Gerenciamento de Risco Operacional

Em atendimento à instrução nº 558 da Comissão de Valores Mobiliários (CVM), de 26 de março de 2015, a presente política visa apresentar as regras e procedimentos de controles do conglomerado econômico do Grupo Citibank no Brasil, a redação abaixo é a mesma disponibilizada para atendimento da Resolução n° 3.380, de 29 de junho de 2006, do Conselho Monetário Nacional – CMN.

A diretoria do Banco Citibank S.A., na qualidade de instituição líder do Conglomerado Financeiro Citibank Brasil, instituiu em junho de 2007 a Política de Gerenciamento de Risco Operacional, de responsabilidade da área de Operational Risk Management (ORM).

Estrutura de Governança: Papéis e Responsabilidades

Enquanto o gerenciamento dos riscos, incluindo riscos operacionais, é de responsabilidade coletiva de todos os funcionários, o Citi define papéis e responsabilidades claras para as Três Linhas de Defesa, que compõem sua Estrutura de Governança:

- **Primeira Linha de Defesa - Negócio**:

As áreas de negócio são proprietárias dos seus riscos e responsáveis pelo seu gerenciamento. Esta estrutura está organizada em 14 entidades locais que incluem as diversas áreas de negócios, suporte e operações. O responsável pela gestão de cada entidade é o Gestor Sênior membro do Comitê Executivo.

- **Segunda Linha de Defesa** - **Gestão de Risco Independente e Funções de Controle – Enterprise Risk Management, Finance, Recursos Humanos e Jurídico:**

As funções de controles do Citi estabelecem padrões para o gerenciamento dos riscos e para garantir a eficácia dos controles. Tais funções tem as seguintes caracteristicas:

- Gestão e Supervisão (estrutura organizacional) independente
- Visões e atribuições múltiplas
- Integração com as áreas de negócio

- **Terceira Linha de Defesa:**

A estrutura de Auditoria Interna fornece, de forma independente, a garantia de que os processos são confiáveis e sustentáveis e que a governança e os controles são efetivos

Operational Risk Management trabalha em parceria com as áreas de negócios (Primeira Linha de Defesa) para garantir a efetiva implementação da Estrutura de

Atividades, Procedimentos e Relatório de Controles Internos

As atividades, os procedimentos e avaliações relacionadas aos Controles Internos do Citi são efetuados através da ferramenta MCA (Manager´s Control Assessment), que consiste em um processo de auto avaliação dos riscos e controles para o Citi e que fornece estrutura de trabalho comum para avaliações amplas e consistentes de riscos e controles chaves, através de todos os negócios e funções do Citi Global, regionalmente e em cada país.

Dessa forma, o processo de Controles Internos da Citi tem início com as áreas de negócios e operacionais que durante o trimestre, efetuam mapeamento de processos, identificação de controles chaves, eventuais fraquezas de controles, riscos emergentes, testes de controle, definição de planos de ação, caso necessários, e que são inseridos no sistema CitiRisk no fechamento de cada trimestre.

Neste contexto, caso sejam identificados problemas nos controles e/ou nos testes realizados, tais problemas são registrados no sistema iCAPS para monitoração de sua resolução, incluindo o devido plano de ação para a correção do problema.

Em uma segunda etapa, as áreas de Compliance, Legal, Operational Risk, Finance e RH do Citi atuam em seu dia-a-dia, como parte de suas atividades, para assegurar o cumprimento de normas, regulamentações, leis, bem como pelo gerenciamento de risco e especialmente a área de Operational Risk também atua para assegurar que as atividades iniciais das áreas operacionais estão sendo cumpridas. A área de Compliance realiza a governança das leis e Descritivo regulamentações pelo processo de RCM que possui reuniões mensais e revisões anuais, e todas as áreas de segunda linha participam do processo de avaliação dos risco e controles de cada linha de negócio no processo de Annual Risk Assessment (ARA).

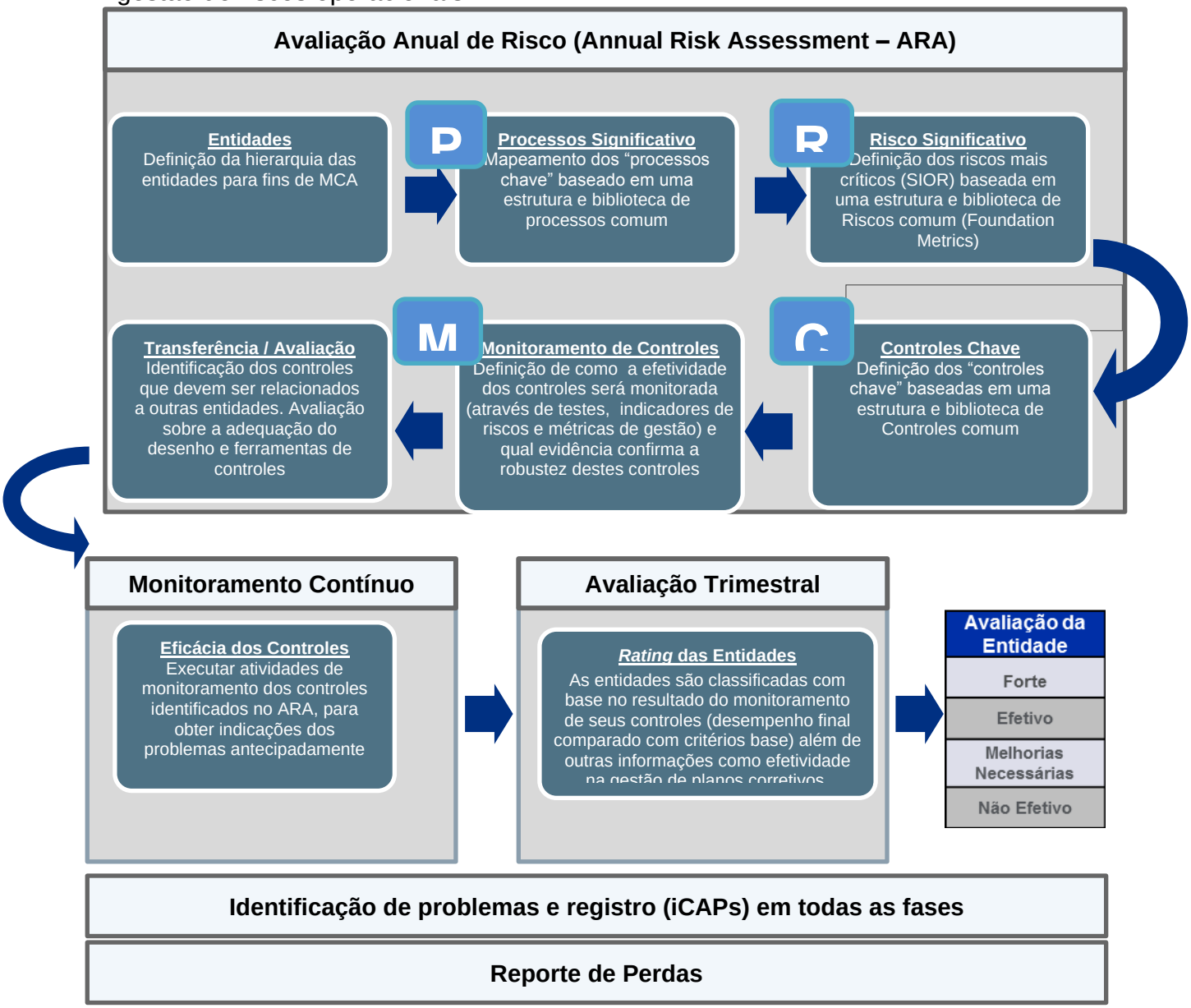
A terceira etapa é realizada pela auditoria interna que, conforme cronograma de auditoria, efetua avaliação das fraquezas de controles, riscos emergentes e testes de controle efetuados pelas áreas operacionais e testes de auditoria adicionais. Com base em tais avaliações, a auditoria interna elabora relatório de auditoria, atribuindo nota de avaliação para os resultados encontrados. As notas podem ser:

- Suficiente;
- Espaço para Melhorias;
- Limitado;
- Insuficiente.

O relatório de auditoria é encaminhado para os heads locais (head do produto e head operacional), para que os mesmos respondam e elaborem planos de ação.

Anexo I

O macro fluxo do MCA (Manager´s Control Assessment) demonstrado abaixo representa a estrutura de trabalho que permite que a 1ª linha de defesa faça a sua gestão de riscos operacionais.



Política de Confidencialidade e Segurança

Em atendimento à instrução nº 558 da Comissão de Valores Mobiliários (CVM), de 26 de março de 2015, a presente política visa apresentar as diretrizes de sigilo, conduta e segurança que devem ser seguidas pelos administradores, empregados do conglomerado econômico do Grupo Citibank no Brasil, a redação abaixo é parte integrante do Código de Conduta vigente.

Privacidade e segurança das informações dos clientes

Como parte do nosso compromisso para com a proteção de ativos tanto do Citi como dos nossos clientes, o Citi está empenhado em proteger as informações pessoais e confidenciais dos nossos clientes e em utilizá-las adequadamente.

Recolhemos, guardamos e utilizamos as informações pessoais dos nossos clientes de uma forma que nos permite proporcionar lhes escolhas e opções de produtos e serviços, conforme designado na lei. Com esta finalidade, esforçamo-nos por assegurar a disponibilidade de sistemas e tecnologias apropriados e, nessa conformidade, formar os colaboradores com acesso a essas informações. Quando utilizamos outras empresas como prestadoras de serviços, exigimos que estas protejam as informações pessoais e confidenciais que recebem.

O Citi deve cumprir as várias leis e regulamentos que governam a privacidade, confidencialidade e segurança de informação. Muitos países têm em vigor leis de proteção de dados, de sigilo bancário e profissional ou de privacidade, as quais afetam a recolha, a utilização, o arquivo e a transferência de informações pessoais e confidenciais dos clientes. Esta é uma área da lei em rápida mudança, pelo que deverá consultar o departamento jurídico interno ou o Responsável por “compliance” caso tenha alguma questão relacionada com a utilização apropriada das informações dos clientes.

É da sua responsabilidade salvaguardar todas as informações pessoais e confidenciais dos nossos clientes, assegurando que as mesmas apenas são utilizadas para fins autorizados relacionados com a sua posição e responsabilidades de trabalho e que são partilhadas apenas com pessoas autorizadas. Tem a obrigação de proteger toda as informações pessoais e confidenciais da utilização indevida por parte de terceiros, de não a divulgar a qualquer pessoa não autorizada e de não a utilizar nem permitir que seja utilizada para um fim não autorizado. Pode recolher, utilizar, aceder, manter, transportar, transmitir e divulgar informações pessoais e confidenciais apenas para o desempenho do seu cargo e dos deveres de trabalho atribuídos e deve eliminá-las apropriadamente em conformidade com a política do Citi.

Nada presente neste Código, ou em qualquer outro contrato ou política do Citi, se destina a proibi-lo ou restringi-lo de divulgar informações confidenciais a qualquer governo, agência reguladora ou autoreguladora, incluindo ao abrigo da Secção 21F da Lei de Mercado de Valores Mobiliários (Securities and Exchange Act) de 1934 e das regras daí provenientes. Não precisa de autorização prévia do Citi para fazer tais divulgações e não tem de notificar o Citi de que fez tais divulgações.

Barreiras de informação

Sempre que for necessário, as áreas de negócio do Citi devem implementar procedimentos de "barreiras de informação", procedimentos esses que os colaboradores do Citi e outros representantes devem cumprir. As barreiras de informação foram concebidas para proteger as informações não públicas potencialmente relevantes recebidas por colaboradores envolvidos em empréstimos, serviços de banca de investimento ou atividades bancárias comerciais (informações privadas) dos colaboradores que negoceiam ou prestam consultoria na negociação de títulos com base em informações publicamente disponíveis ou envolvidos em atividades de gestão de investimentos (atividades públicas). Para além disso, as barreiras de informação são também um dos métodos utilizados para solucionar conflitos de interesse potenciais e reais entre diferentes atividades. Foram também criadas várias barreiras de informação e vários procedimentos aplicáveis a unidades de negócio envolvidas em determinadas atividades privadas para evitar que as informações confidenciais sejam partilhadas com indivíduos que não estão autorizados a ter conhecimento das mesmas. É da sua responsabilidade ter conhecimento e cumprir as políticas de barreiras de informação aplicáveis à sua unidade de negócio e entidade jurídica.

Comunicações, equipamentos, sistemas e serviços

Os equipamentos, sistemas e serviços do Citi, incluindo, entre outros, computadores, telefones, correio de voz, computadores portáteis, equipamentos BlackBerry e PDA, serviços de fax, serviço de correio postal, intranet, acesso à internet, correio eletrónico, mensagens SMS, mensagens instantâneas e outras ferramentas comunicação eletrónica, dispositivos, ligações de dados e serviços de dados para utilização no local, móvel ou remota, são disponibilizados para fins comerciais e para lhe permitir efetuar as tarefas relacionadas com o seu trabalho. Deste modo, dentro do limite permitido pelas regulamentações e leis aplicáveis, o Citi poderá monitorizar e registar, em qualquer momento, a sua utilização destes equipamentos, sistemas e serviços e pode intercetar qualquer informação enviada ou recebida por si como resultado de tal utilização. Assim sendo, não deverá criar nenhuma expetativa de privacidade pessoal quando utilizar os equipamentos, sistemas e serviços do Citi.

Programa de Treinamento

Em atendimento à instrução nº 558 da Comissão de Valores Mobiliários (CVM), de 26 de março de 2015, o documento visa apresentar o programa de treinamento obrigatório que todos os funcionários e estagiários devem completar, independente da área de negócios em que atuam.

- Prevenção à lavagem de dinheiro, Sanções e Anti-Suborno e Corrupção

Orienta os funcionários sobre como evitar que recursos financeiros ilegais transitem pela nossa Organização 'Prevenção a Lavagem de dinheiro'.

- Código de Conduta

Trata dos valores, princípios e procedimentos que devem nortear o comportamento de todos os funcionários da Organização 'Citi Code of Conduct'.

- Treinamento de Fraude

Traz a definição de fraude e maneiras de identificar e prevenir situações de risco, por meio de casos práticos.

- *Securing Our Future*

Destaca a importância da segurança da informação e orienta os funcionários sobre as políticas e procedimentos para manter seguras as informações da Organização e dos Clientes.

- Tutorial *AB&C* (Anti-Suborno e Corrupção)

Aborda questões regulatórias aplicável a nível mundial em matéria de suborno e corrupção, os impactos negativos dos crimes de suborno e corrupção, políticas e conceitos gerais, prevenção e compromissos de risco.

Política de Prevenção à Lavagem de Dinheiro

Em atendimento à instrução nº 558 da Comissão de Valores Mobiliários (CVM), de 26 de março de 2015, a presente política visa apresentar as diretrizes de prevenção à lavagem de dinheiro (AML) seguida pelo conglomerado econômico do Grupo Citibank no Brasil.

Estrutura de Compliance AML

O time de Compliance AML atua de forma independente do negocio reportando ao Diretor de Compliance, cujas principais atribuições são:

1. Supervisão sobre o Programa de Lavagem de Dinheiro (PLD) e análise de riscos;

2. Revisão e aprovação dos procedimentos internos relativos à PLD e Conheça seu Cliente;

3. Divulgação das políticas relativas à PLD, Conheça seu Cliente e Sanções bem como mudanças na legislação aplicável;

4. Investigações dos casos escalados como suspeitos, agências e áreas internas ou casos divulgadas na mídia;

5. Investigações Especiais de casos relevantes publicados pela mídia;

6. Atendimentos a solicitações de informação/documentação recebidas através de ofícios e relacionadas à PLD e Conheça seu Cliente;

7. Revisão e aprovação de clientes de Alto Risco;

8. Coordenação e apresentação dos casos ao comitê de PLD para decisão sobre manutenção do relacionamento e ciência sobre os casos a serem comunicados ao COAF;

9. Comunicações ao COAF dos casos suspeitos;

10. Prover treinamentos relacionados à PLD inclusive Conheça seu Cliente, Sanções, etc.;

11. Avaliação de risco de PLD envolvendo novos produtos;

12. Aprovação de novos produtos revisão de produtos existentes através do Comitê de Produtos com foco em PLD e CFT.

Processo de Detecção dos Alertas

O Citi utiliza critérios para monitorar seus clientes, levando em consideração a movimentação de um determinado cliente contra parâmetros pré-estabelecidos, e gera “alertas” também chamados de “casos” todas as vezes que a movimentação da conta exceder o limite do segmento/produto de monitoramento. O processo utiliza vários parâmetros além dos limites financeiros como, por exemplo, desvios padrão na lógica do sistema que monitoram mudanças de comportamento; “look backs” considerando as transações de períodos anteriores; limites financeiros diferenciados, etc.

Análise dos Alertas

Os casos potencialmente suspeitos são investigados pela área, que aplica metodologia própria do Citi nas investigações dos casos suspeitos. Essa metodologia foi desenvolvida com base na análise aprofundada de seis perfis que cobrem o relacionamento com o cliente em termos de:

a) Perfil geral do cliente: o analista efetua analise geral das informações cadastrais do cliente como atividade, renda, faturamento e patrimônio informados na abertura do relacionamento ou na última revisão do KYC (Conheça seu Cliente) bem como avaliar o risco do cliente através da verificação data de nascimento, ocupação (em caso de Pessoa Física), data da constituição ou atividade declarada (em caso de pessoa Jurídica). O analista também identifica contas e produtos do cliente em outros segmentos de negócios bem como os relacionados com o cliente (sócios, procuradores, beneficiários e representantes legais).

b) Perfil demográfico: através deste perfil o analista avalia o local de nascimento do cliente (em caso de Pessoa física) ou o local de constituição da empresa (em caso de pessoas Jurídicas), endereços de cadastro versus fonte externa a fim de identificar as características físicas do local informado e compatibilidade com o cadastro e KYC do cliente, agência de abertura da conta corrente, e locais cujas transações e ou contrapartes estão concentradas.

c) Perfil socioeconômico: auxilia na identificação da condição econômica e social do cliente perante o mercado financeiro. Os produtos que o cliente tem disponíveis no banco, assim como renda e patrimônio, ou qualquer ligação com

associações externas, devem ser considerados na análise a fim de identificar quem é o cliente analisado e quais meios sociais ele está relacionado. Em caso de Pessoa Jurídica, devemos analisar o porte da empresa, faturamento e quantidade de funcionários.

d) Perfil transacional: análise do fluxo transacional dos últimos 12 meses e atividade esperada para a conta. O objetivo desta análise é avaliar se o comportamento do cliente é recorrente, se movimentação está de acordo com o perfil e a capacidade econômica do cliente. É importante ressaltar que a análise histórica dos 12 últimos meses é feita com o intuito de se obter uma visão macro sobre o fluxo transacional do cliente. Além dessa análise geral sobre a conta, o analista fará uma análise detalhada das transações nos últimos 3 meses incluindo a análise das contrapartes.

e) Perfil reputacional: análise das informações obtidas de fontes públicas e listas internas (watch list) e base de dados de mídia negativa (Softon e CitiScreening) sobre o cliente seja pessoa física ou empresa, sócios, procuradores, contrapartes e outros titulares. Esta analise também inclui bloqueios judiciais que o cliente tem ou teve.

f) Perfil de produtos: identificação e análise do uso de produtos e serviços que o cliente possui.

As pesquisas, análises e conclusões sobre os casos são documentadas no “Relatório do Caso” (Case Log de Compliance). É importante salientar que os analistas de Compliance também podem solicitar esclarecimentos adicionais sobre o cliente ao gerente de relacionamento ou especialista do produto.

Nos casos onde houver algum indício de que o cliente pode estar envolvido em crimes de LD/FT, outra atividade criminosa, ou outra situação que traga risco para o Citi, o analista de Compliance deverá escalar o caso ao AML Compliance Officer ou seu designado, que tem a responsabilidade por avaliar se há necessidade de investigação adicional e decidir se o caso deve ser comunicado ao Coaf e escalado ao Comitê de PLD.

Comunicação ao COAF

A competência para decidir sobre comunicações de operações ao COAF é do Country AML Compliance Officer (AMLCO) e Country Chief Compliance Officer (CCCO). Em casos mais relevantes o Comitê de PLD participa da discussão e decisão sobre as comunicações. É importante salientar que em casos de divergência nas deliberações

sobre as comunicações ao Coaf, a decisão final é do AMLCO e do CCCO. Com relação à manutenção do relacionamento com clientes envolvidos em suspeitas de lavagem de dinheiro a competência é do Comitê de PLD.

Avaliação de Riscos de PLD em Novos Produtos

Em 2013, o Citi definiu através de sua “Política Global de PLD para Novos Produtos” processo que estabelece requerimentos de prevenção à lavagem de dinheiro que devem ser cumpridos antes do lançamento de todos os novos produtos, serviços, expansão de linhas de negócios e aquisições (incluindo fusões e joint ventures).

Todos os novos produtos são avaliados através do processo de aprovação de novos produtos que utiliza o sistema global “NPA”. O objetivo desse sistema é gerenciar e registrar o processo de aprovação bem como garantir que os riscos de PLD sejam adequadamente avaliados antes dos produtos serem lançados.