

# Manual de Controles Internos – Resolução CVM nº 21/2021 e Código ART Anbima/21

UBS Brasil Administradora de Valores Mobiliários Ltda.

# Table of Contents

<b>1.</b>	<b>Introdução .....</b>	<b>3</b>
1.1.	Objetivo .....	3
1.2.	Definição .....	3
1.3.	Processo .....	3
<b>2.</b>	<b>Governança Corporativa .....</b>	<b>3</b>
<b>3.</b>	<b>Responsabilidades .....</b>	<b>4</b>
3.1.	Conselho de Administração .....	4
3.2.	Comitê de Risco .....	4
3.3.	Diretoria Executiva .....	4
3.4.	Divisão de Negócios e Funções Operacionais .....	4
3.5.	Conformidade & Controle de Risco Operacional (C&ORC) .....	5
3.6.	Colaboradores .....	5
3.7.	Diretor Estatutário de controles internos .....	5
<b>4.</b>	<b>Avaliação do Risco Operacional .....</b>	<b>6</b>
4.1.	Taxonomia de Risco Operacional .....	6
4.2.	Controles Internos .....	6
4.3.	Processo de Avaliação de Controles Processuais Chave (KPCi Assessment) .....	6
4.4.	Deficiências de Risco Operacional (Operational Risk Issues - ORI) .....	7
4.5.	Avaliação de Risco .....	7
<b>5.</b>	<b>Eventos de Risco Operacional .....</b>	<b>8</b>
<b>6.</b>	<b>Controles .....</b>	<b>8</b>
6.1.	Recursos Humanos .....	8
6.2.	Finanças .....	9
6.3.	Compliance .....	10
6.4.	Operações .....	13
6.5.	Tecnologia .....	15
6.6.	Controle de Riscos .....	17
6.7.	Área de Riscos do Negócio .....	18
<b>7.</b>	<b>Aprovação, Vigência e Revisão .....</b>	<b>23</b>

## 1. Introdução

### 1.1. Objetivo

Este documento (“Manual”) tem como objetivo delimitar as regras, os procedimentos e os controles internos adotados pela UBS Brasil Administradora de Valores Mobiliários Ltda. (“UBS Brasil”) na condução das atividades de administração de carteiras de valores mobiliários, em atendimento ao que dispõe a Resolução CVM nº 21, de 25 de fevereiro de 2021 (“RCVM21”) e Código ANBIMA de Regulação e Melhores Práticas para Administração de Recurso de Terceiros (Capítulo V) .

### 1.2. Definição

As regras, os procedimentos e os controles internos a que se refere este Manual abrangem todo o relacionamento de cada cliente com a UBS Brasil, desde a captação e/ou originação até a efetiva prestação dos serviços de administração profissional de carteiras de valores mobiliários, e visam a garantir que a regulamentação aplicável seja cumprida durante todas as etapas do relacionamento com o cliente/ através da atribuição de responsabilidades específicas relativas à realização e à implementação dos controles internos junto à departamentos específicos da UBS Brasil.

### 1.3. Processo

O processo básico a ser seguido no âmbito deste Manual consiste na verificação permanente por parte das áreas de riscos da UBS Brasil(originação, produtos de investimentos e serviços e operações), bem como da área de *C&ORC – Compliance & Operational Risk Control* a respeito do cumprimento das regras, dos procedimentos e dos controles internos a que se refere este Manual. Além disso, uma vez identificadas falhas de execução nos processos, nos controles ou de qualquer outra forma, as áreas acima mencionadas serão responsáveis por elaborar, em conjunto com as demais áreas aplicáveis, os planos de ação necessários à remediação do ocorrido, seguindo o modelo de reporte global do UBS Brasil (informações adicionais disponíveis com a área de C&ORC).

## 2. Governança Corporativa

A Diretoria de Compliance, Risco Operacional e Controles Internos (C&ORC) é nomeada pelo Conselho de Administração integrando a Diretoria Estatutária do UBS Brasil ). Sua linha de reporte hierárquica é direcionada ao *Chief Compliance Officer Americas* e ao próprio Comitê Executivo do Brasil (Exco).

A estrutura de Controles Internos é integrada, independente da linha de defesa, através das avaliações detalhadas no capítulo 4 deste documento. Em termos de recrutamento, nomeações, avaliações de desempenho e medidas disciplinares, a atividade é gerenciada em conjunto com o time local de Recursos Humanos.

A atividade de Controles Internos dispõe de autonomia e soberania em todas as avaliações que envolvem a UBS Brasil, examinando-as conforme as normas regulatórias e os princípios de integridade e conduta ética.

O constante diálogo do C&ORC com as linhas de negócios é crucial para manter alinhamento e sinergia. A transparência e comunicação proativa entre a estrutura de controles Internos e as linhas de negócios são essenciais em todos os níveis da organização UBS Brasil. Essa estrutura também contempla todas as atividades propostas pelos gestores, auxiliando-os em relação aos requisitos regulatórios.

Como forma de garantir o acesso a todas as informações consideradas relevantes, a estrutura de Controles Internos possui livre acesso às informações documentais e sistêmicas, assim como a todas as dependências da instituição UBS Brasil.

Em relação aos ideais organizacionais, a Diretoria estatutária do UBS Brasil (Exco), promove a cultura de integridade e a adoção de padrões éticos a todos os colaboradores e áreas da instituição, demonstrando que as boas práticas devem partir, principalmente, de cada colaborador em suas atitudes profissionais e pessoais.

### 3. Responsabilidades

#### 3.1. Conselho de Administração

O Conselho de Administração é responsável por deliberar sobre os assuntos relacionados à gestão de riscos do UBS BRASIL, por aprovar as políticas e estratégias de gerenciamento de riscos.

O Conselho de Administração também dissemina uma cultura de risco sólida e promove a conscientização de risco em toda a empresa, alinhando o planejamento de negócios, execução, avaliação de desempenho e decisões de remuneração com a estratégia, valores, comportamentos e apetite de risco da UBS Brasil.

#### 3.2. Comitê de Risco

O Comitê de Controle de Risco do Brasil (BRCC) é órgão de governança responsável por assessorar o CA no que concerne ao exercício das suas funções relativas à gestão de riscos, emitindo recomendações independentes para auxiliar as decisões do CA.

#### 3.3. Diretoria Executiva

A Diretoria Executiva do UBS Brasil é responsável por propor, cumprir e fazer cumprir esta política, e conduzir os negócios do UBS BRASIL dentro dos níveis de apetite por riscos aprovados pelo CA.

#### 3.4. Divisão de Negócios e Funções Operacionais

A divisão de negócios e os gestores das áreas no centro corporativo são responsáveis pela eficácia da gestão de riscos operacionais.

São responsáveis pela identificação, gestão e mitigação de componentes críticos da execução do dia-a-dia do negócio e devem:

- Estabelecer e manter processos de governança efetivos para identificar e endereçar risco operacional;
- Estabelecer e manter um ambiente de controles internos materialmente abrangente e efetivo;

- Garantir que o risco operacional residual seja mantido dentro dos limites de exposição estabelecidos pelo Conselho de Administração;
- Manter o nível de risco operacional dentro dos limites de exposição estabelecidos pelo Conselho de Administração e assegurar que as ações corretivas necessárias sejam implementadas tempestivamente para reenquadramento do risco nos limites de exposição aprovados, incluindo a adaptação ou restrição de atividades comerciais, se necessário;
- Emitir relatórios de eventos de risco operacional, outros dados de indicadores de risco operacional especificado e ações de remediação, conforme requerido pelo C&ORC;
- Garantir que riscos operacionais que impactam mais de uma área sejam reportados ao C&ORC se a resolução ou o acordo sobre a remediação não forem alcançados; e
- Incluir risco operacional em relatórios gerenciais.

### **3.5. Conformidade & Controle de Risco Operacional (C&ORC)**

C&ORC é responsável por supervisionar de forma independente, desafiar e monitorar a eficácia da gestão de risco operacional e supervisiona atividades de tomada de risco, e verifica de forma independente e objetiva se as áreas estão gerindo de forma adequada os riscos operacionais materiais decorrentes de suas atividades.

### **3.6. Colaboradores**

#### Investimentos Pessoais

Os investimentos pessoais devem seguir as diretrizes da Política Global de Investimentos Pessoais do UBS Brasil. O controle de investimentos pessoais se dá por meio de sistema chamado Trade Surveillance, no qual o colaborador deve registrar cada transação (compra/venda) a ser realizada, que é posteriormente checada contra o extrato mensal do colaborador na sua conta de investimento pessoal. A política supra também menciona quais contas devem ser declaradas pelo colaborador nos sistemas internos do UBS Brasil. O controle é efetuado pelo time de Americas Conduct e violações são escaladas ao RH e ao Compliance, conforme explicada na seção específica deste relatório.

#### Código de Ética

O Grupo UBS possui um Código de Ética que estabelece os princípios e comportamentos que definem as práticas éticas do Grupo UBS e a forma como os negócios são conduzidos. Qualquer violação (seja ao Código de Ética, políticas do UBS Brasil ou leis/regulamentações/regras externas) pode ensejar ação disciplinar, que inclui a possibilidade de desligamento do colaborador na instituição. Essas violações são chamadas internamente de "Violations", que possuem política e procedimentos próprios, havendo, também, área específica dedicada ao assunto que fica fora do Brasil e acompanha os processos juntamente com os times locais de Compliance e RH. O propósito dessa estrutura própria para o tema "Violations" é ter uma abordagem definida e clara, que permita (i) responder de maneira justa e consistente às violações do Código de Ética, políticas internas, procedimentos e diretrizes; (ii) garantir o cumprimento das obrigações legais e regulamentares.

#### "Violations"

Os "Violations" possuem 3 níveis de acordo com sua gravidade, a saber: Level 1 – Alerta de políticas; Level 2 – Incidente e Level 3 – Disciplinar.

### **3.7. Diretor Estatutário de Controles Internos**

Diretor estatutário da instituição responsável pelos controles internos e pelo Compliance, independente das funções relacionadas à Administração de Recursos de Terceiros, à intermediação, distribuição ou à consultoria

de valores mobiliários, ou em qualquer atividade que limite a sua independência, na instituição, ou fora dela.

Dentre suas atribuições, ele deve 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.

## 4. Avaliação do Risco Operacional

### 4.1. Taxonomia de Risco Operacional

O objetivo da taxonomia é fornecer uma classificação clara e lógica do risco operacional inerente do UBS BRASIL em todas as divisões de negócios, para que os colaboradores possam reconhecer e classificar os riscos operacionais a que seus processos, produtos ou serviços estão sujeitos, especificando a origem e a forma de ocorrência, permitindo, assim, uma análise da exposição ao risco e concentrações.

A taxonomia é utilizada pelas funções de gerenciamento e controle para agregar dados relacionados ao risco operacional, apoiando a articulação do perfil de risco operacional, ao mesmo tempo em que fornece as bases da estrutura de risco operacional. A taxonomia é estabelecida por temas no nível 1, nível 2 e nível 3, com cada nível proporcionando maior granularidade (o guia de taxonomias encontra-se disponível no endereço goto/orf).

As categorias de taxonomia são revisadas anualmente e podem evoluir ao longo do tempo para refletir as mudanças no modelo de negócios ou o contexto regulamentar.

### 4.2. Controles Internos

A gestão é responsável por estabelecer e operar um ambiente de controle robusto. O ambiente de controle inclui, mas não está limitado a políticas, procedimentos, sistemas, processos, treinamentos e cultura, além de desenvolver um conjunto mínimo de controles internos suficientes para mitigar os principais riscos a níveis aceitáveis.

Os controles mais significativos estão definidos nos documentos de orientação de controle emitidos pelo C&ORC, são descritos como controles processuais chave (KPCs) e devem ser registrados no Sistema Padronizado de Risco Operacional (SORT e/ou M7).

### 4.3. Processo de Avaliação de Controles Processuais Chave (KPCi Assessment)

O KPCi Assessment é uma auto-avaliação do ambiente de controle que é de propriedade e operado pela respectiva função do negócio / funções operacionais. Esta avaliação é realizada (no mínimo) em base semestral e reportada ao Conselho de Administração, à Diretoria Executiva da empresa e ao C&ORC.

C&ORC verifica a coerência dos resultados e avalia os planos de remediação estruturados para correção de eventuais falhas. O resultado dessa avaliação é apresentada ao Comitê de Riscos da instituição.

O objetivo do KPCi Assessment é avaliar formalmente a efetividade do desenho e da operação do ambiente de controles internos em uma base periódica destacando problemas chave, incluindo uma avaliação dos

planos de remediação e uma revisão do impacto de futuras mudanças relacionadas à organização, regulatórias ou ao processo.

Onde os controles são ineficazes ou parcialmente ineficazes, tanto para o desenho quanto para a operação, a gerência deve avaliar o impacto para a empresa usando as escalas de classificação de ORI (Deficiência de Risco Operacional). Se a classificação de impacto do controle ineficaz é 3 ou acima, um plano de ação com ações corretivas deve ser registrado no sistema de riscos operacionais como ORI.

A orientação completa sobre os requisitos de conclusão do KPCi Assessment está disponível com C&ORC.

#### **4.4. Deficiências de Risco Operacional (Operational Risk Issues - ORI)**

Uma ORI é uma deficiência de controle interno que ocorre se um controle (i) está ausente, (ii) foi inadequadamente desenvolvido para mitigar o risco operacional ou (iii) não está operando efetivamente para mitigar sustentavelmente o risco.

#### **4.5. Avaliação de Risco**

Três avaliações chave de risco são realizadas anualmente. Esta estrutura foi desenvolvida para avaliar o risco inerente, a eficácia do ambiente de controle e o risco residual resultante a partir dos cinco fatores de impacto a seguir:

- Reputacional & Mídia
- Regulatório
- Financeiro
- Impacto no Mercado
- Cliente
- Segurança da Informação

As avaliações chave de risco são:

- Avaliação Anual da Taxonomia de Risco Operacional (ORTA), que é completada para cada taxonomia de risco nível 2 no nível do Grupo UBS BRASIL pelo responsável da taxonomia no Grupo.
- O RCSA (Auto-avaliação de Controle de Risco), que é realizada anualmente pelas divisões de negócio e entidades em uma base front-to-back, incluindo as atividades relevantes. Esta avaliação é revisada/desafiada por C&ORC antes da conclusão do processo.
- A Avaliação de Risco de Conformidade (CRA – Compliance Risk Assessment) consiste em identificar os riscos regulatórios e seus respectivos fatores mitigadores de conformidade aos quais o UBS Brasil está sujeito como unidade de negócios. De acordo com a metodologia utilizada, cada taxonomia e regulamentações locais relacionadas às mesmas devem ser avaliadas. Para o exercício, as políticas globais e os procedimentos locais aplicáveis a cada um dos temas avaliados também foram inventariados.

Onde a ORTA, RCSA e CRA indicarem níveis inaceitáveis de risco operacional a entidade / Divisão de Negócios deve criar uma ORI de acordo com o guia que está disponível em goto/ORF.

## 5. Eventos de Risco Operacional

A comunicação e avaliação dos eventos de risco operacional são essenciais para a gestão do risco operacional a que o UBS BRASIL está exposto no curso de atividades diárias.

Os relatórios abrangentes e tempestivos de eventos de risco operacional fornecem à empresa a oportunidade de analisar e aprender com esses eventos, enquanto toma as medidas necessárias, que podem incluir a implementação de novos controles ou o aprimoramento dos controles existentes, para proteger a empresa contra outras ocorrências.

Os eventos de risco operacional no UBS BRASIL podem ser classificados como eventos financeiros, eventos não financeiros ou quase perdas. Todos os eventos de riscos operacionais ou de conduta significativos devem ser registrados no SORT e/ou M7.

Além disso, a gerência deve avaliar o impacto potencial do evento para a empresa usando as escalas de classificação de ORI e se a classificação for 3 ou superior, um plano de ação com ações corretivas deve ser registrado no SORT e/ou M7.

Dados de eventos internos e externos de risco operacional são usados como dados de entrada para requerimentos de reporte interno.

A orientação completa sobre o registro e reporte de eventos está disponível com C&ORC.

## 6. Controles

Esta seção compreende a descrição de cada controle a ser realizado, segregado por área de execução dentro da estrutura do UBS Brasil.

### 6.1. Recursos Humanos

<b>Título</b>	<b>Descrição</b>
Revisão do acesso físico restrito a prédios e escritórios de RH	A revisão dos aprovadores primários com base no relatório de autorização restrita da GCS Security, trimestralmente, de que o acesso só foi dado às pessoas elegíveis à área de RH restrito.
Revisão dos Manuais dos Funcionários	Relações com funcionários de RH (ou Chefes de Prestação de Serviços Locais/Regionais em locais menores) responsáveis pela manutenção dos Manuais dos Funcionários locais, revisam que as seguintes medidas foram tomadas, no mínimo, anualmente, no H2: Os conteúdos do Manual dos Funcionários estão em consonância com as políticas locais/regionais e globais;
Registros físicos do quadro de governança	Este controle mitiga o risco de que as Funções de Divisão de Negócios/Grupo (BD/GF) não se compromissam em lidar com o não cumprimento dos registros físicos em sua propriedade, de acordo com os requisitos da 'Política de Gerenciamento de Registros (RMP) 1-P-001004" e do Modelo Operacional RM.
Cumprimento das rescisões do UBS	A Entrega de Serviços de R monitora caso a caso se todas as rescisões iniciadas pelo UBS cumprirem todos os requisitos internos antes da rescisão.



## 6.2. Finanças

<b>Título</b>	<b>Descrição</b>
Imposto - Cumprimento de Requisitos e Políticas Fiscais Locais e Em Grupo	O Proprietário do Controle é responsável por cumprir os requisitos fiscais locais e regulatórios para entidades dentro de seu escopo. Isso inclui preços de transferência, imposto retido na fonte, IVA, imposto de renda e ativos fiscais diferidos. É necessário realizar uma revisão regular (conforme especificado na frequência de controle) dos encargos e saldos tributários.
Validação das demonstrações financeiras anuais ou trimestrais divulgadas	Anualmente ou trimestralmente, o Controlador Corporativo elabora e revisa as contas estatutárias. O proprietário do controle garante que uma revisão documentada (incluindo uma revisão de 4 olhos) ocorra antes da apresentação e/ou publicação. Os relatórios classificados como críticos ou aprimorados na estrutura RRF devem seguir os requisitos de relatórios aprimorados de acordo com as Diretrizes da Política RRF.
Segregação de Despesas de Direitos & Pagamentos	O proprietário do controle é responsável por cumprir as políticas locais e do Grupo para todos os processos de pagamento e despesas. Isso inclui a Política de Compras Global do UBS e o Compromisso de Custo, Fatura e Aprovação de Reclamações. O Proprietário do Controle é obrigado a garantir que os pagamentos e as faturas sejam aprovados de acordo com os procedimentos acordados e estejam em conformidade com as políticas globais.
Substanciação do Balanço Patrimonial - Revisão do Proprietário	O Proprietário do Balanço revisa os resultados do atestado do balanço mensalmente. O Proprietário do GBSOV garante que: - os atestados dos revisores na ferramenta de atestado possam ser entendidos. - os problemas de remediação identificados em períodos de relatório anteriores são acompanhados, e - as evidências são mantidas.
Avaliações analíticas	O proprietário do controle é responsável pelo projeto e execução do processo de revisão analítica. Todas as revisões analíticas são realizadas e/ou revisadas, garantindo que quaisquer problemas sejam documentados, investigados e as causas-raiz sejam identificadas. Esses problemas são discutidos com as partes relevantes para garantir que os problemas sejam devidamente resolvidos e corrigidos na fonte em tempo hábil e escalados quando apropriado.
Substantivo de Contas de Controle e Suspense	O o proprietário do controle é responsável pelo projeto e execução do processo de revisão analítica. Todas as revisões analíticas são realizadas e/ou revisadas, garantindo que quaisquer problemas sejam documentados, investigados e as causas-raiz sejam identificadas
Conciliação de Gestão para Receita Financeira	O Controle de Produto concilia a receita de relatórios de gerenciamento ano a ano (conforme relatado à mesa) com as receitas finais do GCRS.
Revisão dos ajustes manuais	A função controladora pode ser necessária para fazer revistas manuais no ambiente de Finanças por uma série de razões.

<b>Título</b>	<b>Descrição</b>
Reconciliação com o Sistema Origem	Os controles estão em vigor para garantir que, para alimentação incremental ao GL, os saldos LTD resultantes sejam reconciliados de volta ao sistema de origem
Tesouraria - Cumprimento dos Requisitos e Políticas de Tesouraria Local e do Grupo	O Proprietário do Controle é responsável pelo cumprimento das políticas locais e da Tesouraria em grupo para todas as entidades em escopo.
Revisão Analítica das Finanças da Entidade	O Proprietário do Controle é responsável pelo cumprimento das políticas locais e da Tesouraria em grupo para todas as entidades em escopo.
Revisão gerencial de relatórios regulatórios	Para todos os relatórios regulatórios, incluindo solicitações ad hoc no âmbito do controle, o proprietário do controle garante que uma revisão documentada ocorra antes da apresentação de cada relatório, para confirmar que os requisitos regulatórios locais foram respeitados.
Avaliação sobre a completude e precisão do registro de TI financeiro de deficiências de feed de dados	As finanças são responsáveis por garantir que os problemas de qualidade dos dados para os feeds no livro geral sejam avaliados de risco (frequência, impacto, materialidade) e elevados ao Group Finance IT .

### 6.3. Compliance

<b>Título</b>	<b>Descrição</b>
Direitos de Uso de Dados - Respondendo às solicitações de direito do assunto de dados	As leis de privacidade de dados de certas jurisdições exigem que as entidades tenham um processo em vigor para responder aos titulares de dados que exercem direitos de uso de dados. Membros designados do Escritório de Proteção de Dados do Grupo / Contatos Locais de Proteção de Dados (OMS) verificam se as solicitações de objetos de dados registradas pela unidade de tratamento responsável são respondidas de acordo com as etapas e cronogramas do processo definidos.
Manter o inventário de atestado de dados pessoais	As leis de privacidade de dados de certas jurisdições exigem que um inventário de processamento de dados pessoais seja estabelecido e mantido. Isso é feito pelos LDPCs (Local Data Protection Contacts) evidenciando a verificação de completude e plausibilidade realizada com base em uma lista de verificação de pré-aprovação definida para cada inicial/reatestação.
Monitoramento ms&c de rescisão de clientes (KYC-03)	As equipes regionais da MS&C monitoram a conclusão dos relacionamentos comerciais encerrados devido a preocupações com AML ou KYC para detectar casos em que a aplicação da lei interna e/ou os requisitos regulatórios locais não foram atendidos. As amostras são selecionadas de acordo com o documento Ms&C Sampling Principles and Best Practices.

<b>Título</b>	<b>Descrição</b>
Monitoramento MS&C de Cliente on-boarding (KYC-01)	As equipes regionais da MS&C monitoram os procedimentos de integração de relacionamento comercial e classificação de risco para detectar casos em que a aplicação da lei interna e/ou os requisitos regulatórios locais não foram atendidos. Isso é feito por meio de uma revisão de amostra das relações comerciais. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais, se houver.
Monitoramento de MS&C de Manutenção KYC (KYC-02)	Documento de Princípios de Amostragem e Melhores Práticas da Ms&C. Quaisquer problemas ou exceções identificadas são escaladas para as partes interessadas relevantes. Os produtos e serviços oferecidos aos clientes também são monitorados para detectar casos em que não estejam alinhados com o perfil de risco do cliente. Se aplicável, as equipes regionais da MS&C monitoram os registros do cliente para detectar quaisquer casos em que eles não tenham sido mantidos.
Monitoramento ms&c de perfil e adequação do cliente (SU-03)	Isso é feito por meio de uma revisão de amostra das contas dos clientes para verificar se os perfis dos clientes são precisos. As amostras são selecionadas de acordo com o documento MS&C Sampling Principles and Best Practices. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas para investigação e ação adicionais, conforme apropriado.
Monitoramento de Distribuidores e Fornecedores de Produtos de Terceiros (SU-04)	As equipes regionais da MS&C monitoram a devida diligência e triagem de distribuidores de produtos UBS, bem como fornecedores terceirizados. Isso é feito por meio de uma revisão de amostra das revisões iniciais de due diligence. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais, se aplicável.
C&ORC GWM UBS Marketing Controle de produção de materiais	Cada site deve seguir uma das duas abordagens: a seguir a metodologia de seleção de materiais de marketing para revisão que já foi estabelecida no sistema/processo incorporado ou b a amostra aleatória de no mínimo 10 materiais de marketing (ou escopo completo se menos de 10 amostras estiverem disponíveis ) devem ser selecionados pelo menos anualmente. A remediação de todos os casos NOK identificados independentemente avaliados pelo C&ORC será liberado junto com o funcionário afetado.
Monitoramento de Conduta Transfronteiriço (CB-03)	As equipes regionais da MS&C monitoram as atividades da equipe-alvo para clientes com clientes em potencial/potenciais transfronteiriços para detectar quaisquer instâncias em que a conduta da equipe voltada para o cliente viole a Política Global Transfronteiriça. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais, se houver.
Monitoramento de Viagens Transfronteiriços da MS&C (CB-01)	As equipes regionais da MS&C monitoram as viagens internacionais dos funcionários voltados para o cliente. Isso é feito por meio da análise direta de uma amostra de aprovações de viagem do TRACT, documentação necessária do processo de viagem e/ou registros de despesas de viagem de negócios. Quaisquer problemas ou exceções identificadas são escaladas para as partes interessadas relevantes.

<b>Título</b>	<b>Descrição</b>
Monitoramento da MS&C de Conformidade Fiscal Transfronteiriço (CB-04 Passo 1)	As equipes regionais da MS&C revisam as atividades dos funcionários nas divisões de negócios GWM e P&C. Isso é feito para detectar casos em que o banco não aderiu a requisitos externos e/ou padrões internacionais relacionados ao status de conformidade fiscal dos clientes. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais.
Monitoramento da MS&C de Conformidade FATCA Transfronteiriço (CB-04 Passo 2)	As amostras são selecionadas de acordo com o documento MS&C Sampling Principles and Best Practices. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais, se houver. As amostras são escolhidas de acordo com os princípios MS & C Sampling e o documento de melhores práticas.
Monitoramento ms&c da adequação do produto (SU-02)	Uma revisão de amostra de produtos/serviços existentes para verificar se o produto/serviço e seus controles, divulgações e material de treinamento associados permanecem relevantes com o ambiente regulatório e de mercado atual. As amostras são selecionadas de acordo com os Princípios de Amostragem e Melhores Práticas da Ms&C. Quaisquer problemas ou exceções identificadas são escaladas para as partes interessadas relevantes.
Monitoramento de Induções/Comissões/Incentivos da MS&C (Col-03)	Isso é feito por meio de uma revisão de amostra de padrões e comportamentos para garantir que os incentivos, comissões e incentivos sejam operados de acordo com as políticas e regulamentações aplicáveis. Isso pode incluir a revisão do uso de produtos internos versus produtos proprietários, revisão da atividade em produtos de alta comissão ou revisão da adequação de acordos de taxas para clientes.
Revisão/atualização anual das principais orientações/documentos	Anualmente, todas as funções de C&ORC verificam se as principais orientações/documentos são revisados e atualizados. A revisão deve validar a integridade, precisão e atualizações, se necessário. Este controle não abrange as apólices do POLO. Existe um controle separado para atualizar os documentos-chave das políticas são aqueles documentos nos quais os negócios/funções dependem.
Revisão dos processos e controles relacionados ao licenciamento e registro de funcionários (Não-CUSO)	Trimestralmente, a pessoa responsável nas Américas da região não CUSO fornece evidências de que os processos e controles de autorização e registro de funcionários foram realizados no local. O não cumprimento desses controles pode resultar em pessoas fazendo negócios sem a devida autorização e podem estar sujeitas a multas, ações regulatórias e danos à reputação.
MS&C Monitoramento de Listagens de Sanções - Teste 1.1 (SA-01)	Cada região é responsável por cobrir diferentes listas de sanções, ou seja, Américas - OFCA, EMEA - UE, APAC - ONU, CH - SECO. As amostras são selecionadas de acordo com o documento MS&C Sampling Principles and Best Practices. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas para investigação e ação adicionais.
Rastreamento de Sanções da MS&C (SA-02)	Anualmente, as equipes regionais da MS&C examinam as partes relevantes em relação às listas de sanções aplicáveis e atualizadas. Isso é feito confirmando que o processo de triagem de verificações por meio do COSIMA é consistente com as políticas aplicáveis. Quaisquer problemas ou exceções identificados são encaminhados às partes interessadas relevantes para investigação e ação adicionais.

#### 6.4. Operações

<b>Título</b>	<b>Descrição</b>
Contas inativas e/ou dormentes GWM	A Gestão de Contas de Clientes Inativas e/ou Dormentes é importante para mitigar fraudes internas e externas, bem como garantir que os ativos do cliente estejam adequadamente protegidos dentro de diretrizes internas/externas.
EOD Control Framework - Revisão das avaliações de risco/distribuição de itens o/s para participação na EOD GWM	O objetivo fundamental do Quadro de Controle do Fim do Dia (EOD) é mitigar o risco de qualidade insuficiente dos dados transacionais.
Autorização e Autenticação SSI	O Documento de Padrões Mínimos SSI está em vigor para garantir que todas as Instruções de Liquidação Padrão (SSI's) e Instruções de Pagamento sejam autorizadas e autenticadas antes da execução, com controles de suporte para garantir que as informações confiadas permaneçam atualizadas
Reconciliações - Desempenho de Reconciliações e Quebra de Escalonamento GWM	As reconciliações são executadas por várias funções, cada uma das quais precisa garantir que as reconciliações que executam sejam realizadas de acordo com o propósito da reconciliação e a frequência acordada.
Gestão de Taxas e Comissões De Dados GWM	Toda a criação e alteração de dados de taxas e comissões deve vir de uma fonte autenticada aprovada para garantir que nenhuma reserva seja feita a corretores/contrapartes não aprovados, e onde as reservas são realizadas verificações de integridade sob medida.
Adesão aos procedimentos de Offboarding GWM	Toda a criação e alteração de dados de taxas e comissões deve vir de uma fonte autenticada aprovada para garantir que nenhuma reserva seja feita a corretores/contrapartes não aprovados, e onde as reservas são realizadas verificações de integridade sob medida.
Adesão à Política e Procedimentos fincrime GWM	Controle para garantir que clientes e não clientes sejam gerenciados através do processo do ciclo de vida do cliente, de acordo com as políticas do UBS FinCrime, procedimentos de conformidade e padrões relacionados.
Gwm de gerenciamento de aprovação do ciclo de vida do cliente	Aplicação de controle de 4 olhos, função de aprovadores autorizados e manutenção de listas de aprovadores Mensal Chefe Regional ou delegado clm (O) verifica que o princípio de 4 olhos aderiu a onde é exigido pelo procedimento.
Gerenciamento de SOP do ciclo de vida do cliente GWM	Procedimentos Operacionais Padrão (SOPs) detalhados, bem definidos e atualizados são importantes para manter o ambiente de controle e o desempenho dos processos.
Estrutura de Gerenciamento de Estoque, Governança e Controle dos Serviços do Ciclo de Vida do Cliente GWM	Este é um controle de asserção para garantir que todas as atualizações necessárias sejam incluídas em um inventário central, as reuniões de governança ocorram de acordo com os ToR definidos e a estrutura de controle seja eficiente e adequada ao objetivo. Este KPC aborda os seguintes Padrões Mínimos de Controle - detalhes desses padrões estão disponíveis.
Remediação da população cliente existente GWM	Este controle mantém auditoria e inventário de tarefas de remediação, seja realizada internamente ou por meio de um Controle de terceiros.

<b>Título</b>	<b>Descrição</b>
GWM de arquivamento e armazenamento	O controle é verificar se, durante o ciclo de vida do cliente, o conjunto completo de documentação do cliente foi capturado de acordo com a devida diligência de KYC/AML/Requisitos Regulamentares e Legais/Acordos Legais. O supervisor da equipe deve amostrar semanalmente para verificar se esta ação ocorreu. Este KPC aborda os seguintes Padrões Mínimos de Controle.
Relatório padrão - Confirma após a produção do relatório GWM	O UBS precisa garantir que os relatórios padrão do cliente (como declaração de ativos ou contas em dinheiro) sejam verificados para conteúdo, layout, cronograma de envio, completude e destinatário correto, independentemente de o relatório ser produzido automaticamente ou manualmente. As funções são responsáveis por determinar o escopo de controles necessários sobre o emissão de relatórios de clientes, a fim de mitigar cenários de risco específicos da função.
Completude e precisão de dados GWM	Este KPC aborda os seguintes Padrões Mínimos de Controle - detalhes desses padrões estão disponíveis. Ao longo do ciclo de vida do cliente, é necessário que o registro do cliente seja mantido com dados corretos e completos. Quando as exceções são identificadas, devem ser fornecidas evidências de que elas são escaladas, relatadas e resolvidas conforme prescrito no SOP. Quando necessário, tais violações/exceções devem ser relatadas nas reuniões de Risco relevantes.
Adesão aos requisitos regulatórios e legais GWM	Controle para verificar se os clientes são gerenciados através do processo de ciclo de vida do cliente, de acordo com os requisitos regulatórios e do UBS Legal, e normas relacionadas.
Am Middle Office - Entrada de pedido / transação agente de transferência de ordem GWM	O necessário para garantir que os pedidos de Fundo sejam colocados na ferramenta agente de transferência apropriado em tempo e precisão e que as confirmações comerciais sejam reportadas de volta ao gerente da carteira para novas ações.
Restrições e Sanções de Instrumentos Financeiros GWM	Regularmente (mínimo mensal), membros da equipe responsável pelos dados estáticos do instrumento garantem que todas as restrições e sanções necessárias estejam em vigor para os instrumentos financeiros adequados.
Gerenciamento de declarações de clientes definidas como GWM não despachante	A fim de mitigar o risco de fraude nas contas do cliente, e garantir que os clientes estejam cientes das informações mais recentes em torno do gerenciamento de suas contas O UBS precisa garantir que os clientes que não recebem declarações físicas sejam adequadamente gerenciados e que as ações necessárias para reduzir os níveis de risco tenham sido tomadas.
Gerenciamento de declarações de clientes enviadas a não clientes GWM	A fim de mitigar o risco de fraude nas contas e garantir que os clientes estejam cientes das informações mais recentes em torno do gerenciamento de suas contas O UBS precisa garantir que as declarações dos clientes enviadas a terceiros internos/externos sejam adequadamente gerenciadas.
Correspondência de instruções	Antes da data de valor, as operações devem gerenciar proativamente as negociações para garantir que o risco de compra e outras penalidades sejam mitigadas, e devem garantir que a pré-correspondência seja realizada de acordo com os SLAs acordados.

<b>Título</b>	<b>Descrição</b>
Revisão de supervisão para pagamentos de saída	o controle do processo de pagamento de saída para cada transação de pagamento que tenha sido digitada manualmente ou alterada manualmente.
Captura e validação de eventos de ação corporativa e renda	Para garantir que os dados do evento recebidos seja completo e preciso, é necessário revisar os dados contra outra fonte confiável e resolver quaisquer discrepâncias.
Capturar, autenticar e aprovar instruções de entrada e saída	Os eventos de Ação Corporativa devem ser totalmente conciliados para garantir que as posições sejam equilibradas e as eleições sejam processadas corretamente com base nas instruções recebidas.
Captura e conclusão das principais tarefas	As principais tarefas garantem que os eventos de ação corporativa e de renda sejam processados com precisão e tempo hápado e que os riscos associados ao processamento de eventos CAIP sejam adequadamente gerenciados e que quaisquer exceções sejam escaladas.
Notificação de eventos para stakeholders internos/externos	O não envio de notificações de eventos para clientes internos/externos em tempo hábil e preciso pode ter impacto de reputação ou P&L para o UBS.
Execução oportuna, reconciliação precisa e gerenciamento de quebra/exceções do CAIP	As posições sobre ações corporativas e eventos de renda devem ser totalmente conciliadas a tempo de garantir que os direitos sejam processados com precisão.
Alterações de Dados de Referência e revisões periódicas GWM	As equipes de Dados de Referência criam e alteram dados de referência mediante solicitação, que devem ser devidamente autorizados antes da execução.

## 6.5. Tecnologia

<b>Título</b>	<b>Descrição</b>
Cis-AC19 Downloads de WM CID de sistemas de informação são aprovados por IO(s) e protegidos	Os downloads de DADOS de Identificação de Clientes WM (CID) de sistemas de informação não são distribuídos no ambiente do usuário final ou em um ambiente de não produção, a menos que aprovado pelo (s) ou delegado do Proprietário de Informações.
Controle de versão CM9	Os artefatos CM9 liberados para produção são confirmados como aqueles que foram testados e aprovados.
Força de autenticação AC33	AC33 É implementado um mecanismo de autenticação para usuários humanos que fornece um nível de segurança adequado para a classificação dos requisitos de dados e integridade que estão sendo protegidos, conforme definido nos padrões da empresa.
Autenticação e autorização AC18 no Runtime	Ac18 Aplicativos e serviços impõem autenticação e verificam a autorização quando uma sessão é estabelecida, antes de conceder acesso a usuários humanos.
Proteção por senha RM7 em código	RM7 Antes da implantação no ambiente de produção, o código fonte ou binários são revisados e confirmados para não incluir senhas de texto claras.

<b>Título</b>	<b>Descrição</b>
Descrição de direitos e funções de acesso AC25	Os direitos de acesso AC25 são definidos para cada ativo de informação. Isso fornece direitos de acesso identificáveis que podem ser usados independentemente para gerenciar o acesso com granularidade suficiente, de acordo com os requisitos de negócios
Política de Senha e PIN AC17	AC17 Quando as senhas são usadas, os seguintes requisitos mínimos são aplicados para usuários humanos. Quando isso não for possível devido a limitações técnicas, a mitigação adequada é definida e implementada.
Implementação cm21 de requisitos mínimos de empresas e dependências arquitetonicas	CM21 O Gerente de Componentes de Software (SWCM) identifica os Requisitos Mínimos de Empresas (MERs) e as Dependências Arquitetonicas (ADs) relevantes para um aplicativo, respondendo com precisão as perguntas do gatilho MER & AD dentro da ferramenta De avaliação de requisitos corporativos de software (SERA) (caso contrário, todos os MERs e ADs do catálogo MER & AD são considerados aplicáveis a um aplicativo)
Segregação CM13 de Deveres na Gestão de Mudanças via Acesso à Infraestrutura	Os direitos cm13 para alterar o ambiente de produção são segregados para reduzir oportunidades de modificação ou uso indevido não autorizados dos ativos da empresa.
Alocação de direitos de acesso AC11	AC11 Os direitos de acesso para usuários humanos não são concedidos a menos que devidamente aprovados para impedir o acesso não autorizado.
Ac12 Desativação de Contas Leaver	O acesso à conta AC12 é desativado para os que saem mediante o recebimento da notificação de rescisão do RH.
Integridade de Backup BR12	Dados e aplicativos relevantes, restaurações de sistemas são realizadas pelo menos anualmente para confirmar que os backups podem ser restaurados com sucesso.
AC4 Identificação exclusiva do usuário humano	As identidades digitais AC4 são claramente identificáveis e atribuíveis a um único usuário humano, por exemplo, pessoas ou clientes do UBS.
O28 Secure Disposal ou Reutilização de Equipamentos	As mídias de armazenamento O28 são apagadas antes de reutilizar ou serem destruídas com segurança de acordo com os padrões da empresa para evitar vazamento de dados.
Monitoramento da capacidade de infraestrutura do CP7	Os requisitos de utilização da capacidade do CP7 e os limites associados são documentados dentro dos padrões aprovados (infraestrutura/aplicação técnica/monitoramento e revisados pelo menos anualmente.
Contas técnicas não personalizadas ac5	As contas técnicas não pessoais do AC5 (por exemplo, contas de serviço, comunicação, aplicativo e banco de dados) são mapeadas para o aplicativo ou serviço relevante e atribuídas ao respectivo proprietário. Configurado com segurança para impedir o acesso não autorizado usando o mecanismo mais forte possível para: (i) impedir o login interativo, (ii) autenticar o certificado ou (iii) aplicar uma política de senha forte.
Segregação cm31 de deveres na gestão de mudanças via acesso a aplicativos	Os direitos cm31 para alterar o ambiente de produção são segregados para reduzir oportunidades de modificação ou uso indevido não autorizados dos ativos da empresa.



<b>Título</b>	<b>Descrição</b>
Remoção do direito do motor ac16	AC16 Quando um membro da equipe muda de função ou responsabilidades, todo acesso sensível é automaticamente revogado ou revisado dentro de prazos acordados com representantes empresariais para confirmar que os direitos permanecem apropriados para sua função profissional e direitos redundantes são removidos.
Metas de nível de serviço SO11 - Aplicações	As Metas de Nível de Serviço (SLTs) estão em vigor para todos os aplicativos no escopo, (Aplicável às aplicações das classificações BCM Tier 1, 2 & 3 ) e são revisadas anualmente para garantir que elas permaneçam apropriadas.
Teste de alterações do CM6	As alterações cm6 são testadas antes de promovê-las ao ambiente de produção.
Gerenciamento de Credenciais AC10	As credenciais de identidade AC10 (por exemplo, senhas, PINs, smartcards) são gerenciadas de forma segura, incluindo solicitação, criação e distribuição.

## 6.6. Controle de Riscos

<b>Título</b>	<b>Descrição</b>
Controle sobre ativos financeiros aflitos	Trata-se de um processo de controle incorporado realizado no dia a dia, o ex-pós-teste baseado em amostra será realizado periodicamente pelas equipes CRO GWM de locais relevantes do CRO GWM.
Controle sobre avaliações colaterais com valores de preço de entrada manual	Este teste de ex-postes baseado em amostra em um processo diário de BAU embutido será realizado periodicamente por equipes [OMS] CRO GWM de locais relevantes do CRO GWM (onde as respectivas funções estão sob a responsabilidade das equipes de CRC CRO GWM) para verificar, com base em políticas que regem tais garantias, a avaliação das garantias é precisa e atualizada como refletido no sistema de registros relevante, usando uma visão instantânea de garantias ao vivo como no final de cada período de avaliação KPCi definido.
Controle sobre gestão de déficits de colaterais	Trata-se de um processo de controle incorporado realizado no dia a dia, o ex-pós-teste baseado em amostras será realizado periodicamente pelas equipes CRO GWM de locais relevantes do CRO GWM (onde as respectivas funções estão sob responsabilidade das equipes cro GWM).
Controle sobre a adesão ao processo de escalonamento da Revisão de Risco Vencido	Um processo de controle incorporado realizado no dia a dia, o ex-pós-teste baseado em amostras será realizado periodicamente pelas equipes CRO GWM de locais relevantes do CRO GWM.
Controle dos valores de empréstimo específicos do cliente definidos manualmente no sistema local	Equipe de controle de risco local mensalmente para realizar uma avaliação completa de que todos os Diretores de Crédito.
Alterações de modelo são revisadas e aprovadas antes de entrar no ar	O KPC mitiga o risco de alterações de modelo (MCs) não seguirem a governança do modelo apropriada antes do go-live (conforme 1-P-001997).

<b>Título</b>	<b>Descrição</b>
Desenvolvimento e Documentação do Modelo - Pré-revisão e Aprovação do Proprietário do Modelo	Esse controle reduz o risco de que o desenvolvimento de 1 modelo e a documentação do modelo (MD) se desviem de 1-P-001997 e suas diretrizes de suporte. Quando um modelo é enviado para validação inicial, revalidação regular ou revisão de alteração de modelo de material, o proprietário do modelo verifica se o pacote de remessa está completo na cobertura do MD.
Monitoramento de desempenho do modelo e relatórios de violação	O controle mitiga o risco de o fraco desempenho do modelo não ser detectado, o que pode, por exemplo, levar a modelos sendo usados com problemas de desempenho não identificados e não resolvidos.

## 6.7. Área de Riscos do Negócio

<b>Título</b>	<b>Descrição</b>
A00 - CIO IO-FGC-03: Independência de outras unidades bancárias	Parcialmente um controle de segundo nível - Em uma base anual, a CIO IO Business Risk Organization e o RH (em CH) fazem uma verificação para detectar potencial não adesão às normas regulamentares quanto à independência da função de pesquisa
CIO-Loc-BR_MX - Revisão das contas	O executor de controle (i) verifica trimestralmente todas as contas de um membro das áreas no âmbito do controle que estas são identificadas, atualizadas e ainda necessárias.
CIO-Loc-BR_MX - IGC-4.5 Verificar banco de dados da estrutura legal e as aprovações e evidências necessárias	O controle do IPS: Legal Structure Database (LSDB) inclui verificações: mensais, semestrais e anuais.
CIO-Loc-BR_MX - IGC-6.3 Revisão regular da documentação do produto	O executor de controle verifica pelo menos anualmente se a documentação do produto disponibilizada através dos canais apropriados para a equipe voltada para o cliente é atualizada e completa.
CIO-Loc-BR_MX - Revisão regular do processo de vida do produto IGC-0009	O executor de controle verifica pelo menos anualmente se os produtos e serviços oferecidos ativamente aos clientes ainda estão em conformidade com o projeto de produto aprovado, processos relacionados e estrutura de controle aplicável. O executor de controle também verifica se os preços são avaliados e revisados regularmente de acordo com os padrões definidos na Política Global de Gestão de Preços.
CIO-Loc-BR - Processo de aprovação do Fundo de Revisão	O executor de controle verifica trimestralmente, no primeiro mês do trimestre, que os fundos aprovados pelo comitê do fundo foram sujeitos à triagem, due diligence e aprovação adequadas.
CIO-Loc-BR_MX - Verificação de Conformidade de Material de Marketing	Esse controle verifica se o material de marketing está em consonância com a política de material de marketing (toda comunicação que visa promover produtos e serviços UBS e/ou específicos UBS para seus clientes e/ou cliente em potencial).

<b>Título</b>	<b>Descrição</b>
CIO-Loc-BR - Adesão de Modelos a limites de alocação de ativos, risco de emissor, limites de VAR e Vola	Sujeito a especificidades locais e sistemas locais, o executor de controle verifica a adesão de modelos aos limites de alocação de ativos e, quando aplicável, o risco do emissor, os limites de Valor-em-Risco e Volatilidade .
CIO-Loc-BR_MX- Adesão às instruções do cliente	Sujeito a especificidades locais e sistemas locais, o executor de controle verifica as instruções do cliente são cumpridas em respectivos mandatos de investimento
CIO-Loc-BR_MX - IGC- 6.1 Aprovações de novas iniciativas de negócios e mudanças nos negócios existentes	Conciliação trimestral de produtos e serviços recém lançados e alterados com inventário na NBC (ou equivalente local) de acordo com o política interna
gKPC-106.02: Mudanças na estrutura da conta	O UBS deve anualmente ter procedimentos em vigor para garantir por meio de revisão que, a documentação do CLIENTE KYC esteja completa, assim como a classificação de risco as alterações em PoAs e/ou BOs (incluindo recém-adicionados) sigam a devida diligência.
Registros eletrônicos de implementação de gerenciamento de registros	Esse controle visa mitigar anualmente o risco das Funções de Divisão de Negócios/Grupo (BD/GF), cuja materialização do risco ocorre via o não cumprimento dos requisitos da 'Política de Gerenciamento de Registros (RMP) 1-P-001004" e do Modelo Operacional RM
gKPC-111.01 GWM P&C Finders	Esse controle visa mitigar o risco relacionado a suborno, corrupção, conflitos de interesse, violação de leis específicas locais sobre Finders, relações comerciais indesejadas levando ao risco de reputação. Desta forma o mesmo consiste em garantir a conformidade da gestão das relações com a GWM e a P&C Finder, com os padrões globais definidos na Política de Localizadores GWM P&C (2-P-000615).
CIO-Loc-BR_MX - Revisão periódica dos fundos aprovados	Esse controle visa verifica anualmente no BCCH que o monitoramento dos fundos aprovados é realizado de acordo com as normas globais de Gerenciamento de Conteúdo IM.
Revisão mensal do inventário de gravação de voz	Esse controle mitiga o risco de violação de requisitos regulatórios internos e aplicáveis para registrar comunicações de voz identificados na Ferramenta de Inventário de Gravação de Voz (VRIT).
gKPC 100.01: Verificação de conformidade AEI/FATCA	Para cumprir as regras e regulamentos da AEI/FATCA, é necessário manter as respectivas políticas, procedimentos operacionais, controles e revisões regulares, bem como as evidências da execução de tais controles, estabelecidos para garantir o cumprimento dos requisitos da UE DAC6/MDR
CIO-Loc-BR - Implementação de mudanças de modelo em mandatos de investimento	Este controle visa verificar se os mandatos são investidos de acordo com os modelos
OKC 202.12 Empresa Domiciliar/Não-Operacional - Validação da Folha de Decisão	Esse controle tem como objetivo verificar em periodicidade trimestral a classificação de clientes/investidores estão de acordo com as normas de FATCA.

<b>Título</b>	<b>Descrição</b>
Manter controles de saída de bloco antifraude? Equipe Sensível	Esse controle é utilizado para monitorar a conformidade com a Política Global de Licença de Bloco em uma base regular e oportuna, para garantir que a população de funcionários sensíveis seja revista e aprovada pelo menos anual
Customer Reporting & Mailing Control Point 4: Entrega forçada de fim de ano	O controle de "Retained Mail" deve ser assegurar a retenção de correio eletrônico que apresentem informações incorretas ou com erros de transação e problemas de adequação. A LRU identifica a exceção concedida ao nível do cliente e confirma as Operações para posteriormente liberar para envio.
OKC 208.03: Verificação do deputado da CA	O UBS atribui a responsabilidade do deputado a cada cliente, para controle desse processo, anualmente o deputado da CA verifica se um deputado válido da CA é designado onde há indícios de que não há nenhum deputado válido .
gKPC 107.06: Relatórios e Correspondências de Clientes	Esse controle tem como objetivo mitigar o risco de que o cliente não seja informado no devido tempo e, portanto, não pode detectar erros ou atividades não autorizadas em suas contas.
OKC 202.07: Revisão de conta adormecida	O controle de revisão de Contas Dormentes, mitiga o risco de uso indevido de fundos de contas inativas/sem contato.
gKPC 107.17: Adesão aos preços de lista	Esse controle é realizado para garantir que os clientes não sejam sobrecarregados quando comparados aos horários de preços divulgados pelo cliente, devido a mau comportamento ou problemas sistemáticos.
OKC-207.16: Controle trx de mudança de substâncias	Esse controle visa manter e, conformidade com as normas divisionais definidas na política de Tratamento de Pedidos de Clientes (2-P-001355) a fim de gerenciar os riscos envolvidos na divulgação de informações confidenciais.
IPS-IGC-Melhor Execução KPC	Esse controle estabelecido pela Gerencia de Serviços de Execução e as equipes correspondentes ,) verificarão continuamente se todas as negociações são executadas de acordo com os princípios de Melhor Execução (BEX), conforme definido na "Política Global de Execução de Pedidos para Transação de Compra/Venda (2-P-005273) ou quaisquer políticas locais correspondentes.
4.08: Extensão de controle e revisão de supervisão remota	Esse controle baseia-se na Política de Supervisão do Grupo que exige que, quando alguém é supervisionado remotamente, um supervisor local deve ser nomeado e registrado. Caso contrário, uma exceção deve ser notada e aprovada pelo comitê superior relevante da MGMT. As medidas apropriadas, conforme detalhado nos padrões mínimos do GWM para supervisão remota, devem ser tomadas para garantir uma supervisão remota eficaz
Informações gerenciais para chefes de mesa	Esse controle tem como objetivo a avaliação sobre se o MI relevante para chefes de mesa está disponível e acessível e se os mesmos estão sendo reportados no Comitê de Risco Local (ou outro comitê de gerenciamento sênior local relevante).
gKPC-102.04: Verificação de consistência da documentação do cliente NTBR	Esse controle visa mitigar o risco relacionado a realização de operações de NTBR com clientes, que não se qualificam no apetite que risco aprovado pelo UBS Brasil
gKPC 102.02: Documentação Obrigatória Ausente	Esse controle objetiva o atendimento dos requisitos legais estabelecidos por reguladores referente ao processo de obtenção e manutenção da documentação atualizada e completa do cliente (KYC).

<b>Título</b>	<b>Descrição</b>
gKPC 102.03 Alteração de dados estáticos do cliente	Esse controle tem como objetivo a validação das alterações estáticas dos dados do cliente. Ele determina que o processo deve estar em conformidade com a política de manipulação de pedidos do cliente (2-P-001355).
gKPC 102.01: Processo de revisão kyc (PKR)	Esse controle estabelece que o O UBS deve documentar o conhecimento das relações comerciais, a fim de gerenciar os clientes de acordo com as normas locais (internas e externas) de lavagem de dinheiro e ao financiamento do terrorismo.
gKPC 104.04: Revisão do KPC de adequação do OCF	O controle é realizado trimestralmente, e verifica a adesão da equipe Front Office para manter informações corretas de risco do cliente e monitorar regularmente as carteiras dos clientes e sua correspondência com a preferência de risco/retorno do cliente, objetivos de investimento e conhecimento e experiênci
gKPC 104.01: OCF Suitability KPC Entenda	Esse controle tem como objetivo verificar a adesão da equipe da Front para manter completude e atualização de classificação de IP de clientes. Importante ressaltar que, esse controle só é aplicável se a regulação local permitir a classificação profissional dos clientes
Dac Onboarding Control Point 3 & 5: Revalidar ordem no perfil de risco e classificação do cliente	Esse controle consiste na execução de uma "due diligence" para novos cliente. O evento de controle é desencadeado no Processo de Onboarding OCF 21-DAC.
gKPC 104.03: OCF Suitability KPC Agree & Implement	Esse controle consiste adesão aos requisitos de adequação do MiFID relacionados à política de Suitability pela equipe Front Office.
gKPC 104.02: OCF Suitability KPC Propose	Esse controle tem como objetivo verificar se a equipe de produtos de investimento, realizou as verificações necessárias para operações envolvendo clientes com restrições especiais.
gKPC 110.01 Reclamações de clientes	Esse controle tem como objetivo verificar se a Unidade de Tratamento de Reclamações (CHU) realizou as verificações necessárias para registro, direcionamento e escalonamento das reclamações de prestação de serviços.
OKC 200.10: PAR ex-post Control	O controle visa apoiar o cumprimento das transações de compra de valores mobiliários e fundos com as Regras de Alinhamento de Produtos (PAR), o UBS CoCo Ban e a Diretiva de Gestores de Fundos de Investimento Alternativo da EEE para transações (AIFMD)
OKC 200.14: Revisão Especial da População	Esse controle visa dar transparência ao BRO e ao Lead Market Head sobre os clientes que se qualificam como relacionamentos com pessoas nos EUA, clientes que estão nos Mercados de Rescisão e forçam a população de clientes de países centralizados e verifica a correção das isenções fornecidas
OKC 200.08: Controle de isenção de SIs transfronteiriços	O controle faz parte do processo OCF 08-Cross-Border max. 5 Processo de Isenção de SIs. Originação - F2B e verifica CAs, DH ou LM de DH cobrindo mais de 5 SI (ou domicílios do cliente, dependendo da configuração de controle local
OKC 200.12: Conformidade Fiscal de Abertura de Conta	O controle faz parte do processo OCF 08_Cross-border Fiscal Compliance. Originação - Funcional e visa obtenção de evidências suficientes sobre a divulgação de impostos na abertura de conta dos cliente

<b>Título</b>	<b>Descrição</b>
gKPC 100.02: Verificação de conformidade com a política de pessoas dos EUA	OCF 08-Cross-Border. Originação - F2B. Para apoiar o cumprimento do marco regulatório de pessoas dos EUA (Política de Pessoas dos EUA (2-P-003039)) e a oferta de serviços a clientes de pessoas físicas dos EUA, o UBS é obrigado a manter as respectivas políticas, procedimentos operacionais, controles, revisões regulares, bem como evidências de tais.
OKC 200.03: Atividade do Centro de Reservas Transfronteiriço	A comunicação entre os clientes de países diferentes deve estar em consonância com a política de clientes não residentes, as IS países diferentes aplicáveis e a Política de Pessoa dos EUA e documentadas dentro do apetite de risco para evitar multas regulatórias resultantes de possíveis violações
OKC 200.04: Verificação da amostra de viagem transfronteiriço material	O controle faz parte do processo OCF 08-Cross-Border Travel. Originação - F2B, onde as viagens relacionadas a clientes/prospect e 3ª partes/ prestadores de serviços devem estar de acordo com a política do UBS e regulamentos externos.
Revisão dos casos do Programa de Colaboração GWM	O controle é realizado semestralmente por uma unidade segregada. Ele é somado ao processo OKC 200.03 e OCF 08- Comunicação Remota Transfronteiriço e tem por finalidade examina as atividades descritas em notas de contato em contas com um Contrato de Colaboração ativo por um período de controle de 6 meses que foram identificados como contatos com clientes e transações realizadas na conta.
OKC 207.15: Verificação da grade da Autoridade de Preços	O controle faz parte do processo OCF 19_Client Manutenção de Relacionamento. Originação - Funcional. Os pedidos de descontos de preços (ou seja, preços abaixo do cronograma padrão de taxas) estão sujeitos a aprovações de acordo com a grade da autoridade de preços para gerenciar riscos operacionais e comerciais associados (ou seja, conflito de interesses, uso indevido de reduções de preços) e garantir a supervisão adequada.
OKC 209.01: Verificação de proteção de dados prospect	O controle faz parte do processo OCF 17-Data Protection. Originação - Funcional. Este controle verifica a adesão às regras e regulamentos aplicáveis sobre a aquisição de prospects e prospecting de armazenamento de dados e garante que não há violação da regulamentação no mercado doméstico
Verificação de dados pessoais confidenciais	Esse controle garante que não haja violação da Política de Proteção de Dados do Grupo (1-P-001061) no que diz respeito ao processamento de categorias sensíveis ou especiais de dados pessoais
OKC 202.10: Verificação de isenção de indenização	O controle faz parte do processo OCF processo OCF 19_Client Manutenção de Relacionamento. Originação - Funcional. A aceitação das instruções de ordem enviadas através de canal de comunicação não assegurado (por exemplo, e-mail, fax, telefone) requer uma renúncia indenizatória assinada por um cliente.
TPRM-IEO-01 Afirmação Anual de Conformidade IEO	Esse controle visa identificar o risco de potencial de não conformidade com os requisitos regulatórios locais para terceirização inter-entidade.

## 7. Aprovação, Vigência e Revisão

A Diretoria de Compliance & *Operational Risk Controle (C&ORC)* é a responsável por este Manual e deverá supervisionar e controlar os processos relativos ao planejamento, manutenção e revisão deste documento sempre que se fizer necessário.

Este manual entra em vigor na data de sua aprovação e deve ser revisada anualmente ou a qualquer momento, caso quaisquer das matérias aqui tratadas sofra alguma alteração.