Política CAAML Março 2019

Nome	Política CAAML
Referência	*CAAML Policy* (AIM No. 102-20-20, 31/07/2018)
Aplicabilidade	Todos os Empregados do AAB Brasil
Data de Início	02/06/2014
Revisado por Compliance em	13/03/2019
Aprovado pelo BREC em	18/03/2019
Versão	V.05

1 Introdução

A presente Política de Aceitação de Clientes, Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo ("Política CAAML") vem traduzir e adaptar a *Client Acceptance and Anti Money-Laundering Policy* do ABN AMRO Bank N.V. ("AAB Holanda") à natureza, complexidade e risco das operações do Banco ABN AMRO S.A. ("AAB Brasil"). A Política CAAML também respeita, no que se aplica: (a) a legislação brasileira; e (b) os normativos emitidos pelo Conselho Monetário Nacional ("CMN"), Banco Central do Brasil ("BCB") e Comissão de Valores Mobiliários ("CVM"). Em caso de conflito entre esta Política CAAML e as legislações e regulamentações aplicáveis, prevalecerá o padrão mais rigoroso e conservador, desde que não infrinja a legislação pertinente.

A Política CAAML é revisada periodicamente pelo Departamento de Compliance do AAB Brasil ("Compliance"). Eventuais atualizações são levadas ao Comitê Executivo (*Diretoria Executiva*, ou "BREC") e/ou ao Comitê de Auditoria, Regulatório e Compliance ("BRARCC"), conforme o caso, para análise, discussão e aprovação. A Política CAAML deve receber ampla divulgação interna no AAB Brasil, bem como ser aprovada pelas instâncias competentes, de acordo com a regulamentação aplicável.

1.1 Proteção da Integridade do AAB Brasil

Os valores institucionais AAB Brasil – confiança, profissionalismo e ambição – são os pilares que sustentam esta Política CAAML. A proteção da integridade do banco é um pré-requisito e um princípio soberano em todos os negócios em que o banco atua. O BREC declara, através da assinatura desta Política CAAML que:

"*Um dos objetivos do BREC é manter e proteger a reputação do Grupo ABN AMRO no Brasil a todo tempo, bem como não permitir que a confiança depositada pelos clientes na integridade do banco seja afetada de alguma forma. O BREC considera qualquer tentativa de lavagem de dinheiro uma ameaça a essa confiança e envida todos os esforços necessários para prevenir que o sistema financeiro nacional seja utilizado para fins ilícitos. O BREC não aceita que o banco comece nenhuma relação comercial com um (potencial) cliente caso suspeite, ou tenha algum tipo de conhecimento, que os recursos de tal cliente sejam provenientes de atividades ilegais; ou as operações do banco serão utilizadas para fins ilícitos.*"

A reputação é um ativo comercial intangível e importante para o AAB Brasil. Os riscos que afetam negativamente a reputação dos bancos aumentaram consideravelmente na última

década. Um dos principais riscos à reputação dos bancos é o risco de um banco ser envolvido com, ou ser tornar um veículo para, atividades ilícitas, tais como: lavagem de dinheiro ("LD"), financiamento do terrorismo ("FT"), fraude e corrupção. Muitos produtos e serviços oferecidos pelo AAB Brasil podem atrair pessoas com a intenção de usar o sistema financeiro para fins ilícitos.

O BREC está comprometido em prevenir que o AAB Brasil se envolva em atividades com clientes que possam vir a prejudicar sua boa reputação. Uma atitude importante para mitigar tais riscos é garantir que o AAB Brasil realize negócios apenas com clientes idôneos. Para tanto, o banco deve possuir políticas e procedimentos adequados para prevenir atividades ilícitas.

Esta Política CAAML garante: (a) atenção e dedicação necessárias a cada cliente, a fim de se estabelecer se o banco quer (ou não) fazer negócios com tal cliente; e (b) que os clientes do banco possuam boa reputação. Deve-se observar que a aceitação do cliente também inclui aspectos não abrangidos por esta Política CAAML, particularmente aspectos de sustentabilidade.

Tal como inserido na definição de "Risco Reputacional" descrita no item 3.1 abaixo, a Primeira Linha de Defesa é responsável pela proteção da reputação e da integridade do banco no contexto geral desta Política CAAML.

O BREC nomeou o Diretor Executivo responsável pelo Compliance (*Compliance Country Head*, ou "CCH") para: (a) ser o responsável pelas atividades de prevenção à LD ("PLD"), combate ao FT ("CFT") e sanções globais (*Chief AML/CFT Officer*, ou "Diretor de PLD/CFT"); e (b) monitorar continuamente o cumprimento de todos os procedimentos de PLD/CFT no AAB Brasil, conforme estabelecido nesta Política CAAML. O Diretor de PLD/CFT é o responsável final por todas as questões de PLD/CTF, incluindo o relacionamento do AAB Brasil com as autoridades de supervisão e a elaboração e/ou supervisão de relatórios internos. Caso sejam pessoas diferentes, o Diretor de PLD/CFT se reportará ao CCH. Porém, para o fiel exercício da sua função, o Diretor de PLD/CFT terá sempre acesso independente e direto ao BREC.

1.2 Lavagem de Dinheiro e Financiamento do Terrorismo

Em linhas gerais, para os fins desta Política CAAML, LD é a introdução ao sistema financeiro de ativos provenientes de atos ilícitos a fim de ocultar ou disfarçar sua verdadeira origem. A origem de recursos obtidos ilegalmente pode ser ocultada por meio de uma série de transferências e operações. O objetivo de tais transferências e operações serve para que tais recursos possam eventualmente reaparecer no sistema como uma receita legítima. O FT pode ser qualquer apoio financeiro, encorajamento, planejamento e qualquer forma envolvimento de uma pessoa com o terrorismo. A característica comum entre LD e FT é a tentativa de ocultação.

2 Escopo e Aplicabilidade

2.1 A Política CAAML é para Todos

O sucesso do AAB Brasil no cumprimento desta Política CAAML depende da cooperação de todos os funcionários. Todos precisam estar atentos e ser prudentes tanto na aceitação de novos clientes, quanto ao lidar com pedidos e operações de clientes existentes. Somente com o comprometimento e dedicação de todos será possível: (a) traduzir o espírito e valores do Grupo ABN AMRO para o dia-a-dia do banco: (b) continuar a proteger a integridade do sistema financeiro nacional; (c) manter a reputação do banco como respeitável e confiável.

Todos os funcionários do AAB Brasil, independentemente do nível hierárquico, devem compreender a relevância, seu significado e agir sempre de acordo com esta Política CAAML. Não somente com o que está escrito na política, mas de acordo com o seu espírito e em linha com os valores do Grupo ABN AMRO.

2.2 Onde aplicar a Política CAAML

A Política CAAML aplica-se a todas as linhas de negócios do AAB Brasil.

2.3 Quando a Política CAAML se aplica

A Política CAAML se aplica quando:

- o AAB Brasil pretender estabelecer uma "relação comercial" com alguém e seus atos posteriores. Uma relação comercial significa uma relação com um cliente, de negócios, bancária, profissional e/ou comercial que, desde o momento que o primeiro contato é feito, é esperado que um elemento de continuidade seja estabelecido.
- o AAB Brasil realizar operações eventuais para pessoas jurídicas, com as quais não tem e não pretende estabelecer nenhuma relação comercial:
    - em um montante igual ou superior ao equivalente em Reais a EUR 15.000 (quinze mil Euros), em uma única operação ou em um conjunto de operações que pareçam interligadas;
    - que constitui uma transferência de recursos em um montante superior ao equivalente em Reais a EUR 1.000 (um mil euros). Transferência de recursos significa qualquer operação realizada, pelo menos parcialmente, por meios eletrônicos em nome de um pagador (originador) para disponibilizar fundos para um beneficiário (ou seja, transferência bancária);
    - para uma pessoa (jurídica) residente e domiciliada em um país de Alto Risco, tal como definido nas Classificações de Risco de Crime Financeiro por País do AAB Holanda (*Country Financial Crime Risk Ratings*), independentemente do montante envolvido;
- há suspeita de LD ou FT, independentemente de outras circunstâncias;
- Existem dúvidas quanto à veracidade ou adequação dos dados de identificação de cliente obtidos anteriormente.

2.4 Procedimento de Avaliação de Risco Operacional – Vulnerabilidade dos Produtos

Novos (ou alterados materialmente) produtos e/ou serviços oferecidos pelo banco devem estar em conformidade com esta Política CAAML. A vulnerabilidade de produtos e/ou serviços à LD/FT deve ser avaliada de acordo com os processos internos do AAB brasil para a aprovação de riscos operacionais, jurídicos e reputacionais. Para tanto, vide a Política de Aprovação de Produtos.

2.5 Alinhamento das Linhas de Negócios

Esta Política CAAML cria um programa consolidado de gerenciamento de risco de LD/FT com a coordenação centralizada no Compliance. Tal centralização permite políticas e procedimentos padronizados sejam totalmente adotados por todas as linha de negócios.

Cada linha de negócios deve garantir sua conformidade com esta Política CAAML, bem como incorporar seus termos em seus processos internos e estruturas. Dadas as particularidades de cada linha de negócios (segmentos de cliente, focos de mercado, localizações geográficas, produtos etc.), a implantação de processos internos deve ser, de certa forma, diferente umas das outras. Porém, não poderão diminuir as exigências contidas nas políticas do Grupo ABN AMRO.

Todas as entidades do Grupo ABN AMRO (AAB Brasil, inclusive) devem garantir o alinhamento desses procedimentos nas suas diferentes linhas de negócios e, em caso de dúvidas, devem contatar o Compliance.

2.6 Responsabilidades

- **BREC.** O BREC deve proteger e promover a estabilidade, transparência e confiabilidade do Grupo ABN AMRO no Brasil e assegurar que a estrutura de PLD/CFT do banco esteja em linha com: (a) a Análise Sistemática de Riscos de Integridade (*Systematic Integrity Risk Analysis*, ou "SIRA"); e (b) o apetite do banco por esses riscos (Risk Appetite Statement, ou "RAS"). Consulte o item 4.3 para obter mais informações sobre a SIRA;

- **Gestores das Linhas de Negócios (*Business Line Management*).** os gestores são responsáveis pela implementação desta Política CAAML em suas respectivas linhas de negócio, levando em consideração os resultados de avaliações periódicas de risco, tais como o SIRA. Além disso, os gestores são responsáveis por: (a) garantir o comprometimento e treinamento das suas equipes; (b) enfatizar as consequências (individuais e para o banco) do não cumprimento desta Política CAAML; (c) determinar e comunicar funções e responsabilidades dentro das equipes; (d) fortalecer a "parceria" com o Compliance; e (e) manter a responsabilidade final em caso de terceirização de funções (internas ou externas). Os gestores das linhas de negócios no AAB Brasil também são responsáveis por garantir que os clientes de Alto Risco (*Increased Risk*) sejam revisados e aprovados por uma pessoa sênior previamente nomeada. Os gestores das linhas de negócio precisam garantir que tais pessoas tenham um nível suficiente de conhecimento dos riscos de PLD/CFT do banco; e senioridade suficiente para tomar decisões que afetem a exposição do banco a este risco;

- **Compliance. (a) CCH.** atuando como Diretor de PLD/CFT, o CCH é responsável pelo monitoramento contínuo do cumprimento de todas as regras e deveres de PLD/CFT do banco. O Diretor de PLD/CFT também é responsável pelo desenvolvimento e aprovação dos padrões globais do grupo referenciados nesta Política CAAML. Adicionalmente, o CCH é responsável por auxiliar as linhas de negócios na implementação desta Política CAAML, bem como por todos os relatórios e reportes, incluindo Relatórios de Atividades Suspeitas (*Suspicious Activity Reports*, ou "SARs") para as autoridades competentes. O CCH, quando solicitado pelo BCB ou por qualquer outo supervisor, pode atuar como Diretor de Prevenção à Lavagem de Dinheiro (*Money Laundering Reporting Officer*, ou "MLRO"), ou uma função regulatória equivalente; e **(b) CO.** cada gerente ou analista de Compliance (*Compliance Officer*, ou "CO") é responsável por auxiliar as linhas de negócios no desenvolvimento e manutenção de procedimentos e treinamentos adequados de PLD/CFT, respondendo à dúvidas diárias e analisando e aconselhando sobre clientes de Alto Risco. Além disso, o CCH e/ou o CO, conforme o caso, monitora a efetividade dos procedimentos de PLD/CFT e reporta os resultados ao BRARCC;

- **SIM.** a Função de Gerenciamento de Integridade & Segurança do AAB Brasil (*Security & Integrity Management*, ou "SIM") é uma função independente dentro de Compliance. O SIM atua em casos de abuso do sistema financeiro e que possam envolver perdas financeiras devido à atividades criminosas internas de empregados e/ou externas de clientes. O Centro de Inteligência de SIM (*SIM Intelligence Center*), através de fontes e sistemas internos e externos, fornece treinamento e análise detalhados de operações e clientes. SIM pode ser envolvido em um caso pela solicitação de uma linha de negócios ou pelo CO para orientar nos casos em que, com base em fatos e/ou circunstâncias, a presença de tais riscos seja evidente ou suspeita. A expertise de SIM pode ser usada para uma análise mais detalhada dos riscos associados. O CO/MLRO pode ser responsável pela comunicação de operações incomuns/suspeitas no banco e pela apresentação dos relatórios SAR para as autoridades, em nome do Diretor de PLD/CTF. Adicionalmente, o CO/MLRO poder ficar com a responsabilidade de troca de inteligências sobre PLD/CFT, conforme especificado pelo Diretor de PLD/CTF; e

- **Auditoria Interna (*Group Audit*).** a Auditoria Interna reporta-se de forma independente ao BREC. Como parte de suas responsabilidades, a Auditoria Interna realiza, periodicamente, testes e avaliações independentes nos controles do AAB brasil, a fim de avaliar a implementação e a subsequente aderência às políticas e procedimentos descritos nesta Política CAAML. Sua função com relação a esta Política CAAML inclui o

desenvolvimento de um Plano Anual de auditoria, além de identificar riscos de LD/FT, testar e avaliar periodicamente controles internos e os programas de PLD/CFT, garantindo consistência nas revisões do banco como um todo, e efetuar reportes periódicos. A Auditoria Interna também acompanha a resolução dos apontamentos anteriores. Vide o Mandado da Auditoria Interna (*Group Audit Mandate*).

2.7 Delegação de Deveres e Responsabilidades

Em linhas gerais, a delegação de deveres e tarefas nesta Polícia CAAML é possível. No entanto, as responsabilidades permanecem conforme definido nesta Política e, portanto, requerem um certo grau de envolvimento de todas as partes.

2.8 Titularidade de Cliente

As linhas de negócios são as unidades titulares de clientes e são responsáveis pela administração de PLD/CFT de seus clientes. Cada linha de negócios deve nomear um "titular de cliente" responsável pelos procedimentos de PLD/ CFT ao longo do ciclo de vida do cliente. De acordo com o modelo de governança de cada linha de negócios, tal responsável pode ser um gerente contanto que as tarefas e responsabilidades sejam atribuídas adequadamente. Quando os clientes têm um gerente de relacionamento individual dentro da linha de negócios, este gerente de relacionamento é o titular do cliente.

A (re)avaliação de risco de um cliente é um componente essencial dos procedimentos de PLD/CFT do banco e é da responsabilidade do titular do cliente na linha de negócios. Esta (re)avaliação não pode ser delegada à equipe de atendimento ao cliente. A equipe de atendimento ao cliente pode ajudar na compilação de listas que devem ser avaliadas, reunindo informações e armazenando documentos. Se o titular do cliente designado não tiver certeza de como interpretar ou avaliar certas informações, ele/ela deve consultar os gestores pertinentes e/ou um CO.

Se um gerente de relacionamento sênior gerenciar todos os negócios do cliente com o Grupo ABN AMRO no mundo inteiro, tal gerente de relacionamento deve garantir que a (re)avaliação de risco seja feita em todas as jurisdições. No entanto, o titular do cliente local designado dentro de cada país ou linha de negócio deve realizar a (re)avaliação de risco e continua a ser responsável pelo gerenciamento de PLD/CFT do cliente e por garantir o cumprimento das leis locais de sua relação específica com o cliente.

3 Ameaças e Riscos

A insuficiência ou a ausência de políticas, padrões, ou procedimentos de PLD/CFT, ou simplesmente não colocá-los em prática, pode colocar o AAB Brasil em sérios riscos e problemas, especialmente riscos reputacionais, operacionais, regulatórios e de concentração. É importante destacar que todos esses riscos estão inter-relacionados. No entanto, qualquer um deles, isoladamente, pode resultar em danos financeiros materiais ao AAB Brasil, tais como: (a) a retirada de investimentos pelos clientes; (b) reclamações contra o banco; e (c) penalidades pelos reguladores. Adicionalmente, o banco terá que arcar com custos de uma eventual investigação, apreensão e congelamento de ativos e ainda, perdas de empréstimos. O gerenciamento e resolução desses problemas desviariam uma quantidade de tempo e energia consideráveis. Adicionalmente, o banco corre o risco de atender de forma insatisfatória as expectativas da sociedade, mesmo com relação aos padrões, normas ou códigos de conduta elaborados pelo próprio banco, o que levaria a uma opinião pública negativa.

3.1 Risco Reputacional

A natureza dos negócios do AAB Brasil exige a confiança de seus clientes, credores e do mercado. O risco reputacional é a possibilidade de existir uma opinião pública negativa com relação às práticas e associações comerciais do banco, independentemente dessa opinião ser com base em fatos reais ou meramente na percepção pública. Um opinião pública negativa

pode causar perda da confiança na integridade do AAB Brasil. Tal risco pode ser resultante de:

- ações e conduta do AAB Brasil como um todo ou de uma determinada equipe, ex.: produtos vendidos, serviços prestados ou interação com as partes interessadas;
- ações e comportamento de contrapartes externas, ex.: clientes, prestadores de serviços, fornecedores etc.; e
- falha no gerenciamento ou do funcionário em identificar, avaliar adequadamente e mitigar em tempo hábil as ameaças e riscos.

3.2 Risco Legal e Regulatório

O AAB Brasil pode se envolver em processos administrativos e/ou judiciais em consequência da não observância desta Política CAAML, ou por não ter realizado uma análise (*due diligence*) adequada na identificação dos clientes e entendimento de seus negócios. Isso também pode levar à multas, responsabilidades criminais e civis, e penalidades especiais impostas ao banco como um todo, ao BREC ou empregados. Finalmente, isso pode levar à restrição das atividades do banco ou, em último caso, resultar na perda da licença do banco.

3.3 Risco de Concentração

Sem saber precisamente quem são os clientes do banco e seus possíveis vínculos societários (incluindo internacionais) com outros clientes potenciais ou existentes não é possível proteger o banco de riscos de concentração referente à LD/FT.

3.4 Risco Operacional

Assim como os demais riscos de compliance, os riscos de LD/FT são considerados riscos operacionais e, como tais, parte da estrutura de gerenciamento de riscos operacionais. A maioria dos riscos operacionais no contexto desta Política CAAML está relacionada a: (a) falha na implantação ou no funcionamento diário dos sistemas, processos e programas do AAB Brasil; (b) procedimentos de controle não efetivos; ou (c) falha nas análises (*due diligence*) de clientes. O Monitoramento & Testes dos Controles do AAB Brasil (*Management Control & Testing*, ou "MC&T") dos riscos operacionais relacionados à LD/FT devem ser incluídos na Ferramenta de Risco de Governança e de Compliance do ABN AMRO (*ABN AMRO Governance Risk Compliaqnce Tool*, ou "AGRC") do banco para gerenciamento de riscos operacionais. Referência é feita ao sumário do principais controles globais mandatórios e indicativos no Anexo desta Política que devem ser usados para medir e/ou evidenciar a aderência a esta Política CAAML. Qualquer exceção a tais controles deve ser reportada para, e requerem a aprovação do, Diretor de PLD/CF.

3.5 Penalidades

Os empregados que não cumprirem com esta Política CAAML, com os demais padrões e procedimentos e/ou com as leis e regulamentos, devem saber que estão colocando em risco a reputação do AAB Brasil e, consequentemente, serão responsabilizados por isso. Tal responsabilização pode levar a diversas ações disciplinares, incluindo demissão. Além disso, o empregado envolvido no dano pode enfrentar consequências legais rigorosas, incluindo, mas não se limitando a, multas, processos criminais e possivelmente prisão.

Se um empregado deliberadamente evitar ou ignorar informações que poderiam levar à descoberta de uma atividade ilícita, conhecida como cegueira deliberada (*willful blindness*), o BREC poderá aplicar as penalidades mais rígidas. O BREC deve estar ciente da "doutrina do gestor responsável". Isso significa que o gestor que deixar as coisas acontecerem e aceitar o risco material do não cumprimento das leis pelo AAB Brasil ou por sua equipe, poderá ser criminalmente responsável em diversas jurisdições. O banco também os considerará responsáveis.

4 Sobre esta Política CAAML

4.1 Objetivo

Esta Política CAAML descreve a filosofia e a abordagem dos controles de PLD/CFT do AAB Brasil tendo em vista o combate aos crimes de LD e FT e a proteção da reputação do banco. Ela estabelece os: (a) procedimentos de análise (*due diligence*) para os clientes novos e existentes; (b) requerimentos para manter informações e documentações da *due diligence* devidamente atualizadas; e (c) monitoramento contínuo da relação comercial com clientes, a fim de cumprir com as obrigações de identificação e reporte de operações suspeitas para as autoridades competentes.

A Política CAAML busca traduzir a essência, reforçar e complementar os valores do AAB Brasil. Dentro do contexto desta Política CAAML, é muito importante: (a) conhecermos nossos clientes, (b) realizarmos de forma rigorosa nossos procedimentos de PLD/CFT; e (c) avaliarmos cuidadosamente as operações comerciais antes de contratá-las, considerando, também, os aspectos não financeiros. A Política CAAML abrange:

- identificação e verificação de clientes, dos seus beneficiários finais ("UBOs") e de suas partes relacionadas relevantes (se houver);
- avaliação de risco, incluindo a filtragem de clientes, dos UBOs e das partes relacionadas relevantes (se houver) nas listas aplicáveis;
- filtragem de operações;
- monitoramento de operações;
- comunicação/reporte de atividades suspeitas ou incomuns; e
- não aceitação/recusa ou encerramento de relacionamentos comerciais.

A Política CAAML também abrange a conscientização e treinamentos de funcionários; armazenamento de dados e descreve os deveres e responsabilidades necessários para a implantação do acima descrito.

Esta Política CAAML não reflete somente o comprometimento do banco e do BREC em combater ativamente a LD e o FT, mas também cumpre com as recomendações, leis e regulamentos oficiais, tais como:

- Recomendações da Força-Tarefa de Ação Financeira sobre Lavagem de Dinheiro (*The Recommendations of Financial Action Task Force on Money Laundering – FATF*);
- Gerenciamento de Risco de lavagem de dinheiro e financiamento do terrorismo do Comitê de Basiléia de Fevereiro de 2016 (*Sound management of risks related to Money laundering and terrorismo financing of February 2016)*);
- Legislação da União Européia ("*EU*");
- Lei de PLD/FT dos Países Baixos (WWFT);
- Lei de Supervisão Financeira dos Países Baixos (Wft);
- no caso do AAB Brasil, leis e demais regulamentações brasileiras, emitidas pela Presidência da República, CMN, BCB, CVM e demais autoridades competentes

NOTA: Esta Política CAAML estabelece também certas obrigações relativas à privacidade dos dados e à utilização e processamento dos dados pessoais dos clientes. Deve ser dada devida atenção para que o uso e o processamento de dados pessoais de clientes atendam todos os requisitos legais e regulatórios. Isto inclui, mas não se limita à, obrigação de informar aos clientes sobre a utilização e processamento dos seus dados pessoais e de obter o consentimento do cliente sempre que for necessário, sem, no entanto, permitir o acesso aos

dados pessoais a pessoas ou organizações suspeitas (*tipping off*) (vide itens 4.9 e 5.6 abaixo).

4.2 Padrões Globais

Esta Política CAAML também descreve os Padrões Globais do Grupo ABN AMRO (*ABN AMRO's Global Standards*, ou "Padrões Globais"). Quando os padrões locais do AAB Brasil forem governados por normas mais estritas às que são estabelecidas nesta Política CAAML, a norma mais estrita deverá prevalecer. Quando a lei do país não permitir a aplicação desta Política CAAML ou parte dela, tal situação deve ser reportada ao Diretor de PLD/CFT. Quando apropriado ou requerido, Compliance informará o regulador do ABN AMRO adequadamente.

Quando, com base nesta Política CAAML, uma informação relacionada a um cliente for compartilhada entre uma entidade e outra do Grupo ABN AMRO, é necessário que primeiro se tenha verificado a permissibilidade do compartilhamento da informação com as leis de proteção de dados e sigilo bancário.

4.3 Abordagem com Base no Risco (*Risk-based Approach*)

A Política CAAML defende uma abordagem baseada em risco, o que significa que as medidas de PLD/CFT podem variar em função dos riscos específicos aos quais o AAB Brasil pode estar exposto, mas devem ser proporcionais a esses riscos, a fim de mitigá-los eficazmente.

Esta abordagem possibilita a utilização de diferentes medidas e controles dependendo das linhas de negócios e dos modelos de negócio em relação à diferentes situações e indicadores de risco (inerentes) aplicáveis. Para isso, o banco avaliará periodicamente e sistematicamente os riscos inerentes de LD/FT aos quais está exposto nos níveis apropriados, como parte da SIRA. Os indicadores de risco inerentes incluem, mas não estão limitados a:

- clientes ou segmentos de clientes, incluindo suas atividades e operações comerciais;
- produtos e serviços oferecidos;
- localidades geográficas envolvidas; e
- canais de distribuição utilizados.

Tal avaliação periódica de risco deve ser concluída e aprovada pelo BREC. Seu resultado forma a base para o desenvolvimento de políticas e medidas para mitigar o risco inerente de LD/CF analisado, em linha com o apetite de risco do banco. Quando aplicável/disponível, riscos de LD/CT identificados em análises setoriais e nacionais nas jurisdições relevantes, e também os identificados na *EU Supranational Risk Assessment* devem ser avaliados por todo o grupo, linhas de negócios e/ou país.

4.4 Análise do Cliente (*Client Due Diligence*, ou "CDD")

Conhecer o cliente e seus respectivos negócios através de uma CDD é o coração desta Política CAAML. CDD significa levar em conta todos os fatores que o banco precisa para determinar se as atividades de um cliente precisam ser reportadas para as autoridades competentes e se o cliente é e permanece aceitável ao banco. Isso inclui os procedimentos de identificação e avaliação de risco na aceitação e durante o ciclo do cliente no banco. A CDD precisa ser realizada antes ou durante o estabelecimento do relacionamento com o cliente, mas em nenhuma hipótese depois de se ter iniciado a prestação de um serviço. CDD precisa ser realizada com base no risco e ter um alcance suficientemente razoável para permitir que o banco forme uma opinião e fique seguro de que:

- conhece o cliente;
- tem informações sobre a natureza e o histórico das atividades comerciais do cliente;
- tem ciência da existência e identidade dos UBOs, beneficiários (se houver) e partes relacionadas relevantes (se houver);

- não tem motivos para acreditar que os ativos e recursos do cliente têm origem ilícita;
- tem conhecimento do que o cliente precisa em termos de produtos e serviços;
- tem conhecimento a todo momento de todos os riscos a que está sujeito a fim de gerenciá-los adequadamente; e
- garante que as informações, dados e documentos que suportam os itens acima estão devidamente atualizados a todo momento.

As CDDs estão sujeitas a um controle duplo, o que significa que o princípio do "*four-eyes*" deve sempre ser aplicado antes da aceitação ou da decisão de continuidade do relacionamento comercial com um cliente.

4.5 Notas de Orientação Globais de CAAML

Junto desta Política CAAML, as Notas de Orientação de CAAML são publicadas pelo Compliance através dos canais formais de publicação interna do banco para discussão sobre assuntos/tópicos específicos. Tais Notas de Orientação são aprovadas pelo Diretor de PLD/CFT (em reunião do BRARCC). Embora tais Notas de Orientação não sejam uma política do AAB Brasil em si, elas se baseiam nas normas desta Política CAAML, nas principais normas da indústria e nas melhores práticas e orientações da Força-Tarefa de Ação Financeira sobre Lavagem de Dinheiro (FATF), do Comitê de Supervisão Bancária da Basileia (BCBS) e de nossos reguladores, incluindo o regulador nacional do AAB Holanda, o DNB.

As orientações fornecidas nas Notas de Orientação devem, portanto, ser seguidas e são aplicáveis a todos. Em circunstâncias nas quais – com base na prática, regulamentação e/ou legislação locais – não for viável seguir a orientação, é necessário obter uma orientação específica de um CO. As exceções e desvios das Notas de Orientação requerem a aprovação do Diretor de PLD/CFT e devem ser devidamente registrados de acordo com as normas de retenção da Política de Gerenciamento de Documentos. A regra é: "cumprir ou explicar".

4.6 Anti-Retaliação

O AAB Brasil promove um ambiente no qual os funcionários se sentem confortáveis ao denunciar violações ou atividades incomuns ou suspeitas, sem medo de retaliação e sem o risco de danos de reputação de nenhum tipo, de nenhuma forma, em nenhum momento. Vide a Política de Comunicação de Irregularidades. Os funcionários que reportarem de boa-fé uma suspeita de violação não serão disciplinados ou retaliados**.**

4.7 Conscientização e Treinamento

Treinamento e conscientização são elementos importantes de um programa de PLD/CFT. Para serem eficazes, as atividades de treinamento e conscientização devem ser orientadas para as necessidades específicas dos diferentes tipos de participantes e devem ser contínuas. Cada linha de negócios deve planejar e implementar um Programa de Treinamento e Conscientização sobre PLD/CFT. Este Programa deve ser atualizado regularmente e deve, pelo menos, determinar:

- que toda a equipe receba treinamento básico, conscientizando-se sobre o risco de LD/FT;
- que toda a equipe (pelo menos a equipe com contato direto com o cliente, responsável pela operação de transações e manipulação de documentação de CDD) receba programas especiais de treinamento contínuo para ajudá-la a reconhecer as operações que possam estar relacionadas com LD ou FT, bem como para instrui-la sobre como proceder nesses casos.

É responsabilidade do Compliance garantir que exista material de treinamento adequado e atualizado regularmente.

Os gestores das linha de negócios são responsáveis, em conjunto com o Compliance, por garantir que todos os funcionários (relevantes) nas linhas de negócio recebam treinamento

adequado para criar consciência e que isso seja registrado no sistema do Departamento de Recursos Humanos. Toda a equipe deve receber treinamento geral de PLD/CFT ao ingressar na linha de negócios. Treinamento complementar deve ser prestado à equipe relevante sempre que for adequado às suas atividades, de forma contínua, e deve ser realizado com a frequência que for apropriada para a linha de negócios de acordo com os riscos inerentes ao segmento do cliente, produtos, serviços e atividades nos quais o membro da equipe está envolvido.

Especificamente, gestores e empregados devem, através do treinamento, ter conhecimento:

- desta Política CAAML e os Padrões Globais, das políticas e procedimentos de PLD/CFT da linha de negócio e do país para evitar o uso do banco para crimes financeiros;
- de quaisquer requisitos legais exigidos da linha de negócio pela jurisdição em que opera e onde o funcionário está alocado (incluindo o efeito das violações na equipe e nos clientes);
- da identidade e dos dados de contato da pessoa ou departamento responsável por PLD/CFT, incluindo a equipe de Compliance pertinente;
- dos procedimentos para denunciar conhecimento ou suspeita de lavagem de dinheiro ou financiamento de terrorismo;
- quando apropriado, da vulnerabilidade à lavagem de dinheiro e ao financiamento do terrorismo de seus produtos, serviços, linha(s) de negócios, clientes ou segmentos de clientes específicos.

A equipe deve ser informada de que pode ser responsabilizada pessoalmente por não comunicar qualquer conhecimento ou suspeita de LD de acordo com esta Política e que, além de quaisquer sanções penais aplicáveis localmente, processos disciplinares também podem ocorrer. Além disso, a equipe deve ser informada sobre a Política de Comunicação de Irregularidades.

4.8 Gestão Consolidada de Risco de PLD/CFT

Os riscos de LD/FT não têm fronteiras. Por isso, o Grupo ABN AMRO deve gerenciá-los globalmente. O Grupo ABN AMRO apoia plenamente o documento do Comitê de Supervisão Bancária da Basileia (*Basel Committee on Banking Supervision*) sobre a gestão correta dos riscos relacionados com LD e FT. O Diretor de PLD/CFT do AAB Holanda tem a responsabilidade de monitorar continuamente o cumprimento de todos os deveres de PLD/CFT pelo banco. Para cumprir essa função de supervisão, é essencial que todas as jurisdições nas quais o grupo opera proporcionem uma estrutura jurídica apropriada que permita que informações para fins de gerenciamento de riscos de LD/FT sejam passadas para o Compliance para uso dentro do grupo inteiro.

As linhas de negócios são obrigadas a promover e apoiar a troca proativa de informações sobre clientes de Alto Risco e atividades relevantes para a gestão global dos riscos de LD/FT e devem responder aos pedidos de informações do Compliance em tempo hábil.

Dentro dos limites legais e regulatórios, todas as linhas de negócio devem disponibilizar informações relevantes de LD/FT para o Compliance para uso em todo o banco. As informações trocadas devem ficar restritas ao Compliance, incluindo o SIM quando aplicável, a fim de preservar a confidencialidade requerida e evitar o risco de fornecimento de informações privilegiadas (*tipping off*).

Em caso de uma SAR local estar relacionada com um relacionamento internacional, o Compliance deverá compartilhar essa informação em uma "*need to know basis*" ("necessidade de conhecer") com o Grupo, a menos que as autoridades na jurisdição do local determinem algo diferente.

4.9 Troca de Informações Relacionadas à LD/FT

Para combater eficazmente a LD e o FT, o AAB Brasil encoraja, sempre que permitido pela lei, a troca de informações com outras instituições financeiras e/ou autoridades sobre qualquer suspeita de atividades terroristas ou de lavagem de dinheiro. Atualmente, nem todas as jurisdições permitem a troca dessas informações dentro de um grupo ou com terceiros, como outras instituições financeiras, autoridades e tribunais.

Se a troca de tais informações com base em suspeita de atividades de LD e FT for permitida pela legislação, deve-se ter o devido cuidado para que tal troca também atenda aos requisitos das leis de privacidade aplicáveis. Para evitar a troca não autorizada de informações com terceiros, tal troca deve ser feita através do Compliance ou aprovada antecipadamente por ele, incluindo SIM quando aplicável, e somente com suas contrapartes designadas em outras instituições financeiras (ambos em consulta com o Departamento Jurídico ("Jurídico")).

Outros empregados estão proibidos de fornecer as informações acima mencionadas sobre clientes, os negócios ou transações deles a qualquer pessoa fora do Grupo ABN AMRO, a menos que seja solicitado por ordem judicial ou administrativa. Todas as linhas de negócios devem criar procedimentos para garantir que todos os pedidos que possam estar relacionados com LD ou FT, ou outros assuntos considerados relevantes pelo Compliance, e as respectivas respostas, sejam fornecidos ao Compliance, incluindo SIM, quando aplicável, que, em consulta com o Jurídico, tomará a decisão final sobre a divulgação solicitada.

Isto permite que o Grupo ABN AMRO tome as medidas apropriadas, por exemplo, *modus operandi*, monitoramento aprimorado ou arquivamento de SAR.

Qualquer troca de informações, como mencionado acima, deve ser mantida em estrita confidencialidade. O princípio da "necessidade de conhecer" (*Need to Know*) deve ser aplicado rigorosamente para evitar que:

- A troca de informações vaze para pessoas ou organizações potencialmente suspeitas ("*tipping off*", fornecimento de informações privilegiadas); ou
- Os nomes da equipe do ABN AMRO, da equipe de outra instituição financeira ou de equipe de organismos autorizados sejam divulgados a pessoas ou organizações potencialmente suspeitas (proteção da equipe envolvida).

4.10 Registros e Retenção de Registros

Esta seção é regida pela Política de Gerenciamento de Arquivos. Além disso, aplicam-se as seguintes declarações:

- ao manter seus arquivos atualizados, o AAB Brasil é capaz de demonstrar o cumprimento de todos os aspectos desta Política CAAML e, assim, demonstrar que suas ações em um dado momento foram adequadas em relação às circunstâncias da época. Em particular, o raciocínio por traz de todas as decisões deve ser sempre claramente registrado, bem como a documentação, os dados e as informações que embasaram a decisão tomada;
- todos os registros relacionados à PLD/CFT podem vir a ser necessários em futuras investigações internas ou externas. Portanto, esses registos devem ser conservados durante toda a vida útil da relação comercial com o cliente e – na medida do permitido por lei – durante, pelo menos, 05 (cinco) anos após o término da relação ou, no caso de uma operação eventual, durante pelo menos 05 (cinco) anos após a data da operação. Os arquivos relativos ao arquivamento de SARs devem ser conservados – na medida do permitido por lei – por pelo menos 05 (cinco) anos após a data da comunicação e devem incluir todos os detalhes para possibilitar a reconstrução da operação relatada;
- devido à natureza das investigações, é importante que os arquivos sejam mantidos num formato facilmente recuperável e em conformidade com quaisquer requisitos legais/regulamentares; e
- dados pessoais obtidos exclusivamente para os propósitos de PLD/CFT não podem ser usados para outras finalidades (comerciais) e devem ser destruídos depois de expirados

os períodos de armazenamento aplicáveis, a menos que a legislação determine o contrário.

5 Diretrizes desta Política CAAML

5.1 Identificação e verificação do cliente

Cada linha de negócios deve conhecer e verificar a verdadeira identidade de todos os seus clientes. O "titular do cliente" é responsável pela identificação e verificação adequadas. Identificar clientes não é apenas uma questão formal, mas é parte fundamental desta Política CAAML. O vínculo entre as partes envolvidas pode ser muito mais amplo do que mostrado formalmente em um contrato e pode incluir também os representantes e beneficiários finais (UBOs) pessoas físicas . Cada linha de negócios deve ter procedimentos baseados no risco para estabelecer, quando aplicável, a identidade da(s) pessoa(s) física(s) que é/são UBO(s) e para tomar as medidas necessárias para verificar sua identidade, de modo que o banco esteja seguro de que conhece o verdadeiro UBO. Dependendo do nível de risco, a identificação e antecedentes de mais pessoas físicas e jurídicas devem ser verificados para a aceitação (ou não) de um potencial cliente.

Em caso de dúvidas, o Compliance deve ser consultado. Quando for o caso, as circunstâncias e motivos pelos quais o banco poderá começar ou continuar uma relação comercial, sem a identificação e verificação padrão, devem ser registrados na pasta do cliente, e os registros devem ser mantidos de acordo com a Política de Gerenciamento de Arquivos.

Quando não for possível obter prova satisfatória da identidade do cliente e suas partes relacionadas relevantes, num prazo razoável, a relação comercial não pode ser estabelecida ou deve ser encerrada.

5.1.1 Identificação e verificação do cliente

Um cliente pode tentar estabelecer uma relação comercial sob uma falsa identidade com a finalidade de ficar anônimo, ou para garantir que não possa vir a ser rastreado ou ligado ao produto de um crime, que está sendo lavado.

Estabelecer a verdadeira identidade dos clientes ajuda a impedir que o banco seja usado para fins criminosos. Para estabelecer a verdadeira identidade uma pessoa, física ou jurídica, 02 (dois) passos separados devem ser tomados:

- identificação através da obtenção de informações do cliente; e
- verificação da veracidade e exatidão da informação obtida.

O princípio primordial é que o AAB Brasil deve ter uma crença razoável e segurança de que obteve e documentou a verdadeira identidade do cliente, e de que o cliente não está agindo em benefício de um terceiro desconhecido.

Para cada país onde o Grupo ABN AMRO está ativo, o Compliance fornece orientação para documentação de identificação e verificação conforme os requisitos e procedimentos locais.

5.1.2 Identificação

A identificação é o ato de determinar quem é uma pessoa. Isso é feito pela obtenção e registro de informação fornecida pelo cliente, cobrindo os elementos de sua identidade, ou seja:

- razão social completa e todos os outros nomes usados, quando aplicável;
- endereço de residência permanente atual ou, para pessoas jurídicas, seu endereço estatutário e o endereço operacional, se diferentes. Uma caixa postal não pode ser um endereço válido para efeitos de identificação;
- número de registo principal ou único ou o número do documento de identidade oficial;

- para pessoas físicas: data de nascimento.

Em qualquer caso, as seguintes pessoas devem ser identificadas:

- pessoa(s) física(s); e
- pessoa(s) jurídica(s), UBOs), diretor(es) e pessoa(s) autorizada(s) a representar a pessoa jurídica perante o ABN AMRO.

5.1.3 Identificação de Partes Relacionadas Pertinentes

Dependendo dos riscos de LD/FT e outros requisitos legais e regulamentares não cobertos por esta Política CAAML, pode ser necessária a obtenção de informações sobre mais partes relacionadas ao cliente. Portanto, estas partes devem ser consideradas relevantes no processo de análise e verificação (*due diligence*) deste cliente e ser tratadas de acordo. Cada linha de negócios deve ser capaz de identificar quais partes relacionadas são consideradas relevantes na avaliação de risco de seus clientes. As partes relacionadas identificadas devem ser submetidas ao procedimento de filtragem de clientes (ver item 5.2.5 abaixo).

5.1.4 Verificação

Verificação da identidade é o processo de provar se uma pessoa é realmente quem ela alega ser. Isso é feito através de um processo de exame cuidadoso da exatidão dos dados, das informações e dos documentos fornecidos.

No contexto desta Política CAAML, verificação é o processo de procurar evidências satisfatórias da identidade daqueles com quem a linha de negócios tem, ou procura ter, uma relação comercial. Isto é feito através de verificações independentes sobre a exatidão de informações, dados e documentos fornecidos pelo cliente..

A representação adequada dos diretores e/ou representantes autorizados deve ser determinada e verificada para a obtenção de transparência jurídica, não só para prevenir os riscos de LD/FT.

Em regra, as provas de identidade devem ser obtidas considerando as circunstâncias de cada cliente e do seu país de origem, de acordo com fontes confiáveis de documentos, dados ou informações. Algumas formas de prova de identidade são menos confiáveis do que outras e, quando confrontadas com tais provas, é aconselhável proceder com investigações adicionais para determinar a qualidade dos documentos, dados e das informações ou coletar fontes adicionais e confiáveis de documentos, dados ou informações para adquirir uma crença razoável de que a informação fornecida é correta.

Cada linha de negócios deve tomar medidas razoáveis para verificar a identidade do UBO, para que o banco possa ter uma crença razoável e ficar confiante de que sabe quem é o UBO e que isso está devidamente documentado. Estruturas jurídicas complexas podem ser usadas para ocultar a identidade do UBO. Portanto, a estrutura de controle da organização do cliente deve ser documentada através de um organograma que esclareça e verifique a identidade do UBO. As disposições legais, tais como, ou semelhantes a, um *trust* ou fundação, devem ser explicitamente documentadas como parte da estrutura de controle.

5.1.5 UBO

UBO (Beneficiário Final) significa: (a) qualquer pessoa física que, em última instância, possui ou controle o cliente; e/ou (b) a pessoa física em benefício da qual uma operação ou atividade está sendo conduzida. O UBO é uma pessoa física que, com base em fatos, documentos ou circunstâncias, aparentemente exerce uma influência determinante sobre o cliente. Isso inclui, pelo menos, as seguintes pessoas físicas, que devem ser consideradas UBOs:

Em caso de pessoa jurídica:

- Uma pessoa física que, em última instância, direta ou indiretamente (por meio de estruturas complexas), detenha ou tenha o controle sobre mais de 25%1 das ações, dos direitos de voto ou dos *ownership rights* de uma pessoa jurídica. Pessoa jurídica que não seja listada em um mercado regulado e sujeira à regras de divulgação consistentes com a legislação da União Europeia ou sujeita à padrões internacionais equivalentes que assegurem uma transparência adequada da informação sobre sua participação acionária.

Em caso de um arranjo jurídico, tal como, ou semelhante a, um *trust*:

- Uma pessoa física que é ou possui uma posição semelhante a instituidor (*settlor*), *trustee,* protetor, beneficiário ou qualquer outra pessoa física exercendo o controle final sobre o *trust* por meios diretos ou indiretos de participação ou ainda por outras formas. Note que o beneficiário pode ser mais de uma pessoa. O beneficiário também pode ser um grupo definido ou classe de pessoas, independentemente de as identidades de cada membro individual desse grupo poderem ser determinadas com antecedência em um determinado momento (por exemplo, um *trust* familiar).

Com base nos critérios acima mencionados para cada pessoa jurídica ou arranjo jurídico, todos os UBOs devem ser identificados. Se o detentor do cliente, após ter esgotado todos os meios possíveis, acreditar e estiver confiante de que, com base nos critérios acima, nenhuma pessoa física pôde ser identificada como UBO, então os executivos seniores do cliente devem ser considerados como UBO. A crença razoável, nesse caso, também depende de, baseado nos fatos e circunstâncias, não haver suspeitas de que o UBO está sendo ocultado.

Para os fins desta Política, as seguintes pessoas devem ser consideras como executivos seniores:

- diretor executivo de uma pessoa jurídica ou, no caso de um conselho de administração, os membros desse conselho; e
- todos os sócios gerais de uma sociedade.

5.1.6 Momento da Verificação

A identidade do cliente precisa ser conhecida antes do início de uma relação comercial. A verificação da identidade do cliente e, se for caso, do UBO, deve, salvo exceção mencionada abaixo, ocorrer antes do início de uma relação comercial ou da realização de uma operação eventual. Excepcionalmente, a verificação da identidade do cliente e, se for o caso, do UBO, pode ser concluída durante o estabelecimento de uma relação comercial se:

- o negócio não puder ser interrompido; e
- se o risco de LD ou FT for mínimo.

O início de uma relação muitas vezes coincide com a abertura de uma conta. A partir do momento em que o banco entra em uma relação contratual, ele adquire certas obrigações e fica exposto a riscos e responsabilidades. Por exemplo, a partir do momento em que "recebe" ou disponibiliza recursos ou ativos em nome de um potencial cliente, o banco já pode estar incorrendo na facilitação de um crime financeiro. Mesmo quando a legislação permitir que bancos iniciem contas antes de a verificação ter sido concluída, isso só será permitido com aprovação específica do gestor sênior, após recebimento do aconselhamento do Compliance, incluindo a consideração sobre os riscos de responsabilidade (criminal) potencialmente envolvidos para o banco ou sua equipe. Nessas situações, deve-se garantir e monitorar se a documentação/verificação faltante será obtida em tempo hábil.

5.1.7 Identificação e Verificação de Linha de Negócios Cruzados (*Cross Business Line)*

A menos que seja proibido por leis ou regulamentos locais, cada linha de negócio pode aceitar o resultado do processo de identificação e de verificação de identidade e endereço,

[1] De acordo com a Politica Global CAAML da linha de negocio *Corporate Banking,* o requisito é de 10%.

realizado de acordo com esta Política CAAML por outra linha de negócios do ABN AMRO ou país, desde que esteja de acordo com os procedimentos específicos de PLD/CFT.

5.2 Avaliação de Risco

5.2.1 Processo de Avaliação de Risco

A avaliação de riscos deve ser um processo de monitoramento contínuo ao longo do ciclo de vida do cliente. O AAB Brasil só pode gerenciar eficazmente seu risco se compreender as atividades normais dos seus clientes, o que permite a identificação, por exclusão, as atividades que estão fora dos padrões normais. Em certos momentos, essas avaliações de risco são formalizadas e os resultados são armazenados e mantidos em formato prontamente recuperável, quais sejam:

- na aceitação do novo cliente;
- sempre que ocorrer um evento que justifique uma revisão; e
- periodicamente para clientes específicos (segmentos).

Uma avaliação de risco é obrigatória para cada cliente, a fim de determinar seu perfil de risco. A avaliação de risco deve ser baseada nos riscos de LD/FT inerentes, identificados para a linha de negócio específica como parte do SIRA. Esses indicadores de risco inerentes incluem: os segmentos do cliente, as suas atividades e transações comerciais, os produtos e serviços que lhes são oferecidos, as questões geográficas envolvidas e os canais de distribuição utilizados, e devem ser ajustados às características específicas relacionadas ao cliente. Nesta avaliação de risco, as circunstâncias que apresentam um alto risco para o banco devem ser identificadas, avaliadas e documentadas.

Segundo a avaliação de risco, o cliente é classificado como cliente de risco neutro, médio, alto ou inaceitável. Cada linha de negócio define, para cada segmento de cliente, os clientes que devem ser tratados como clientes de alto risco, com base nos indicadores de risco listados neste item 5.2.1.

Para tornar a abordagem baseada em risco mais precisa, as linhas de negócio podem atribuir a classificação de risco médio para diferenciar em:

- (nível de) aprovação da gestor sênior; e/ou
- a necessidade de revisão periódica ou ajuste da frequência das revisões; e/ou
- o nível de intensidade do monitoramento do cliente e de seu comportamento.

Para a aceitação de clientes de alto risco, a orientação do Compliance e a aprovação pelo gestor sênior são exigidas de acordo com os procedimentos específicos de PLD/CFT. Em caso de recomendação negativa do Compliance, o gestor sênior deve obter a aprovação do próximo nível superior de hierarquia na linha de negócio, se ela ainda quiser fazer negócios com o cliente. Os procedimentos normais de encaminhamento para outro nível hierárquico aplicam-se para o Compliance. Consulte a Política de Conformidade.

Deve-se observar que todos os clientes exigem o monitoramento de suas atividades de forma contínua, a fim de cumprir as obrigações de identificar e comunicar as transações incomuns e/ou suspeitas às autoridades competentes (COAF). Se o AAB Brasil optar por fornecer produtos ou serviços a um cliente de alto risco, o aperfeiçoamento da gestão de risco deve levar a um monitoramento aumentado do cliente e de suas transações. Isso também significa que o banco deve reavaliar o risco desse cliente regularmente, a ser definido por cada linha de negócio e aprovado pelo Compliance.

Dependendo do risco, pode ser impróprio confiar apenas nas declarações do cliente e, nesses casos, a verificação deve ser feita sempre que razoavelmente possível com base em documentos, dados ou informações de fonte independente e confiável. Em caso de alto risco, o foco deve ser saber quais são os riscos que o banco corre para gerenciá-los

adequadamente. Tal avaliação de risco melhorada exige fazer perguntas adicionais até que fique claro que tipo de riscos o banco corre com o cliente. Se os riscos não puderem ser entendidos ou forem considerados demasiado elevados, o cliente é inaceitável.

Cada linha de negócios deve definir em seus processos e procedimentos as informações e documentação mínimas necessárias para realizar a avaliação de risco. Isso deve incluir pelo menos todas as circunstâncias com relação a:

- histórico do cliente e atividades comerciais (A);
- as questões geográficas envolvidas (B);
- produtos e serviços necessários (C); e
- a fonte e a natureza dos fundos (D).

(A) Histórico do Cliente e Atividades Comerciais

É essencial compreender os negócios e as atividades comerciais nos quais o cliente está envolvido. Algumas empresas ou atividades envolvem um risco maior e são mais vulneráveis a riscos criminais do que outras. A mesma condição é verdadeira para aspectos relacionados ao comportamento ambiental e social. A avaliação de risco deve incidir sobre os riscos inerentes relacionados com negócios/atividades de um cliente. Sem ser limitantes, os seguintes aspectos devem ser considerados:

- natureza das atividades comerciais;
- antecedentes das pessoas que podem exercer influência na empresa ou na gestão;
- estrutura societária da organização à qual o cliente pertence;
- relacionamento bancário, se houver, com outra instituição, e a possibilidade de um relacionamento bancário anterior ter sido encerrado unilateralmente por outra instituição financeira;
- razões para suspeitar que o UBO está tentando ocultar sua identidade, escondendo-se atrás de outras pessoas;
- a representação da situação do cliente é plausível ou "boa demais para ser verdade?";
- a reputação do cliente ou possível publicidade negativa sobre o cliente;
- operações incomuns ou suspeitas nas áreas de risco de lavagem de dinheiro, evasão fiscal2, financiamento de terrorismo, fraude ou intenção maliciosa em relação a terceiros;
- relação entre endereço postal e endereço residencial/principal local de negócio. Atenção deve ser conferida à *PO Box and Hold Mail Exceptions Policy* (AIM 103-01-15);
- a adequação do modelo de negócio ao perfil do cliente e os serviços solicitados;
- razões pelas quais o cliente deseja entrar na relação comercial;
- a natureza da relação entre o cliente e a(s) pessoa(s) autorizada(s). Quando a relação não parece ter uma base lógica (como um membro da família, no caso de uma pessoa física, ou um empregado, no caso de uma pessoa jurídica), pode haver um risco mais elevado.

O AAB Brasil identifica as seguintes circunstâncias como um indicador potencial de alto risco que requer uma pesquisa adicional e uma análise mais aprimorada (*Enhanced Due Diligence*, ou "EDD", conforme detalhada no item 5.2.2*)*:

[2] Consulte a Política Tributária (*Tax Policy*) (AIM 101-21-03) para conferir os princípios, definições e explicações tributárias adicionais.

- negócios/atividades que são conhecidos por serem vulneráveis a atividades ilegais ou criminosas;
- relacionamento de negócios é conduzido em circunstâncias não usuais;
- pessoas ou arranjos jurídicos que são veículos de gestão de recursos pessoais;
- empresas/atividades que estão sujeitas a uma forte opinião pública negativa;
- quando parecer que a pessoa jurídica não realiza atividades comerciais ou econômicas ou não participa ativamente na economia do país onde tem a sua sede (as chamadas empresas "shell" ou “off-shore");
- quando a estrutura da organização à qual o cliente pertence parece incomum ou excessivamente complexa devido à natureza do negócio do cliente;
- clientes que possuem acionistas nomeados ou ações ao portador;
- clientes cujas atividades empresariais estejam ligadas a um país submetido a sanções econômicas ou a outras sanções relevantes por organismos nacionais ou internacionais reconhecidos (consulte a Política de Sanções (*Sanctions Policy*) (AIM 102-20-35));
- quando o cliente é objeto de um relatório de atividades suspeitas (SAR).

A presença de um potencial alto risco não significa automaticamente que o cliente é classificado como alto risco. A classificação de risco real depende dos riscos potenciais serem materializados ou mitigados com base nas informações, dados e documentação obtidos.

O AAB Brasil identifica as seguintes circunstâncias como alto risco e o cliente deverá ser classificado pelo menos na categoria de alto risco:

- clientes sobre os quais haja mídia negativa grave localizada em fontes respeitáveis, justificando dúvidas razoáveis sobre a integridade do cliente.

(B) As Questões Geográficas Envolvidas

Determinados locais geográficos são mais vulneráveis à LD e ao FT ou a outras atividades criminosas do que outros. Os países podem ser conhecidos por estarem envolvidos na produção ou transporte de drogas ilegais ou outras atividades criminosas. Os países também podem estar associados a atividades terroristas ou a altos níveis de corrupção. Alguns países são também considerados paraísos de sigilo bancário para fins de LD, FT ou evasão fiscal3. O banco deve não só considerar onde está localizado o cliente, mas também os locais onde o cliente realiza negócios, de onde a fonte de recursos e a riqueza do cliente se originam e onde o cliente solicita os produtos e serviços do AAB Brasil. Para um cliente não residente, o banco também deve considerar as razões para iniciar uma relação bancária fora do seu país de residência. Para fins de classificação das localizações geográficas acima mencionadas, devem ser utilizadas as Classificações de Risco de Crime Financeiro do País do banco.

O ABN AMRO identifica as seguintes circunstâncias como potenciais indicadores de alto risco, exigindo escrutínio adicional e EDD:

- clientes que são residentes/sediados em ou que operam a partir de países de alto risco/risco aumentado (*high/increased risk countries*), conforme designado nas Classificações de Risco de Crime Financeiro do País.

(C) Produtos e Serviços Necessários

É importante entender como o cliente pretende usar os produtos ou serviços solicitados. Quaisquer negociações com o banco devem ser consistentes com o conhecimento do banco sobre os negócios e atividades do cliente. Se a explicação do cliente potencial para solicitar um produto ou serviço bancário for incomum ou ilógica, é importante fazer perguntas

[3] Consulte a Política Tributária (*Tax Policy*) (AIM 101-21-03) para conferir os princípios, definições e explicações tributárias adicionais.

adicionais e verificar as explicações. Se a explicação do cliente para uma solicitação de serviços financeiros específicos ou de serviços de uma determinada subsidiaria for inconclusiva e permanecer assim, o gerente de relacionamento deve recusar a solicitação do cliente.

Não é permitido auxiliar na criação de estruturas financeiras ou em negócios que se destinam a manter o dinheiro oferecido ao banco fora do controle das autoridades competentes. É política do AAB Brasil não abrir contas ou executar pagamentos, valores mobiliários ou outras transações sob um nome fictício de cliente ou esconder deliberadamente o nome do cliente para esse fim. O AAB Brasil não se envolverá em produtos e serviços solicitados pelos clientes, destinados a evadir impostos, o que é crime e, portanto, plenamente abrangido por esta Política CAAML. A linha entre a evasão fiscal e elisão de tributos e o que é considerado aceitável e apropriado numa perspectiva social e de reputação nem sempre é fácil de estabelecer. Consulte a Política Tributária (*Tax Policy*) (AIM 101-21-03) para obter mais orientação ou consulte o Compliance.

O AAB Brasil identifica as seguintes circunstâncias, no que diz respeito às necessidades de um produto e serviço de um cliente, que são consideradas como um potencial indicador de alto risco, exigindo pesquisa adicional e EDD:

- produtos e serviços que são conhecidos por serem vulneráveis a atividades ilegais ou criminosas;
- produtos ou transações que possam favorecer o anonimato;
- produtos ou serviços de *Private Banking* que por sua natureza impõem um alto risco de LD/FT;
- pagamentos recebidos de terceiros desconhecidos ou não associados;
- produtos que envolvem transações e estruturas financeiras incomuns para um cliente ou negócio de um cliente, levando em consideração todas as circunstâncias relevantes; e
- as intenções declaradas do cliente com relação ao uso do produto financeiro não são consistentes com a natureza do negócio e das operações do cliente.

(D) A Fonte e a Natureza dos Fundos

Como mencionado na introdução desta Política CAAML, o AAB Brasil não deseja estabelecer nenhuma relação comercial, se souber ou suspeitar que o dinheiro ou os instrumentos financeiros oferecidos ao banco são produtos do crime ou que os benefícios de crédito oferecidos pelo banco serão utilizados para fins criminosos. Portanto, é essencial que o banco tenha clareza sobre o contexto da origem dos recursos do cliente, que são oferecidos ao banco, e dos fundos que passam pela conta. Isso pode exigir clareza sobre a fonte de riqueza do cliente. Se esta clareza não puder ser obtida e as dúvidas persistirem, a questão deve ser encaminhada ao Compliance para orientação.

5.2.2 Análise Aprimorada (*Enhanced Due Diligence* - EDD)

Como resultado da abordagem baseada no risco descrita no item anterior, as medidas de análise (*Due Diligence*) do AAB Brasil devem ser proporcionais aos riscos identificados. Em situações que, pela sua natureza, apresentam um risco mais elevado de LD, FT ou risco de reputação para o Grupo ABN AMRO, as medidas de análise do AAB Brasil= durante todo o ciclo de vida do cliente devem aumentar de acordo, resultando em uma EDD. A realização de uma EDD não necessariamente conduz a uma classificação de alto risco do cliente. Além das circunstâncias descritas acima, o banco deve sempre aplicar EDD nas seguintes situações:

- quando uma Pessoa Exposta Politicamente (“PEP”) está envolvida;
- em situações sem contato presencial direto, sem certas garantias, como assinaturas eletrônicas;

- quando transações complexas, atipicamente grandes ou com padrões atípicos ocorrerem, sem que haja aparente finalidade econômica ou legal;
- envolvimento de relações com correspondentes internacionais (incluindo, mas não se limitando a, bancos correspondentes) estabelecidas em Estados não membros da União Europeia;
- quando os clientes são residentes ou registrados em países identificados como de alto risco, como assim designados pelas Classificações de Risco de Crime Financeiro do País ;
- envolvimento de bancos que operam sob uma licença bancária estrangeira;
- quando há suspeita de lavagem de dinheiro ou de financiamento de terrorismo.

Nota 01: Estados Membros são Estados da União Europeia e Estados que são parte da área econômica da União Europeia.

Nota 02: A lista de países considerados de alto risco (*high risk*) pela Comissão da União Europeia está publicada pelo Compliance na intranet do banco.

Cada linha de negócio deve preparar uma proposta por escrito de situações em que a EDD deve ser aplicada. Essa proposta requer a aprovação do Compliance e da gerência de linha de negócio relevante. Esta abordagem deve ser adaptada periodicamente de acordo com novos conhecimentos sobre lavagem de dinheiro, financiamento de terrorismo e os riscos de reputação.

PEP

A PEP é uma pessoa física a quem estão, ou foram, confiadas funções públicas proeminentes e inclui um membro familiar direto ou um associado próximo conhecido de tal pessoa.

O AAB Brasil possui um sistema apropriado de gerenciamento de riscos, incluindo procedimentos baseados em risco, para determinar se o cliente, o UBO ou uma parte relacionada relevante (se houver) é uma PEP ou se tornou uma PEP. Se uma PEP estiver envolvida em uma relação comercial, a identidade da PEP deve ser sempre verificada, a aceitação deve ser submetida à aprovação da gerência sênior, e a orientação do Compliance é obrigatória, de acordo com os procedimentos de PLD/CFT específicos da linha de negócio. PEPs, por sua natureza, apresentam maior risco de LD/FT e de reputação, pois podem abusar de sua função pública proeminente para ganho pessoal, incluindo suborno e corrupção. Portanto, é sempre necessário estabelecer a fonte de riqueza, bem como a fonte de fundos que estão envolvidos na relação comercial ou transações com essas pessoas, o que exige monitoramento contínuo melhorado dessas relações comerciais.

Relações com Correspondentes Internacionais Estabelecidos em Países não Membros da UE

Relação com correspondente significa:

- a prestação de serviços bancários por um banco como correspondente para outro banco como respondente, incluindo uma conta corrente ou outra conta de passivo e serviços relacionados, tais como gestão de caixa, transferências de fundos internacionais, compensação de cheques, contas a pagar e serviços de câmbio; e
- a relação entre as instituições de crédito e as instituições financeiras, incluindo quando serviços semelhantes são prestados por uma instituição correspondente a uma instituição respondente, e incluindo relações estabelecidas para transações de valores mobiliários ou transferências de fundos.

Uma relação correspondente/respondente significa que a instituição correspondente processa e/ou executa transações para os clientes da instituição respondente, e a conta da respondente é usada para processar e/ou executar a transação de seu cliente.

As relações com correspondentes estabelecidas em Países não Membros da EU exigem EDD. Elas representam riscos únicos a respeito dos quais o AAB Brasil precisa ter atenção especial, devido a preocupações sobre a dificuldade de performance de qualquer *Due Diligence* ou monitoramento dos clientes da instituição. Deve-se prestar atenção à transparência da propriedade, suas políticas de PLD/CFT, suas contas correspondentes que atendem a instituições financeiras não bancárias, como o câmbio monetário, as licenças bancárias internacionais e a força de supervisão local. A aprovação da gerência sênior deve ser obtida antes do estabelecimento de novas relações com correspondentes.

ATENÇÃO:

É proibido ter uma relação com um Banco de Fachada (*Shell Bank*), ou um banco ou outra instituição financeira que permite que suas contas sejam usadas por bancos de fachada. Um banco de fachada significa uma instituição financeira sem presença física na jurisdição que foi incorporada, envolvendo gestão relevante, e que não está afiliada a um grupo financeiro regulamentado.

5.2.3 Análise Simplificada (*Simplified Due Diligence*, ou– "SDD")

A análise SDD pode ser aplicada quando a combinação de fatores de risco relativos ao cliente, produtos ou serviços, ou localização geográfica envolvidos pode ser considerada como potencialmente baixa.

Cada linha de negócio deve preparar uma proposta escrita demonstrando por que uma combinação de segmento/produto/localização de cliente identificada deve ser submetida a procedimentos de SDD. Tais propostas requerem aprovação do Compliance e dos gestores pertinentes da linha de negócio e aprovação do Diretor de PLD/CFT para assegurar o cumprimento dos requisitos do *Dutch ML/FT Prevention Act*.

A SDD deve ser sempre suficiente para garantir que o cliente de fato cumpre todos os requisitos que permitem a SDD e deve incluir, como mínimo, a identificação e a verificação do cliente, do UBO e de outras partes relacionadas (se houver), e checagem em listas de risco de PLD/CFT internas e externas aplicáveis. Essas listas devem incluir a lista de Classificação de Riscos de Crime Financeiro no País, listas de entidades de alto risco, listas de sanções e lista de PEP e devem incluir categorias de alto risco predefinidas, por exemplo, profissões ou negócios de alto risco, conforme indicado nas políticas (comerciais) do banco, notas de orientação ou regulamentos locais. Se um cliente corresponder com uma entrada em tal lista ou categoria, o cliente deve ser tratado adequadamente. A SDD não resulta automaticamente em uma qualificação de cliente como cliente de risco neutro.

A SDD não isenta o banco de estabelecer a natureza pretendida e o propósito das atividades. Além disso, a SDD não isenta o banco do filtro e do monitoramento contínuo de transações ou do monitoramento contínuo da relação comercial para possíveis suspeitas de PLD/CFT.

5.2.4 Atualizações e Revisões

Como parte do processo contínuo de avaliação de riscos, as informações, dados e documentação necessários para avaliar o risco de um cliente devem estar atualizados para refletir a situação real. Quando alterações no perfil do cliente ou detalhes impactam os riscos de LD/FT do cliente, uma reavaliação de risco pode ser justificada. As reavaliações de risco podem ser executadas periodicamente ou com mudanças específicas no perfil de risco do cliente (eventos). As revisões periódicas ("PR") são obrigatórias para todos os clientes classificados como alto risco ou médio, para os fins de diferenciá-lo em (momento de) revisões periódicas. Para clientes classificados como risco neutro, uma revisão periódica pode ser aconselhável quando fatos e circunstâncias dão motivo para monitoramento aprimorado (por exemplo, certas atividades comerciais de alto risco). Para todos os clientes, uma revisão motivada pela ocorrência de eventos específicos (*Event Driven Review*, ou "EDR") é sempre necessária:

- quando alterações no perfil ou detalhes de um cliente dão motivos para realizá-la;

- quando o cliente solicita produtos ou serviços diferentes que podem aumentar o risco;
- quando o gerente de relacionamento ou a pessoa de contato com o cliente sabe ou suspeita que o cliente começou a se envolver em negócios que são considerados negócios de alto risco;
- quando ocorrem transações complexas, excepcionalmente grandes e em padrões incomuns, que não têm nenhuma finalidade econômica ou jurídica aparente; e
- quando forem detectados sinais de possível lavagem de dinheiro ou financiamento de terrorismo.

5.2.5 Filtragem de Cliente

Uma maneira importante de mitigar os riscos de LD/FT é a checagem de clientes, UBOs e partes relacionadas relevantes em listas (internas e/ou externas) de entidades ou indivíduos conhecidos ou suspeitos de estarem envolvidos ou que apresentam um alto risco de LD/FT. O mesmo se aplica para mitigar a violação das regulamentações de sanções através da filtragem de dados relevantes em listas de sanções aplicáveis. Para ambos os propósitos, o banco desenvolveu um conjunto de padrões e ferramentas globais de checagem de clientes. Ele deve ser implementado sempre que esta Política e a Política de Sanções do banco forem aplicáveis. O AAB Brasil considera a aplicação destas normas e ferramentas globais de filtragem de clientes um componente essencial para atender ao gerenciamento global consolidado de riscos de LD/FT. Permite também que o banco cheque de forma eficaz a sua base global de clientes para fins de LD/FT ou a pedido das autoridades competentes.

5.3 Filtragem de Transação

A segunda forma importante de mitigar os riscos de LD/FT e de violações de sanções é a checagem de transações internacionais, tanto de entrada como de saída, antes da pesquisa em listas (internas e/ou externas) de entidades ou indivíduos conhecidos ou suspeitos de estarem envolvidos em LD/FT e em listas de sanções aplicáveis. Para ambos os propósitos, o banco desenvolveu um conjunto de padrões e ferramentas globais de filtragem de transações, que deve ser implementado sempre que esta Política CAAML e a Política de Sanções forem aplicáveis.

A fim de preservar uma abordagem e metodologia consistentes, o AAB Brasil alinhou padrões, ferramentas e gerenciamento de listas globais para filtragem de clientes e de transações.

5.4 Informações que Acompanham a Transferência de Fundos

Todas as linhas de negócio devem garantir que as informações básicas sobre pagador (originador) e recebedor (beneficiário) que acompanham a transferência de fundos sejam mantidas à disposição de:

- autoridades judiciais apropriadas para ajudá-las a detectar, investigar e processar terroristas ou outros criminosos e rastrear os bens deles;
- unidades de inteligência financeira, para analisar atividades suspeitas ou incomuns e disseminá-las, quando necessário;
- instituições financeiras solicitantes, intermediárias e beneficiárias para facilitar a identificação e notificação de transações suspeitas e implementar os requisitos para medidas de congelamento e cumprimento de proibições de transações com pessoas e entidades designadas, de acordo com as obrigações estabelecidas nas resoluções do Conselho de Segurança da Organização das Nações Unidas.

Qualquer manipulação, modificação, alteração ou omissão para evitar que um pagamento seja capturado pelo processo de filtragem é visto como uma violação grave dos princípios comerciais do ABN AMRO e pode ser submetida a medidas disciplinares. Consulte a Política de Pagamento (*Payment Policy*).

A fim de detectar informações faltantes ou incompletas sobre o pagador e o beneficiário nas transferências de fundos e executar ações de acompanhamento baseadas em risco, conforme exigido pelas leis e regulamentos aplicáveis, o banco desenvolveu normas globais para rastreio de dados relevantes em transferências de fundos em que o banco está envolvido como prestador de serviços de pagamento. Estas normas incluem medidas de acompanhamento adequadas, tais como a rejeição ou suspensão da transferência de fundos, a restrição ou a cessação da relação com prestadores de serviços de pagamento em não-conformidade e a comunicação de falhas e/ou atividades suspeitas às autoridades competentes. Esses padrões devem ser implementados em todas as unidades responsáveis pelas transferências de fundos.

5.5 Monitoramento de Transação

As linhas de negócio são obrigadas a monitorar mudanças no padrão de transações em uma conta ou mudanças nas circunstâncias que não são consistentes com as transações normais e esperadas do cliente e que podem levar a uma investigação mais aprofundada. Isso é necessário para revisar o padrão de transação real em relação ao que é conhecido sobre o cliente e suas atividades e objetivos, a fim de detectar uma atividade suspeita de LD/FT que precisa ser comunicada às autoridades competentes (COAF).

Muitos países e organismos internacionais produzem listas de indicadores de atividade incomum ou suspeita com base na análise de risco de LD/FT inerente em nível nacional e supranacional. No nível de grupo, o banco mantém uma visão geral desses indicadores. Com a SIRA aplicada aos níveis do grupo e de cada linha de negócio assim como a lista de indicadores mantida ao nível do grupo, as linhas de negócio devem manter e divulgar uma lista de indicadores que lhes são aplicáveis. Devem também ser consideradas as listas aplicáveis e as avaliações de riscos nas jurisdições em que o Grupo ABN AMRO operam.

Essas listas servem de entrada para uma revisão anual da abordagem de monitoramento de PLD no nível da linha de negócio e de país, usando um formato predefinido fornecido pelo diretor de PLD/CFT (o modelo global de Monitoramento PLD/CFT Baseado em Risco – "RBA"). Parte da revisão estabelece como as atividades de transação de um cliente devem ser monitoradas com o uso de cenários do sistema automatizado de monitoramento PLD do banco ou de outra forma. Isso requer envolvimento e apoio do Compliance. As alterações da abordagem de monitoramento PLD com base na revisão anual devem ser aprovadas pela gerência de cada linha de negócio/país e, subsequentemente, enviadas ao diretor de LD/FT global para supervisão.

O Grupo ABN AMRO desenvolveu normas globais de monitoramento automatizado de transações. Estas normas devem ser implementadas em todas as unidades responsáveis pelos alertas gerados pelo sistema automatizado de monitoramento de PLD.

Independentemente das transações a serem monitoradas através da utilização de ferramentas automatizadas ou de outra forma, toda a equipe, especialmente as que são titulares ou o contato do cliente, e aqueles que cuidam de transações, têm a obrigação de comunicar ao seu gestor direto e/ou ao Compliance qualquer transação possivelmente incomum ou suspeita que for percebida. Quando uma transação possivelmente suspeita for comunicada internamente, e uma avaliação inicial resultar em novas investigações, o Compliance relevante deve ser informado.

5.6 Relato de Atividade Incomum ou Suspeita (SAR)

Com base nos requisitos de monitoramento acima mencionados, todas as linhas de negócios devem estar em posição de identificar atividades incomuns que possam resultar em suspeita de LD/FT. A linha de negócio deve reportar esta atividade ao Compliance. O Compliance é responsável por relatar às autoridades as atividades suspeitas em nome do AAB Brasil, conforme exigido pela legislação local.

É proibido informar ao cliente, diretamente ou indiretamente, de que uma SAR foi ou será realizada (fornecimento de informações privilegiadas). Isso é considerado crime na maioria

das jurisdições onde o Grupo ABN AMRO atua. Todas as medidas necessárias devem ser tomadas para evitar a divulgação não intencional de realizações de SAR ao cliente ou a outras partes.

5.7 Rejeição de Clientes/Encerramento de Relacionamento com Clientes

A (re)avaliação de risco de um cliente pode levar à recusa de qualquer cliente em potencial ou ao término de uma relação existente. Quando uma relação com o cliente é rejeitada ou encerrada com base nesta Política CAAML, os detalhes dos clientes –incluindo as razões para a rejeição ou rescisão da relação com o cliente - devem ser registrados e relatados ao Compliance.

O monitoramento de relações e/ou reavaliação periódica de risco pode resultar em uma decisão de encerrar a relação com um cliente. Ao terminar uma relação, a legislação local, toda a informação disponível e qualquer implicação devem ser consideradas, incluindo os requisitos de comunicação de atividades suspeitas.

Em vários países, o cliente tem o direito de ser informado das razões que levaram o banco a encerrar a relação (às vezes, somente mediante solicitação de um cliente). Antes de terminar a relação, o Departamento Jurídico deve ser consultado, quando for previsto que dificuldades legais podem ocorrer (incluindo o risco de fornecimento de informações privilegiadas).

6 Clientes Apresentados por Terceiros

6.1 Clientes Apresentados por Outras Entidades do Grupo ABN AMRO

É preferível reunir-se com um cliente pessoalmente antes de iniciar uma relação comercial. No entanto, sabe-se que isso nem sempre é viável, especialmente quando um cliente já tem uma relação com outra unidade do banco (incluindo as suas filiais ou *joint ventures*). Independentemente da fonte e da natureza da apresentação do cliente, ela não isenta a unidade receptora do cumprimento desta Política CAAML. A unidade que faz a apresentação deve fornecer à unidade receptora todas as informações e documentação pertinentes. É dever da unidade receptora e da unidade de apresentação informarem-se sobre quaisquer alterações materiais nas informações e dados que possam influenciar o perfil de risco do cliente.

Quando a unidade que apresenta o cliente faz parte do Grupo ABN AMRO, uma cópia da avaliação de risco mais recente deve ser enviada à unidade receptora. Isso não isenta a unidade receptora da sua obrigação de realizar a sua própria avaliação de risco considerando a sua relação específica com o cliente. As legislações sobre sigilo bancário e proteção de dados pessoais devem ser consideradas. Sempre que a legislação de sigilo bancário e de proteção de dados impedir que a unidade do Grupo ABN AMRO apresentadora do cliente forneça à unidade receptora a avaliação dos riscos, a unidade receptora deve proceder com sua própria avaliação dos riscos e garantir o cumprimento desta Política CAAML.

6.2 Terceiros

O Grupo ABN AMRO pode confiar em alguns terceiros para a realização das seguintes medidas de análise relativas aos clientes do banco:

- identificação do cliente e verificação de sua identidade;
- identificação e, quando aplicável, verificação da identidade do UBO; e
- obtenção de informações sobre a finalidade e natureza pretendida da relação comercial.

Quando o banco confia em um terceiro, a responsabilidade final pela *Due Diligence* do cliente permanece com o banco. Os terceiros em quem o banco pode confiar são:

- instituições financeiras titulares de uma licença válida e registrada numa jurisdição que, de acordo com as normas globais do banco, possuem um regime de PLD/CFT eficaz e uma supervisão rigorosa do cumprimento dessas obrigações; e
- qualquer outra parte sujeita ao registro profissional obrigatório reconhecido por lei, que tenha normas de PLD/CFT equivalentes a esta Política e seja supervisionada por um órgão regulador ou profissional de uma jurisdição que, de acordo com as normas globais do banco, possui um regime de PLD/CFT efetivo e uma supervisão rigorosa do cumprimento dessas obrigações.

NOTA: Consulte a lista de jurisdições equivalentes da Política CAAML na intranet do Compliance.

É proibido confiar em terceiros estabelecidos em países de alto risco, conforme designado pela Comissão da União Europeia. Esta proibição não se aplica à confiança em filiais e subsidiárias com maioria de participação detida pelo ABN AMRO Group N.V. e pelo AAB Holanda nesses países, uma vez que essas entidades são obrigadas a cumprir com esta política de grupo. A lista de países designados como de alto risco pela Comissão da UE é publicada na intranet do Compliance.

Exceto nos casos em que o terceiro atua como agente, o banco exige que o terceiro forneça cópias autenticadas de documentos originais que verifiquem a identidade do cliente e, quando aplicável, do(s) UBO(s).

Em qualquer ocasião em que o terceiro se recusar a agir em conformidade com estas medidas, deve haver encaminhamento à gerência da linha de negócio para consideração em conjunto com o Compliance, se necessário.

7 Exceções

7.1 A Política CAAML representa as normas mínimas que devem ser aplicadas em todas as linhas de negócio e operações do país. No entanto, sabe-se que as linhas de negócio operam num mercado comercial competitivo e, como tal, devem considerar a prática, a regulamentação e a legislação locais. Além disso, sabe-se que podem existir circunstâncias excepcionais, em que, por exemplo, as leis locais (de proteção de dados pessoais) não permitem o cumprimento dos requisitos completos de identificação, verificação e documentação do cliente, tal como descritos nesta Política. Se esse for o caso, e a administração do banco quiser continuar com o negócio, a linha de negócio ou país deve solicitar formalmente uma exceção do cumprimento de uma disposição específica desta Política.

7.2 É importante envolver o Diretores Jurídicos e de Compliance locais, fornecer explicações adequadas sobre as leis locais e aconselhar sobre possíveis alternativas e medidas mitigadoras adicionais. Tal pedido de exceção deve ser dirigido ao diretor de PLD/CFT e requer a sua aprovação. Essas aprovações de exceção são confirmadas por escrito pelo diretor de PLD/CFT e mantidas em um banco global de dados de exceções pelo Compliance. Além disso, a Política de Exceções (*Policy Deviations)* também é aplicável quando se solicita uma exceção. Exceções são concedidas apenas em casos excepcionais, nos quais as circunstâncias do mercado ou as leis/regulamentações locais constituem um argumento convincente para fazê-lo, e quando não enfraquecem outras áreas de PLD/CFT de uma linha de negócio ou de um país e não prejudicam a reputação do banco.

8 Implementação

8.1 Cada linha de negócio garante que suas políticas e procedimentos ficarão alinhados com esta Política CAAML.

8.2 Alterações à Política CAAML podem afetar os requisitos de análise (*Due Diligence*) existentes. Sempre que esse for o caso, uma nova avaliação de risco deve ser efetuada na "primeira oportunidade disponível", com base na abordagem baseada em riscos. Isso significa que a

linha de negócios deve ativamente contatar esses cliente para a condução de *Due Diligences* necessárias (adicionais). Em casos de mais alto risco, em especial quando EDD é necessária, a linha de negócios deve contatar esses clientes imediatamente. Isso também se aplica a situações em que uma SDD exige medidas adicionais devido a mudanças feitas nesta Política.

9 Atualizações

Versão	Data	Detalhes
V.05	03/2019	Revisão anual. Atualizações substanciais feitas com base na versão atualizada em 28/05/2018 da CAAML Policy 2.3. Dentre as mudanças, houve: (i) reelaboração e complementação de textos baseadas na lei de implementação da *Dutch AML/CFT*; (ii) adição da categoria de risco "média"; e (iii) mudança para que o indicador de "países de alto risco" não resulte como regra na classificação do cliente como de alto risco (depois da EDD).
V.04	04/2018	Revisão anual. Pequenas atualizações de texto.
V.03	02/2017	Integração dos apêndices na política. Mudança na definição de PEP e UBO, SDD, Implementação da 4a Diretiva Europeia sobre a Prevenção à lavagem de dinheiro, inclusões sobre clientes e filtro e monitoramento de transação como parte do projeto *Connecting the Chain*.
V.02	05/2016	Atualização da última versão da CAAML Policy de 08/09/2015, pequenas atualizações quanto ao processo local (item 4.3 e anexo III) e atualizações mínimas no texto.
V.01	06/2014	Primeira versão.

10 Aprovações AAB Brasil

A presente Política CAAML foi preparada pelo Compliance e foi revisada, discutida e aprovada pelos seguintes membros do BREC:

_____
Fausto José Caron
Diretor Presidente

_____
Mateus Praxedes
Diretor de Risco

_____
Jaques Mester
Diretor Financeiro e de Operações

_____
Nicolau Nardi
Diretor Jurídico e de Compliance

_____
Carla Ruggeri
Recursos Humanos

ANEXO

Principais Controles Globais

Escopo	Assunto	Indicador	Evidência	Referência[4]
Equipe com contato direto com o cliente	Aceitação de novo cliente	Cada linha de negócios deve conhecer e verificar a verdadeira identidade de todos os seus clientes com base em uma avaliação de risco para determinar o perfil de risco	Registros da identidade verificada de todos os clientes e formulários de avaliação de risco são mantidos	Monitoramento da aceitação do cliente (RC_CO-03.01)
Equipe com contato direto com o cliente	Atualizações e revisões	Manter informações, dados e documentação dos clientes atualizados e executar revisões periodicamente (PR) ou com base em mudanças específicas no perfil de risco do cliente (EDR)	Registros da (re) avaliação de risco e, se aplicável, informações, dados e documentos de clientes são mantidos	Monitoramento da revisão do cliente (RC_CO-03.02)
Equipe com contato direto com o cliente	Saídas do cliente	A (re) avaliação de risco pode levar, quando aplicável, ao término de um relacionamento existente	Evidência do término de um relacionamento com o cliente deve ser mantida no arquivo do cliente	Monitoramento do término do relacionamento com o cliente (RC_CO-03.03)
Equipe com contato direto com o cliente	Revisão periódica do RBA	Cada linha de negócio revisa a Abordagem Baseada em Risco em relação ao Monitoramento de Transações. Todas as transações relevantes são inseridas no sistema de monitoramento.	Documento RBA revisado e assinado. Relatório sobre a integridade dos fluxos de dados.	Revisão do RBA e da integridade da transação (RC_CO-04a-1)
Equipe operacional	Tratamento de alerta	Todos os alertas do sistema de monitoramento são avaliados por um	Resultado do tratamento de alerta	Tratamento de alerta (RC_CO-04a-2)

[4] É feita referência aos números de controle de risco de conformidade registrados na Ferramenta de Conformidade de Controle e Risco de Governança (AGRC) do AAB Holanda.

		analista de comportamentos suspeitos.		
Equipe com contato direto com o cliente e equipe operacional	Arquivamento de SAR interno	Comportamentos e/ou transações suspeitos precisam ser arquivados internamente	Detalhes do arquivamento interno de SAR	Arquivamento de SAR interno (RC_CO-04a-3)
Equipe de Compliance	Arquivamento de SAR externo	SARs reportados internamente são avaliados e reportados às autoridades relevantes.	Detalhes do arquivamento de SAR externo	Arquivamento de SAR externo (RC_CO-04a-4)
Equipe com contato direto com o cliente, GRID, equipe operacional	Reunião sobre desempenho operacional dos processos TM, CF e TF	Periodicamente, todos os acionistas na cadeia de valores discutem o desempenho operacional como parte de seu papel de supervisão.	Painéis, atas de reuniões, ações e decisões	Reunião de desempenho (RC_CO-04a-5)
Equipe de Compliance	Atualização dos Global Standards (Padrões Globais)	Garantir que o RBA, a estrutura de filtragem e os Padrões Globais de TM, CF e TF estejam alinhados com a política CAAML e as diretrizes aplicáveis.	Modelos de Padrões Globais, RBA e Estrutura de Filtragem atualizados e aprovados	Atualização dos Padrões Globais (RC_CO-04a-6)
Equipe com contato direto com o cliente e GRID	Revisão da estrutura de filtragem de clientes	A estrutura de filtragem de clientes e as configurações são revisadas periodicamente de acordo com os Padrões Globais.	Documento da Estrutura de Filtragem revisto e assinado e ajuste das configurações do sistema. Relatório sobre a integridade dos fluxos de dados.	Revisão da estrutura de filtragem de clientes (RC_CO-04c-1a)
Equipe operacional	Avaliação de alertas da Filtragem do cliente	Os alertas de clientes/parceiros de negócios e as listas de sanção e PEP são investigados pelos analistas.	Resultado da avaliação de alertas e solicitações de EDR para verdadeiros PEPs.	Avaliação de alertas (RC_CO-04c-1b)
Equipe de Compliance	Gerenciamento de listas CF e TF	Verificar se são necessárias atualizações de sanções, listas locais e PEP.	Documentação de fontes para atualizações de listas e extratos de configurações	Gerenciamento de listas (RC_CO-04c-1c)

			do sistema/filtros para atualizações.	
Equipe de Compliance	Gestão de Hits relativos a Sanções, CF e TF	Com base em hits reais de sanções, as medidas apropriadas são tomadas de acordo com os Padrões Globais.	Detalhes dos hits reais e acompanhamento das ações tomadas	Gestão de Hits relativos a Sanções (RC_CO-04c-1d)
Equipe com contato direto com o cliente e GRID	Revisão da Estrutura de Filtragem de Transações	A Estrutura de Filtragem de Transações e as configurações são revisadas periodicamente de acordo com os Padrões Globais.	Documento da Estrutura de Filtragem revisto e assinado e ajuste das configurações do sistema. Relatório sobre a integridade dos fluxos de dados.	Revisão da Estrutura de Filtragem de Transações (RC_CO-04d-1)
Equipe operacional	Avaliação de alertas na filtragem de operações	Alertas de detalhes em transações transfronteiriças de clientes e listas de sanções são investigados pelos analistas.	Resultado da avaliação de alertas e *hits* verdadeiros para o AML/ *Sanctions Desk*.	Avaliação de alertas (RC_CO-04d-2)
Equipe operacional	Avaliação de alertas na filtragem de operações FATF 16	Alertas são investigados pelos analistas com detalhes adequados do originador da informação.	Resultado de alertas e estatísticas e tendências	avaliação de alertas FATF 16 (RC_CO-04d-3)