISO.

Com relação a sistemas gerenciados e mantidos pela área de TI, eles possuem gestão de controle de acesso e senhas, e o Information Owner, o dono da informação e acessos. Testes periódicos para detecção de vulnerabilidades são aplicados de acordo com o Application Security Framework (ASF, ou Estrutura de Segurança de Aplicativos, em tradução livre, disponível em goto/asf), que é baseado nas seguintes políticas e padrões: a) Application and Infrastructure Security Vulnerability Management Guidance (Guia de gerenciamento de vulnerabilidades para aplicativos e infraestrutura - 9-G-004387), e b) Cyber & Information Security (CIS) Technical and Specialist Requirements (Requisitos técnicos e de especialista de Segurança cibernética e da informação - 1-P-002103).

Incidentes relacionados a dados pessoais que tenham sido reportados pelas áreas que os geraram e analisados em relação à sua relevância ou necessidade de ação adicional (tal como, reporte aos envolvidos ou autoridades) são reportados pelo DPO local ao Brazil Risk Control Committee (BRCC, ou, em tradução livre, Comitê de Controles de Riscos do Brasil) semestralmente na apresentação do relatório de Proteção de Dados.

O Grupo UBS possui um processo de reporte de incidentes em sua intranet (goto/incident). Este processo é divulgado em treinamento mandatório específico sobre Privacidade e Proteção de Dados, no treinamento de Segurança da Informação, em treinamentos no "Dia de Boas-vindas" do RH, entre outros, incluindo treinamentos conduzidos pelo DPO para as áreas de negócio e de suporte. Esse processo contempla a análise de diversos fatores para a determinação do nível de risco e relevância do incidente, de maneira a determinar a necessidade ou não de reporte, tanto para as autoridades competentes, como para as partes afetadas e possíveis ações corretivas.

Os critérios avaliados em cada incidente para determinação do risco são: o número de indivíduos afetados, existência de dados sensíveis, tipo de dados pessoais, possibilidade de identificação dos indivíduos, quem é o recebedor da informação, ações de remediação adotadas, causa do incidente, criticidade do incidente (em casos em que a disponibilidade é afetada) e potencial de danos em função

do dado vazado. O conjunto dessas informações é avaliado e o risco e ações necessárias determinado pelas áreas do DPO, segurança da informação e jurídico.

Como apontado acima, no entanto, existem outras regras da CVM, além da Res. 21, de 2021, que impõem a criação e cumprimento de políticas. A fim de catalogá-las e mantê-las atualizadas, WM C&ORC executa o teste chamado Key Documents, ou documentos-chave, por meio do qual são coletadas e avaliadas as exigências regulatórias e é verificado se tais políticas devem ser divulgadas ao público externo e se estavam atualizadas. Anualmente, a lista de políticas-chave pode ser atualizada, por isso recomenda-se que C&ORC seja consultado a fim de verificar quais políticas são consideradas chave.

Ao tempo da publicação deste Manual, vinte e uma políticas do Grupo UBS ou da UBS Administradora faziam parte da lista de documentos-chave. Sua existência, e consequente cumprimento, é imposta pela CVM e/ou pela ANBIMA. São eles: Business Continuity & Resilience Framework (ou, em tradução livre, Estrutura de Continuidade dos Negócios e Resiliência - 1-P-00057); Código de Conduta e Ética nas Atividades de Wealth Management Brasil – UBS WM Brasil; Cyber & Information Security (ou, em tradução livre, Segurança da Informação e Cibernética - 1-P-00162); Group Data Protection Policy (ou, em tradução livre, Política de proteção de dados do Grupo - 1-P-001061); Information Barriers Policy (ou, em tradução livre, Política de Barreiras da Informação - 1-P-004686); Manual de Procedimentos de controles Internos; Política de Compra e Venda de Valores Mobiliários; Politica de exercício de direito de voto; Política de Gestão de Riscos das Carteiras e Fundos de Investimento geridos pelo UBS WM Brasil; Política de Gestão de Riscos das Carteiras e Fundos de Investimento geridos pelo UBS WM Brasil; Política rateio e divisão UBS Consenso; Política de gestão de liquidez; Procedimento de Certificação Profissional; Relatório de Adequação dos Investimentos ao Perfil do Investidor; Third Party Funds Selection and Portifolio Management Operational Manual Policy (ou, em tradução livre, Manual Operacional de Seleção de Fundos de Terceiros e de gerenciamento de carteira); UBS Brasil Contratação de Fornecedores; UBS Brazil WM: Anti-Money Laundering and Sanctions Policy (Política de prevenção à lavagem de dinheiro); UBS Brazil: WM Know Your Client Procedure (Procedimento de conheça seu cliente); UBS Consenso - Manual de Renda Fixa; Wealth Management Brasil Manual de Precificação de Ativos; WM Brasil: Procedimento de Suitability.

É importante notar, quanto às políticas, que não estão incluídas no controle de Key Documents políticas referentes a crimes financeiros e prevenção à lavagem de dinheiro. De acordo com a governança

da UBS Administradora e do Grupo UBS no Brasil, a análise da regulação aplicável a esse tema é feita por meio de outros controles e/ou exercícios, os quais não são descritos neste Manual, mas em documentos próprios da área de Financial Crimes.

5. Treinamentos

Anualmente, o Grupo UBS realiza o planejamento de treinamentos, os quais serão disponibilizados na ferramenta UBS University (universidade), um sistema automatizado que controla os prazos para que os colaboradores completem os treinamentos e que exige nota mínima para aprovação em testes de conhecimento. Os colaboradores devem passar por esses treinamentos de tempos em tempos, mas, no mínimo, anualmente. Sempre que se aproxima a data de vencimento de um ou mais treinamentos, o sistema automaticamente envia e-mails aos colaboradores lembrando-os de realizarem os treinamentos.

Eventuais incidentes relacionados a, ou descumprimentos de, quaisquer políticas do Grupo UBS pelos administradores, empregados e colaboradores são verificados e endereçados de acordo com a Employee Incidents Policy (em tradução livre, política de incidentes relacionados a colaboradores – 1-P-004710). Essa política foi criada para estabelecer princípios e regras na apuração de casos de descumprimentos das políticas do Grupo UBS. Inclui, portanto, a UBS Administradora.

Essa gradação de sanções ou consequências e os passos a serem tomados em cada caso também está prevista na Política de incidentes relacionados a colaboradores (Employee Incidents Policy - 1-P-004710). De maneira resumida, são chamadas de Employee Incident (EI, ou incidente com colaborador, em tradução livre), violações confirmadas de políticas. Cada EI é avaliado pelo dono (owner) da política. Para a avaliação são levados em conta a) o nível de risco que a violação gera; e b) o comportamento do colaborador do Grupo UBS. Existem três classificações possíveis para as violações: Um lembrete – que isoladamente, não afeta a avaliação de fim de ano do colaborador (deve ser aplicado sob o espírito de lições aprendidas e para a continuidade do aperfeiçoamento, como previsto na política); ECI – o qual pode ser levado em consideração, pelo chefe imediato (line manager) na avaliação de fim de ano do colaborador; e Encaminhamento ao departamento de recursos humanos (RH), em que o colaborador passará por revisão disciplinar e poderá ser submetido à sanção disciplinar.

No que diz à necessidade de inserção de novos treinamentos na ferramenta, sejam eles obrigatórios ou não, qualquer área pode requerer a inclusão por meio da intranet em goto/mandatorylearning.

Cabe notar a personalização da ferramenta de acordo com o perfil do integrante da UBS Administradora. Cada perfil de colaborador, de acordo com sua função, deve completar uma lista específica de treinamentos, cuja realização é monitorada por meio de controles executados pela área de Compliance

Além disso, é possível que treinamentos sejam estruturados e ministrados para atender necessidades específicas de certas áreas dentro do Grupo UBS e da UBS Administradora. Esses treinamentos podem ser realizados fora das ferramentas acima mencionadas de forma presencial ou por meio de vídeo conferência.

6. Regulatory Reporting Framework (RRF) (Estrutura de reportes regulatórios)

A Regulatory Reporting Framework (RRF) (ou, em tradução livre, Estrutura de reportes regulatórios - 1-P-002980) estabelece a estrutura para os princípios de governança e requisitos mínimos obrigatórios aplicáveis à empresa no que diz respeito aos relatórios produzidos e submetidos aos reguladores do UBS. A RRF não identifica novas exigências ou regras regulatórias nem as respectivas alterações, mas impõe às Divisões de Negócios / Funções do Grupo:

- Detalhar a existência relatórios obrigatórios devidos aos reguladores do UBS e definir e atribuir propriedade e responsabilidade pelos processos contínuos de produção e governança; inclusive garantindo a transparência prevista para todas as funções e Entidades do UBS (UBS Entitites) impactadas como objeto / beneficiária dos relatórios;
- Implementar padrões mínimos prescritos pela RRF e controle(s) baseado em risco e criar/manter documentação de procedimento operacional para sustentar os processos de produção e governança de relatórios;

- Avaliar, detectar, gerenciar e prevenir exposições potenciais a riscos que impactam a Taxonomia de Risco Operacional 12.3 - Relatórios Regulatórios.

A produção de relatórios completos, precisos e dentro do prazo para um regulador do UBS é uma responsabilidade da Divisão de Negócios / Função do Grupo. A RRF foi criada para facilitar e fornecer transparência para definir a responsabilidade e a prestação de contas da produção de relatórios, bem como para garantir processos mínimos de controle e governança.

Para assegurar a efetividade desses processos e governança o Grupo UBS disponibiliza informações catalogadas sobre a RRF em goto/rrf, e para a elaboração de relatórios com os requisitos mínimos necessários para atendimento à governança do Grupo, na RRF, há, ainda, o RPM Process Manual Best Practice Guidelines (ou, em tradução livre, Guia de Melhores Práticas do Gerenciamento de Processos Regulatórios), a qual visa verificar se:

- os requisitos regulatórios foram plenamente compreendidos;
- os processos de produção e apresentação de relatórios regulamentares estão suficientemente organizados, especificando-se todas as etapas de produção necessárias;
- as responsabilidades são claramente atribuídas e a documentação existe para facilitar as transições e reduzir as dependências das pessoas-chave;
- controles eficazes estão vigor.

7. Obrigações destacadas da Res. 21, de 2021.

Além das obrigações previstas nas normas internas do Grupo UBS e da UBS Administradora, este manual visa sintetizar, neste capítulo obrigações oriundas da Res. 21, de 2021. Deve-se notar, no entanto, que não são previstas aqui obrigações regulatórias previstas nas referida Resolução. Tampouco, constam neste Manual as obrigações relacionadas ao tema da prevenção de lavagem de dinheiro e financiamento ao terrorismo e que, em sua maioria, estão previstas na Resolução 50, de 31 de agosto de 2021, a qual é de observância obrigatória pela UBS Administradora.

Dentre as obrigações regulatórias da UBS Administradora quanto ao tema de controles internos, destacam-se aquelas previstas na Res. 21, de 2021, mencionadas abaixo, ressaltando-se não ser o rol abaixo taxativo.

7.1. Artigo 4º

Para a manutenção do registro de administrador de carteira de valores mobiliários, pessoa jurídica, deve atender às exigências do artigo 4º da Res. 21, de 2021.Cabe a C&ORC:

a. verificar anualmente o atendimento a tais exigências e a comunicação aos fóruns e comitês responsáveis caso detecte que não se está adimplindo com a norma.

b. preencher anualmente o formulário do Anexo E, da Res. 21, de 2021, o formulário de referência e submetê-lo via internet à CVM.

Ainda no que diz a requisitos para a manutenção do registro da pessoa jurídica, é importante notar que cabe à C&ORC a condução de diligências para verificar sobre a reputação ilibada dos diretores. Essa regra não está prevista na Res. 21, de 2021, mas no Ofício-Circular n. 2/2021/CVM/SIN, de 23 de fevereiro de 2021, o qual faz referência à Instrução CVM n. 558, revogada pela Res. n. 21, de 2021, mas ainda adotado, ao menos em caráter orientativo por C&ORC.

7.2. Artigo 5º

No caso de eventuais impedimentos de qualquer dos diretores responsáveis pela administração de carteiras de valores mobiliários por prazo superior a 30 (trinta) dias, conforme a Res. 21, de 2021, o substituto deve assumir a referida responsabilidade, e a CVM deve ser comunicada, por escrito, no prazo de 7 (sete) dias úteis a contar da sua ocorrência. Essa comunicação é de responsabilidade de C&ORC, mas a equipe da respectiva diretoria ou qualquer um dos fóruns e Comitês deve comunicar C&ORC sobre o impedimento.

7.3. Artigo 18

O administrador de carteiras de valores mobiliários deve informar à CVM sempre que verifique, no exercício das suas atribuições, a ocorrência ou indícios de violação da legislação que incumbe à CVM fiscalizar, no prazo máximo de 10 (dez) dias úteis da ocorrência ou identificação.

Uma vez verificadas eventuais ocorrências, por quaisquer meios, cabe à C&ORC comunicá-la à CVM.

7.4. Artigo 25

Cabe à C&ORC encaminhar aos órgãos de administração do administrador de carteiras de valores mobiliários, até o último dia útil do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo:

I – as conclusões dos exames efetuados;

II – as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e

III – a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

Esse relatório ficará sob a guarda de C&ORC, o qual deverá disponibilizá-lo à CVM, sempre que solicitado.

8. Avaliações realizadas

8.1. KPCi Assessment – Key Procedural Control Instance Assessment (Avaliação de Controles-chave de processos)

Conforme o Control Management Guidance (ou, em tradução livre, Guia de Gerenciamento de Controles –1-G-007621), a UBS Administradora possui os Key Procedural Controls (KPCs, ou Controles-

chave de processos, em tradução livre) e os KPCi (Key Procedural Control Instance, ou Controles-chave de processos, em tradução livre), em conjunto nomeados como "Controles-chave". Os Controles-chave contribuem substancialmente para a mitigação de riscos não financeiros, sendo definido como "chave" se for concebido para mitigar um nível de risco que, se o controle estiver ausente ou pare de funcionar inteiramente (ou seja, não existe mitigação do risco inerente), pode dar origem a um caso (issue) de risco não financeiro (NFR Issue) classificado como Gravidade 3 ou equivalente na escala de Emissão NFR, conforme o NFR Issue Guidelines (ou, em tradução livre Guia de casos de NFR – 1-G-007620). Cada KPC deve ter pelo menos um KPCi ativo.

Os Controles-chave são definidos pelos seus responsáveis (owners), os quais são os responsáveis pela efetividade do desenho do controle e pela manutenção dos elementos de dados priorizados definidos no próprio controle. Caso seja identificada uma deficiência de desenho durante as avaliações, a correção deve ser coordenada por seu responsável. Se o controle atenuante satisfizer os critérios de um KPC, deve ser registado no sistema ERMS logo que identificado.

O KPCi Assessment é uma autoavaliação da efetividade operacional e de desenho de um KPCi, com o objetivo de identificar deficiências e oportunidades de melhoria do KPCi. Quando forem identificadas as classificações "inefetivo" ou "efetivo com pequenos melhoramentos possíveis", deve-se definir planos de regresso à efetividade ("de volta ao verde"). Se o risco associado à deficiência for igual ou superior à gravidade 3 na escala de classificação de NFR Issue, um caso (issue) deve ser criado, conforme NFR Issue Guideline (ou, em tradução livre, Diretrizes de NFR Issue - 1-G-007620).

Durante o KPCi Assessment, os C&ORC Controller são responsáveis por supervisionar e questionar (challenge, no original da política) os KPCi Assessments e por participar nos fóruns de governança. Em 2022, para questionamento (challenge), ou revisão de segunda linha de defesa, C&ORC usou como base os resultados obtidos das avaliações da efetividade do desenho e da operação do controle, realizou entrevistas e avaliou as evidências fornecidas pelas áreas responsáveis, bem como eventuais apontamentos constantes em ORIs.

C&ORC selecionou uma amostra dos resultados dos KPCis considerado regulatórios em 2022; utilizando-se de critérios previstos no capítulo "Sample Size" (ou, tamanho de amostra) do Global MS&C Minimum Control Standards (ou, em tradução livre, Padrões Mínimos de Controle Globais de MS&C).

8.2. CRA – Compliance Risk Assessment (Avaliação de risco de Compliance)

Conforme CUSO - Combined US Operations Compliance Risk Management Framework (ou, em tradução livre, Estrutura de Gerenciamento de Risco de Conformidade de Operações Combinadas dos EUA – 1-E-005664), existem duas avaliações de risco principais que são integradas no Non-Financial Risk Framework (NFRF, Estrutura de Riscos Não-Financeiros – 1-P-000017): a Avaliação de Risco de Compliance (CRA, Compliance Risk Assessment) e a Autoavaliação de Controle de Risco (RCSA, Risk and Control Self-Assessment).

C&ORC projeta, implementa e conduz a CRA como um componente do CRMF (Compliance Risk Management Framework, ou Estrutura de Gerenciamento de Risco de Compliance, em tradução livre)[1]. O CRA é a avaliação independente de C&ORC do risco de conformidade associado às leis, regras e regulamentos mais impactantes e às orientações de supervisão (LRRs – Laws, Rules and Regulations). O CRA segue uma metodologia padrão de avaliação de risco, conforme descrito a seguir:

a. Risco Inerente – Avalia a natureza, complexidade, volume e probabilidade das atividades que geram risco.

b. Ambiente de Controle – Fornece uma conclusão baseada na avaliação de atividades de controle individuais.

c. Risco Residual – É o risco que permanece após a consideração do risco inerente e do ambiente de controle.

O principal objetivo é avaliar o ambiente de controle em vigor para mitigar o risco inerente associado aos requisitos regulatórios específicos e identificar lacunas nas atividades de controle com planos de ação associados para remediação. Os resultados do CRA são agregados no CUSO e na divisão de negócios – nesse caso a divisão de gestão de fortunas localmente realizada pela UBS Administradora – para facilitar a elaboração de relatórios ao Comitê de Riscos e aos Comitês de Gestão. Os relatórios do CRA fornecem subsídios sobre a integridade do programa de compliance no que se refere às LRRs

[1] O objetivo da Estrutura de Gerenciamento de Risco de Compliance (CRMF) de Operações Combinadas dos EUA (CUSO, Combined US Operations) é fornecer uma visão abrangente da abordagem de ponta a ponta para gerenciar o risco de compliance. A falha em gerenciar adequadamente o risco de conformidade pode afetar a capacidade de atender aos objetivos estratégicos, pode levar a litígios, representa um risco de sanção ou penalidade e/ou coloca a reputação em risco. Penalidades financeiras, danos à reputação, custos associados a processos judiciais e/ou determinações judiciais ou regulatórias desfavoráveis também podem afetar adversamente nossos negócios, operações e/ou condição financeira. Para mais detalhes sobre o CRMF, consulte 1-E-005664.

avaliados. As informações dos resultados do CRA também são fornecidas e disponibilizadas para consideração ao processo RCSA.

As CRAs avaliam os riscos em nível de LRR por BD, função e/ou LE. A agregação de riscos ocorre no nível do CUSO, bem como pelo BD e LE, quando apropriado, e avaliam os LRR para:

a. Identificar e medir a conformidade inerente e residual, a conduta e as exposições ao risco regulatório em todo o CUSO, incluindo visões nos níveis BD e LE.

b. Identificar lacunas nas atividades de controle, com o desenvolvimento do plano de remediação associado.

c. Atuar como uma entrada no desenvolvimento de testes baseados em risco e programas de treinamento.

d. Fornecer informações para o processo anual de Autoavaliação de Risco e Controle (RCSA) executado pela 1ª Linha de Defesa (LOD).

8.3. RCSA – Risk and Control Self-Assessment (Autoavaliação de risco e controle)

Conforme Risk Control Self-Assessment (RCSA) Guidance (ou, em tradução livre, Guia de Autoavaliação de risco e controle – 1-G-007624), a RCSA, por sua vez, tem como principal objetivo:

c. Fornecer uma visão sobre o nível de RI (Risco Inerente);

d. Identificar deficiências/lacunas de controle e planos de ação de remediação associados;

e. Avaliar o nível de RR (Risco Residual) e mitigar as ações quando necessário.

O resultado da RCSA fornece:

a. Visão detalhada para a alta administração do perfil de risco em todas as funções/produtos/negócios, permitindo que estratégias sejam desenvolvidas para mitigar ou eliminar os riscos identificados;

b. Entrada fundamental para o planejamento da estratégia de negócios, ajudando a alinhar prioridades e recursos aos principais riscos operacionais e de conformidade;

c. Base para atualizar a Declaração de Apetite ao Risco Operacional (RAS), conforme definido no Operational Risk Appetite Guidance (ou, em tradução livre, Guia de Apetite ao Risco Operacional -1-G-007626);

d. Resultados transparentes de avaliação de riscos, incorporados ao Relatório Anual de Conformidade e Risco Operacional (ACOR) e ao Relatório de Risco de Grupo (GRR);

e. Informações abrangentes e relevantes de risco e controle para GCRG e Auditoria Interna do Grupo (GIA) no trabalho de planejamento/revisão de atividades;

f. Impulsiona a conscientização dos riscos operacionais e aumenta a consciência de controle em todas as funções E2E e F2B envolvidas no RCSA.

Na UBS Administradora, o RCSA é conduzido por BRO e as evidências relacionadas ao exercício e as respectivas avaliações ficarão disponíveis junto a BRO para acesso mediante solicitação da Alta Administração.

A RCSA é conduzida de acordo com as dezoito taxonomias atualmente utilizadas pelo Grupo UBS para a classificação de riscos inerentes.

8.4. GMMCS – Global Monitoring, Surveillance & Controls Minimum Control Standards (Padrões Mínimos de Controle Global de Monitoramento, Vigilância e Controles)

Para alcançar consistência na abordagem das atividades de monitoramento, vigilância e controle em toda a empresa, foram estabelecidos os Padrões Mínimos de Controle Global MS&C (GMMCS) que definem a frequência, o escopo e o objetivo mínimos para os controles das taxonomias de risco crítico. O Fórum Operacional de MS&C das Américas foi estabelecido para que a MS&C comunique riscos emergentes, questões operacionais, mudanças no programa, cobertura e/ou controles subjacentes e descobertas significativas emergentes do programa para as principais partes interessadas regularmente.

O Quadro Operacional de MS&C das Américas detalha a estrutura operacional para MS&C das Américas e a governança para gerenciar e escalar questões decorrentes de tais atividades. Ele descreve a missão e o mandato do MS&C das Américas e define os respectivos papéis e responsabilidades das equipes regionais de Execução do MS&C e de Gerenciamento de Produtos globais sob o modelo operacional global da MS&C. Além disso, a Estrutura Operacional MS&C (MS&C das Américas) fornece orientação

sobre o que, quando e como escalar as questões para permitir a supervisão adequada e contínua dos programas de monitoramento e vigilância da MS&C, conforme Combined US Operations Compliance Risk Management Framework (Estrutura gerenciamento de risco de compliance CUSO, em tradução livre, 1-E-005656).

No mínimo, anualmente, a equipe de Gerenciamento de Produtos da MS&C realiza uma Annual Product Framework Review (APFR, ou Revisão Anual da Estrutura de Produtos, em tradução livre) para as taxonomias de risco cobertas pela MS&C. O MS&C APFR é uma avaliação front-to-back (de frente para trás) que avalia a estrutura de monitoramento e controle de vigilância, incorporando uma série de insumos (RCSA, CRA, Conselhos de Taxonomia, Revisões Temáticas C&ORC, alterações nos LRRs, etc.), para avaliar os principais riscos que afetam a Empresa para determinar se a estrutura de controle de monitoramento e vigilância mitiga os principais riscos subjacentes e é adequada à finalidade. Caso alguma lacuna(s) seja identificada na estrutura de monitoramento do GMMCS, a MS&C tomará e comunicará as ações tomadas para resolver qualquer lacuna de cobertura de monitoramento identificada.

C&ORC realiza o GMMCS. Na UBS Administradora, eles consistem em 10 (dez) testes.

8.5. Observação diária

Todos os colaboradores da UBS Administradora são orientados a praticar a observação diária das atividades desempenhadas por sua área, visando assegurar um ambiente de controle seguro e eficaz. Frequentemente, ocorrem mudanças nas atividades diárias e no ambiente de negócios, ocasionadas por diversos fatores como p. ex. novas regulamentações, desenvolvimento e aprimoramento de produtos e serviços. O ambiente de controles deve acompanhar tais movimentos e ser atualizado sempre que necessário.

A observação diária permite que, em complemento aos demais processos de controle, seja possível identificar incidentes relevantes. A depender da significância desse achado, ele será reportado nos fóruns de governança da UBS Administradora, ou mesmo do Grupo UBS, e poderá ser enquadrado em alguma das rotinas e fluxos de monitoramento e controle.

8.6. Auditoria Interna

A Group Internal Audit (GIA, ou, em tradução livre Auditoria Interna do Grupo) é a terceira linha de defesa no modelo adotado pelo Grupo UBS. É responsável por avaliar de forma independente se os processos de gestão, controle e governança de riscos são concebidos e operam de forma sustentável e eficaz.

9. NFR Issues – Problemas de risco não financeiro

9.1. O que são NFR Issues?

Conforme o NFR Issue Guidelines (ou, em tradução livre, Guia de Incidente de risco não financeiro - 1-G-007620) um Incidente de NFR (non-financial risk, ou, em tradução livre, risco não financeiro) é uma deficiência de controle interno que existe se um controle estiver ausente ou não for adequadamente projetado para mitigar um risco (deficiência de desenho), ou se um controle adequado tiver sido definido, mas não for executado corretamente (deficiência operacional). Por exemplo, existe uma deficiência de projeto quando um controle foi encontrado ausente ou o projeto de controle se revelou ineficaz para mitigar o risco para o qual foi projetado, ou há necessidade de novos controles devido a mudanças no ambiente de negócios ou regulamentação. No caso de uma deficiência operacional, um controle existente não foi executado corretamente (por exemplo, restrições de recursos, treinamento insuficiente ou falhas de ferramentas).

Existem quatro tipos de Incidente:

1. Caso Auto identificado (SII) – Incidente identificado pelas funções de gestão/controle do BD/GF;

2. Caso de Auditoria – Questão identificada pela Auditoria Interna do Grupo (GIA), Revisão do Risco de Crédito (CRR) e Auditoria Externa (ver também secção 3.1);

3. Caso Regulatório – Questão identificada pelos Reguladores; e

4. Caso regulatório restrito – Todas as descobertas identificadas pelos reguladores dos EUA sujeitas a restrições de Informações Confidenciais de Supervisão (CSI) (1-G-005643), consulte também a seção Restrições de informações

Os NFR Issue são registrados para apoiar a administração em (i) completar suas responsabilidades de gerenciamento de riscos e supervisão, (ii) priorizar medidas de remediação e (iii) relatar deficiências de controle interno à governança relevante e às partes interessadas relevantes de forma padronizada e consistente. Portanto, é imprescindível que as informações relativas às Questões sejam corretas, claras e completas; e que fornece NFRs de alta qualidade, claras e bem descritas, deficiências de controle interno e medidas mitigadoras.

9.2. Quando um NFR issue deve ser registrado?

É obrigatório registrar um NFR Issue quando uma deficiência ou lacuna de controle interno é identificada[2] (por exemplo, através de Auto-avaliação KPCi, resultados de testes de controle, um evento NFR, revisão temática, avaliações NFR etc.) que é equivalente a uma classificação igual ou superior a 3 nas escalas de classificação de emissão previstas na seção 3.6 do NFR Issue Guidelines (ou, em tradução livre, Guia de incidente de risco não financeiro - 1-G-007620).

10. C&ORC Controller

Os C&ORC Controller são responsáveis por revisar, questionar e monitorar de forma independente a conclusão dos processos de NFRF - Non-Financial Risk Framework (ou, em tradução livre, Estrutura de Riscos Não-Financeiros); pela gestão de riscos; e pela aderência às orientações da NFRF na gestão, avaliação, medição e controle de riscos não financeiros, de acordo com a Non-Financial Risk Framework (NFRF, Estrutura de Riscos Não-Financeiros – 1-P-000017). Ainda segundo a NFRF, os C&ORC Controller são responsáveis por questionar a adequação da NFRMM (NFR Management Methodology, ou em tradução livre, Metodologia de gerenciamento de risco não financeiro) como parte da revisão a cada dozemeses para confirmar que a NFRMM é suficiente para gerenciar a exposição a NFR. Para obter mais detalhes, consulte goto/nfrf.

De acordo com a RRF (Regulatory Reporting Framework, ou, em tradução livre, Estrutura de reporte regulatório - 1-P-002980), os C&ORC Controllers alinhados às divisões de negócio e às funções do Grupo (BD/FG) são responsáveis pela supervisão, revisão e questionamento de suas áreas alinhadas à

[2] Exceto se houver excepcional acordo em contrário C&ORC Controller relevante.

BD/FG; além de apoiar a implementação efetiva dos requisitos descritos na RRF e avaliar os riscos que afetam a Taxonomia 11 de Relatórios Financeiros e Regulatórios de Risco Operacional.

Conforme a Non-Financial Risk Events Management Guidance (Orientação para a Gestão de Eventos de Risco Não Financeiro 1-G-001454), os C&ORC Controller são responsáveis por questionar a adequação da documentação dos eventos NFR Internos de responsabilidade de sua Divisão de Negócios / Função de Grupo alinhada, e a adequação as ações definidas e a remediação são adequadas. De acordo com a RACI, os C&ORC Controller analisam a documentação de todos os Eventos NFR Internos com impacto monetário com pelo menos "impacto moderado" e Eventos NFR Internos com impacto não monetário e Quase-Ocorrência (near-miss) com um impacto pelo menos "significante".

Ainda de acordo, com a NFR Events Management Guidance, os C&ORC Controller são responsáveis por realizar uma revisão inicial dos eventos NFR externos que ocorreram em Divisões de Negócios / Funções de Grupo alinhadas em empresas pares para determinar se uma Revisão do GCRG deve ser proposta ao membro relevante da Equipe de Gerenciamento do GCRG (Management Team) (consulte Diretrizes de Revisão do GCRG). A revisão inicial deve considerar se o evento NFR externo tem potencial para ocorrer no UBS.

Ainda em conformidade com a NFR Events Management Guidance, no mínimo trimestralmente, os C&ORC Controller devem revisar todos os eventos NFR externos relatados no banco de dados de eventos SAS NFR e atribuídos à sua linha de negócios alinhada com um impacto superior a 1 milhão de dólares americanos para determinar se uma revisão do GCRG deve ser concluída. Quando esta revisão inicial concluir que é necessária uma revisão do GCRG, esta deve ser concluída em conformidade com as orientações de revisão do GCRG. Os fatores a serem considerados ao determinar se uma Revisão do GCRG é necessária podem incluir (i) a probabilidade de o UBS enfrentar exposição semelhante ao Risco Inerente à empresa de pares (com base nos produtos/serviços do UBS) e (ii) as prioridades existentes e o portfólio de Revisão do GCRG em andamento.

Considerando o NFR Issue Guidelines (ou, em tradução livre, Guia de Incidentes de NFR -1-G-007620), os C&ORC Controller são obrigados a realizar uma revisão dos incidentes nos principais estágios do seu ciclo de vida para avaliar se:

- O incidente está devidamente descrito e se a responsabilidade está adequada

- O incidente foi avaliado com precisão, segundo o ranking estabelecido
- O IMD é apropriado
- Os Planos de Ação são claros e adequados para garantir a remediação sustentável do incidente
- O mapeamento de dados para função afetada – o local está correto.

Quanto às avaliações iniciais pelo C&ORC Controller, eles devem realizar uma revisão inicial de incidentes auto identificados e Regulatórias (pré-publicação) conforme abaixo:

- Todos os SIIs (a serem concluídos em até 30 dias após a mudança para o Período de Carência Aberta)
- Questões Regulatórias e Regulatórias Restritas - Quando a carta de resposta regulatória está sendo elaborada (antes de ser levantada no ERMS) Uma verificação subsequente é necessária para garantir que a resposta apareça no ERMS conforme acordado (dentro de 30 dias após a publicação)

Como parte da revisão inicial, o C&ORC Controller deve questionar a definição do Incidente (por meio de uma revisão documentada capturada no sistema ERMS).

Já de acordo com Control Management Guidance (Guia de gerenciamento de controle - 1-G-007621), os C&ORC Controller são responsáveis por revisar e questionar a metodologia pela qual as Divisões de Negócios / Funções do Grupo / Entidades UBS garantem que um conjunto adequado e eficaz de KPCs e KPCis internos sejam definidos, implementados e testados [veja Orientação da Metodologia de Gestão de Riscos Não Financeiros (1-G-007629)]. Além disso, os C&ORC Controller são responsáveis por revisar e desafiar as conclusões e respostas de revisão do portfólio de controle da Divisão de Negócios / Função de Grupo. Os C&ORC Controller também são responsáveis por questionar os resultados da Avaliação KPCi e relatar durante a Estrutura de Controle.

Durante a Avaliação KPCi, os C&ORC Controller são responsáveis por fornecer supervisão e questionamento das Avaliações KPCi (KPCi Assessment), e por participar dos fóruns de governança. Especificamente, os C&ORC Controller são obrigados a cobrir as atividades de acordo com a Lista de Verificação do C&ORC Controller (modelo disponível em goto/NFRF).

No âmbito da RCSA, conforme Risk Control Self-Assessment (RCSA) Guidance (ou, em tradução livre, Guia de Autoavaliação de Controle de Risco 1-G-007624), as equipes de C&ORC Controller fornecem revisão e questionamento em todo o RCSA, inclusive quando GF/BD/SGEs estão determinando seu escopo e resultados finais. Cada fase do RCSA é facilitada pela gerência GF/BD/SGE e/ou ORM/BRM e questionada pelas equipes de C&ORC Controller.

Em atenção ao Operational Risk Appetite Guidance (ou, em tradução livre, Guia de Apetite ao Risco Operacional - 1-G-007626), os C&ORC Controller são responsáveis por questionar a RAS (declaração de apetite ao risco) e a avaliação de apetite de risco do C&ORC pode impor limites operacionais, se necessário, como resultado da avaliação.

Já em atenção ao Operational Risk Management Methodology Guidance (Guia da Metodologia de Gestão de Risco Operacional 1-G-007629), os C&ORC Controller são responsáveis por questionar a adequação do projeto da metodologia ORM como parte do processo de revisão anual para confirmar que a metodologia é suficiente para gerenciar a exposição ao risco operacional e que o(s) documento(s) da metodologia ORM atende(m) a padrões mínimos previstos no próprio guia.

Compete, ainda, ao C&ORC Controller, questionar (i) o desenvolvimento inicial, (ii) a revisão anual e (iii) quaisquer alterações materiais provisórias no(s) documento(s) da Metodologia ORM. Os C&ORC Controller são obrigados a questionar a metodologia documentada. Quando a metodologia ORM for considerada inadequada para gerenciar o risco operacional dentro da Divisão de Negócios / Função do Grupo / Entidade do Grupo Significativo, não tiver sido documentada de acordo com os padrões mínimos descritos neste documento, ou a documentação não tiver sido revisada e reaprovada dentro de 12 meses, o C&ORC Controller é obrigado a desafiar o Gerenciamento de Risco, e onde o desafio não for resolvido, escale para o Chefe de Divisão / Grupo Funcional / Entidade Significativa Grupo da C&ORC.

11. Comitês e fóruns

A governança da UBS Administradora e do Grupo UBS no Brasil é composta, entre outros, por uma série de comitês, os quais serão mencionados abaixo em lista não exaustiva focada em risco operacional e controles internos.

Além desses comitês, há, ainda, o Conselho de Administração da empresa o qual é composto por no mínimo três e no máximo de sete membros efetivos. A assembleia de sócios pode indicar também igual número de suplentes. Todos eles, plenos ou suplentes, possuem mandato de três anos, permitida a reeleição e podem ser destituídos a qualquer tempo.

As atividades de gestão dos negócios da empresa são conduzidas por uma diretoria composta por uma ou mais pessoas físicas residentes e domiciliadas no país eleitas para mandatos com prazo indeterminado.

11.1. Brazil Executive Committee (EXCO)

11.1.1. Funções

As principais atribuições do comitê são:

- definir e supervisionar o quadro geral de governança;
- facilitar a coordenação interdivisional e interfuncional;
- disseminar informações de outros comitês regionais/globais e tomar decisões sobre assuntos que lhe são encaminhados por fóruns de outros países;
- priorizar projetos, iniciativas e tarefas conforme necessário;
- analisar e discutir tendências relevantes de negócios;
- supervisionar a estratégia e os planos de negócios, incluindo alocação de custos/recursos, e sua execução;
- decidir sobre questões críticas de risco do negócio, trabalhando em conjunto com o Comitê de Controle de Riscos do Brasil (BRCC) para iniciar e monitorar ações de eliminação ou mitigação de deficiências, conforme apropriado;
- monitorar indicadores gerais do negócio e desempenho financeiro;
- revisar e escalar, conforme apropriado, questões relacionadas às atividades comerciais gerais para o país e entidades locais no escopo (Anexo A), incluindo avaliação e avaliação

de novas iniciativas de negócios importantes sob a estrutura de controle de novos negócios do Banco;

- promover um comportamento e cultura alvo para o Brasil, consistente com os princípios e comportamentos da UBS;
- supervisionar as Entidades locais no escopo de acordo com as responsabilidades descritas na Política de Entidades do UBS (1-P-000355), nos casos em que não estejam em conflito com quaisquer disposições legais, regulamentares ou estatutárias para um Conselho de Administração (CA) específico de uma Entidade local, se constituído. As Entidades no escopo incluem a UBS Administradora.

Ainda de acordo com os Terms of Reference (regimento interno, em tradução livre), cabe aos diretores estatutários das Entidades UBS no escopo:

- supervisionar e monitorar as Entidades locais (entre as quais a UBS Administradora), atuando como seu principal órgão de governança, em todos os assuntos relacionados às funções dos Diretores da Entidade local (Estatutários) – quando não conflitar com quaisquer disposições legais, regulamentares ou estatutárias do Conselho de Administração (BOD), se constituído;
- Revisar e aprovar as demonstrações financeiras anuais, sujeitas às exigências legais e regulatórias locais;
- aprovar os documentos constitucionais (por exemplo, Estatutos, Estatutos ou Regulamentos Organizacionais) e a estrutura de governança das Entidades locais (incluindo a UBS Administradora), de acordo com os padrões mínimos estabelecidos pelo Grupo;
- seguir os Princípios de Estrutura Jurídica Corporativa e Governança de Entidades locais descritos na Política de Entidades UBS (1-P-000355);
- auxiliar o Administrador Corporativo para garantir que cada Entidade local (incluindo a UBS Administradora) seja registrada e atualizada no Banco de Dados de Estrutura Jurídica (LSDB);

- garantir que os negócios realizados através de cada Entidade local (incluindo a UBS Administradora) estejam de acordo com seus documentos constitucionais (estatutos, regulamentos de organização da Entidade local etc.) e no âmbito de sua licença, se aplicável;
- iniciar e patrocinar mudanças que afetem a estrutura jurídica corporativa, incluindo a formação de novas Entidades locais ou qualquer mudança material subsequente no status ou atividades de uma Entidade local, de acordo com a avaliação ex ante apropriada de acordo com a política de Entidades UBS.

11.1.2. Integrantes

Integram o ExCo, com direito a voto:

- Líder de país do UBS Brasil;
- Líder de Mercados Globais;
- Diretor executivo do UBS BB Investment Bank e Líder do Global Banking;
- Co-Líder de Wealth Management Brasil;
- Diretor de Riscos (CRO);
- Diretor Financeiro (CFO);
- Líder de C&ORC;
- Diretor Jurídico;
- Líder de Recursos Humanos;
- Líder de Operações IB (UBS BB);
- Líder de Tecnologia da Informação;
- Chefe de Gabinete.

11.2. Brazil Risk & Control Committee (BRCC)

11.2.1. Funções

Compete ao BRCC:

- definir os níveis de apetite ao risco da instituição no RAS a nível nacional e analisá-los com o apoio dos membros do Comité Executivo e do CRO;
- avaliar as estratégias para a gestão dos níveis de apetite ao risco estabelecidos na RAS, considerando os riscos individualmente e de forma integrada;
- discutir e coordenar informações sobre tendências regulatórias, legislativas e de riscos relevantes;
- promover a disseminação da cultura de gestão de riscos na instituição;
- Escalar decisões regulatórias ou de reputação relevantes;
- discutir e coordenar as estratégias de franquia e negócios do UBS;
- facilitar uma coordenação interdivisional eficiente da infraestrutura operacional;
- garantir, com suporte jurídico e compliance, que o UBS esteja fazendo interface adequada com os reguladores de serviços financeiros.

11.2.2. Integrantes

Integram o BRCC, com direito a voto:

- Líder de Wealth Management América Latina e Líder de país do Grupo UBS no Brasil;
- Diretor de riscos, ou Chief Risk Officer (CRO) do Grupo UBS no Brasil;
- Diretor Financeiro (CFO) Brasil;
- Líder de C&ORC Wealth Management América Latina e do Grupo UBS no Brasil;
- Líder de Operações;

- Líder de Tecnologia da Informação do Grupo UBS no Brasil
- Líder ou líder de mesa para WM Brasil;
- Diretor executive do UBS BB Investment Bank e Líder do Global Banking UBS BB Investment Bank;
- Líder de Mercados Globais LatAm;
- Líder de Recursos Humanos;
- Líder de Investimentos no Brasil;
- Diretor Jurídico para o Brasil e América Latina.

11.3. WM Brazil Management Forum (WM MF)

11.3.1. Funções

O fórum foi criado para promover uma avaliação e coordenação abrangentes dos negócios, riscos e governança relevantes dentro da WM Brasil. Foi instituído para auxiliar os Co-líderes da UBS Consenso no exercício de suas responsabilidades.

Fornece análise e profere decisões sobre iniciativas estratégicas, desempenho empresarial, deveres regulatórios, iniciativas de conformidade, como monitoramento e gerenciamento de potenciais conflitos de interesse e atualização de políticas e procedimentos.

Garante a eficácia das práticas de governança no local, supervisiona o ambiente operacional front-to-back e dá suporte à tomada de decisões críticas em relação à pauta de negócios da WM Brasil.

Suas Principais responsabilidades e deveres são:

- desenvolver, implementar, monitorar e promover a estratégia de negócios da WM Brasil;
- avaliar e monitorar o desempenho financeiro geral da WM Brasil e estabelecer critérios, quando apropriado, para eficiência e eficácia operacional;

- resolver e/ou escalar itens de ação de risco relevante e regulatório identificados e encaminhá-los para o representante da função de negócio ou grupo para posterior análise, tomada de decisão e ação;
- tomar decisões sobre assuntos escalados para ele por outros fóruns WM no local;
- servir como fórum para escalada de questões e assuntos que necessitam de resolução;
- gerenciar assuntos relacionados ao RH, quando necessário;
- revisar questões relacionadas à estrutura, organização e governança da WM Brasil;
- atuar como o Órgão de Decisão de Preços de Localização, que define e revisa as práticas de gestão de preços de clientes da WM Brasil e padrões anuais

11.3.2. Integrantes

Integram o fórum:

- Co-Líderes da UBS Consenso ("tomadores-chave de risco")
- BRO
- Representantes da área de negócios
- Representantes de funções do grupo (por exemplo, CRO, C&ORC, Jurídico, TI, Operações, Finanças, RH)

Deve-se notar que os representantes de CRO e C&ORC possuem poder de veto para assegurar a independência exigida pela regulação.

11.4. Brazil Compliance Forum (BCF)

11.4.1. Funções

O Brazil Compliance Forum (BCF) é o foro para discutir e escalar formalmente os riscos de compliance que afetam as entidades jurídicas locais do UBS Brasil em suas áreas de negócios de Investment Banking (IB) e Wealth Management (WM), bem como funções de grupo e áreas

interdivisionais, e determinar se tais riscos são compreendidos e gerenciados dentro do apetite de risco da empresa. Este Fórum é estabelecido pelo líder de C&ORC Brazil & Wealth Management LatAm para fornecer à alta administração de Compliance uma visão consolidada dos riscos significativos de compliance presentes e emergentes.

O BCF fornece supervisão para a identificação e escalonamento de temas, eventos, problemas e remediação de riscos em todo o Brasil. Em particular, o Fórum permite o gerenciamento coletivo do risco de compliance (incluindo o risco de conduta e crime financeiro), avalia a aderência às Estruturas UBS e ao Programa de Compliance Brasil, avalia mudanças e tendências regulatórias, facilita a colaboração entre divisões e revisa métricas e indicadores relevantes. Quaisquer questões materiais decorrentes do BCF são encaminhadas para o Americas Compliance & Operational Risk Control Risk Forum (AC&ORC RF), que é copresidido pelo Chief Compliance Officer das Américas, com potencial escalonamento adicional, quando apropriado, para o CUSO Operating Management Forum (CUSO OMF), o Comitê de Gestão CUSO (CUSO MC) ou fóruns/comitês globais de Compliance da divisão de negócios. O Fórum avalia periodicamente seu desempenho para identificar oportunidades de melhoria de processos e aprimoramento da gestão de riscos.

11.4.2. Integrantes

- Presidente: Head da C&ORC Brasil e WM LatAm
- Representante de Compliance das Américas
- Líder de Compliance de Gestão de Patrimônio no Brasil
- Líder Compliance do banco de investimentos no Brasil
- Líder de Prevenção de Crimes Financeiros
- Encarregado de Proteção de Dados
- Líder de Controle de Risco Operacional
- Secretário do BCF

11.5. WM Local Risk Forum (WM LRF)

11.5.1. Funções

O Local Risk Forum tem as funções de:

- Manter a responsabilidade pelo equilíbrio adequado entre riscos e recompensas
- garantir que o apetite de risco para a Unidade de Negócio/Localização seja devidamente definido através de políticas, declarações de apetite ao risco, normas, procedimentos e limites operacionais e seja implementado e monitorado por meio de um ambiente de controle eficaz
- garantir que o apetite ao risco seja consistente com a capacidade de risco da Divisão de Negócios, da Unidade de Negócios e da Localização, bem como com requisitos regulamentares aplicáveis e políticas e limites do UBS
- supervisionar a implementação, manutenção e monitoramento das estruturas de controle, conforme aplicável
- monitorar todos os riscos primários e operacionais relevantes (i.e., risco de crédito, risco de mercado, compliance e risco operacional, risco legal e risco reputacional)
- garantir que as recomendações da Auditoria Interna do Grupo, auditores externos, funções de controle interno ou quaisquer reguladores sejam abordados oportunamente e de forma sustentável
- aprovar a avaliação trimestral de riscos (relatório de riscos)
- monitorar a atividade regulatória relevante para garantir que a interface da Unidade de Negócios/Local com qualquer regulador seja adequadamente coordenada e que quaisquer respostas tenham todo o peso da gestão

11.5.2. Integrantes

- Líder da Unidade de Negócios/ Localização) - "Tomador de Risco Chave"

- BRO
- Representantes das áreas de negócios
- Representante das Funções de grupo (por exemplo, CRO, GC, CDIO, C&ORC), quando aplicável
- Opcional: GIA, Finanças, RH

11.6. Escalation Forum

11.6.1. Funções

O fórum tem a função de promover uma avaliação abrangente e atuar como órgão de escalonamento para carteiras de clientes que não aderem aos limites da política de risco local. Tem como objetivo auxiliar os principais tomadores de risco perante o regulador em casos em que a carteira de clientes não está aderente aos limites atribuídos, bem como avaliar as justificativas de apetite de risco do negócio para manter determinadas violações, apesar dos critérios estabelecidos definidos na política de risco local.

Discussões relevantes para o procedimento e a política de riscos, bem como qualquer exceção ou mudança de metodologia também podem ser apresentadas e discutidas dentro dos membros do fórum.

O fórum decide se uma carteira de clientes que esteja violando os limites atribuídos deve ser mantida em violação, considerando a plausibilidade da justificativa apresentada pelos assessores de clientes (CA) como parte de seu monitoramento regular da carteira, bem como determinar possíveis ações a serem tomadas pelos CAs para resolver oportunamente a violação se a justificativa não for aceita. O fórum garante que as carteiras dos clientes sejam devidamente avaliadas à luz da política de risco local, a fim de garantir que os investimentos dos clientes permaneçam dentro dos limites regulatórios locais aplicáveis.

Principais responsabilidades e deveres:

- Avaliar, debater e decidir sobre violações da carteira de clientes;
- Aprovar a plausibilidade da lógica de desalinhamento da carteira dos clientes;

- Decidir sobre outras ações a serem tomadas para resolver violações de portfólio e garantir que eles aderem à política local;
- Aprovações ad hoc de metodologias e desvios em relação à política de riscos local;

11.6.2. Integrantes

Integram o forum:

- Líder de investimentos
- Diretor de gestão de riscos (CRO)
- Representantes das funções de grupo (C&ORC, Jurídico, TI, Operações)
- Business Risk Organization (BRO)

12. Controles

Anexado a este manual está a lista de controles internos, especificamente de KPCis, considerados relacionados às obrigações oriundas da Res. 21, de 2021. É importante notar, porém, que essa lista pode sofrer alterações com frequência maior do que a de atualização deste Manual. Assim, recomenda-se verificar a lista de controles internos aplicáveis à UBS Administradora no sistema M7.

13. Anexo 1: Documentos relacionados

POLO ID	Título
1-P-000017	Non-Financial Risk Framework Policy
1-P-004686	Information Barriers
1-P-000162	Cyber & Information Security Policy
9-G-004387	Application and Infrastructure Security Vulnerability Management Guidance
1-P-002103	Cyber & Information Security (CIS) Technical and Specialist Requirements
1-P-00057	Continuity & Resilience Framework
1-P-001061	Group Data Protection Policy
1-P-004710	Employee Incidents Policy
1-P-002980	Regulatory Reporting Framework (RRF)
1-G-007621	Control Management Guidance
1-G-007620	NFR Issue Guidelines
1-E-005664	CUSO - Combined US Operations Compliance Risk Management Framework
1-G-007624	Risk Control Self-Assessment (RCSA) Guidance
1-E-005664	Combined US Operations Compliance Risk Management Framework
1-G-001454	Non-Financial Risk Events Management Guidance
1-G-007629	Operational Risk Management Methodology Guidance
1-P-000355	UBS Entities