Manual de Risco Operacional
Investment Management Brazil

ARX Investimentos Ltda.

Versão

Responsável	Alteração	Data
Risco Operacional	Criação do manual resumido para publicação no site.	Junho de 2016
Risco Operacional	Revisão e ajustes de redação.	Janeiro de 2019
Risco Operacional	Revisão periódica.	Abril de 2020
Risco Operacional	Revisão periódica.	Junho de 2022
Risco Operacional	Revisão periódica e inclusão de versionamento.	Abril de 2024

ÍNDICE

1 INTRODUÇÃO

O presente manual se aplica a todas as sociedades da linha de negócios de "Investment Management" do The Bank of New York Mellon Corporation no Brasil, notadamente a ARX Investimentos Ltda. ("ARX"), também designada neste manual como "companhia", conforme o caso.

2 OBJETIVO

Este manual tem como objetivo estabelecer os procedimentos e rotinas da área de Risco Operacional alocada na linha de négocio de Investment Management do grupo BNY Mellon no Brasil.

3 SISTEMAS ENVOLVIDOS

São utilizados os sistemas proprietários do grupo BNY Mellon, baseados na web.

4 PROCEDIMENTOS

4.1 Eventos de Risco Operacional

O evento de risco operacional é a materialização do risco operacional e pode ou não resultar em perda ou ganho financeiro, para o cliente ou para a instituição. Os eventos podem ser classificados nas seguintes categorias:

- Perda Efetiva – Perda financeira do cliente ou da empresa associado a um evento de risco operacional. Cabe esclarecer que perdas relacionadas ao risco de crédito não são consideradas perdas operacionais.
- Perda Potencial – Evento onde um erro operacional foi identificado e pode gerar perda financeira ou ganho fortuito, mas o resultado ainda não foi determinado.
- "*Near Miss*" ou Quase erro – Evento onde uma perda potencial ou um ganho inesperado não chegou a se materializar, mas o erro não foi evitado pelos controles já implantados.

4.1.1. Notificações e reporte de eventos

Conforme estabelecido nas políticas coorporativas do grupo:

- Os funcionários devem comunicar imediatamente a sua gestão todos os eventos de risco operacional que venham a identificar, independentemente do impacto financeiro.
- São chamados "*Significant Event*" ou evento significativo aquele onde a perda ou ganho provável seja de USD 10.000 (dez mil dólares) ou mais.
- Eventos classificados como *"Significant Event"* devem ser comunicadas no prazo máximo de 30 dias.
- *"Significant Event"* que gere perda ou ganho superior a USD 50.000 (cinquenta mil dólares), deve ser reportado no prazo de 72 horas, a partir da data de determinação, para a Alta Administração, conforme determina a política corporativa do grupo.
- Eventos classificados como "*Near Miss*" ou quase erro que possam gerar perdas ou ganhos superiores à USD 10 milhões, devem ser reportados no prazo de 24 horas, a partir da data de determinação, para a Alta Administração, conforme determina a política corporativa do grupo.
- Relatórios internos de eventos de risco operacional são considerados informação confidencial e devem ser tradados conforme estabelecido nas políticas internas do grupo.

Todos os "*Significant Events*" são reportados, mensalmente, no Management Meeting do Investment Management EMEA & LatAM, através de relatório próprio.

Todos os eventos são reportados no Comitê de Compliance e Risco da ARX.

A área de Risco Operacional é responsável pelo monitoramento de eventuais ações propostas para corrigir/evitar novos erros operacionais. O monitoramento do status das ações é consolidado na plataforma de risco operacional do grupo, ou no diretório de rede da área, conforme a criticidade do caso.

4.1.2. Registro dos eventos

A área de Risco Operacional disponibiliza um formulário para registro dos eventos, que é preenchido pelo funcionário caso algum erro operacional seja identificado, podendo ter impacto financeiro ou não. Todos os formulários são salvos no diretório de rede da área.

Caso trate-se de um "*Significant Event*" ou "*Near Miss*", classificado como elegível à registro na plataforma do grupo, a área de Risco Operacional registrará o evento.

O formulário contém as principais informações relativas à origem do evento e a ação remediadora, caso aplicável, estabelecida em conjunto com a área responsável. O registro e acompanhamento dos eventos de risco operacional são realizados conforme definido nas políticas corporativas do grupo.

4.1.3. Associação financeira dos eventos

A associação dos eventos com o lançamento contábil é realizada manualmente na plataforma do grupo. Para que a associação financeira seja realizada na plataforma, mensalmente, a equipe de Finance Accounting envia para a área de Risco Operacional os lançamentos contábeis realizados no mês anterior nas contas de risco operacional associadas a companhia.

4.1.4. Encerramento de eventos na plataforma

O evento de risco operacional deverá ser encerrado quando:

a. A informação do evento estiver completa e precisa;
b. A perda financeira estiver lançada contabilmente e associada ao evento; e
c. A ação remediadora, caso aplicável, estiver concluída.

4.2 Risk Control Self-Assessment

O Risk Control Self-Assessment ("RCSA") é o documento central de mapeamento de riscos do grupo BNY Mellon. Esse documento fornece uma visão geral dos riscos do negócio e os controles existentes para mitigar estes riscos.

O RCSA deve ser atualizado pelo menos anualmente ou caso ocorra alguma mudança significativa que impacte o negócio.

4.3 Key Risk Indicators

Indicadores chave de risco ou Key Risk Indicators ("KRI") são métricas relacionadas a aspectos críticos do negócio que são monitoradas e comparadas com padrões/limites definidos pelo grupo. Estes padrões e limites são definidos com base na tolerância de risco de cada negócio.

A área de Risco Operacional faz o acompanhamento mensal dos indicadores chaves definidos internamente. Adicionalmente, existem alguns KRIs que são definidos corporativamente e são acompanhados por todas as boutiques de Investment Management do grupo.

Caso algum indicador esteja acima da tolerância definida, a área de Risco Operacional fará um acompanhamento junto à área responsável pelo processo e, caso necessário, completará uma análise da origem e da ação corretiva.

4.4 Risk Assessments

De forma a mapear, avaliar e definir os riscos associados a determinados produtos, serviços e processos são realizados, sempre que necessário, procedimentos de avaliação de risco ou "risk assessments".

4.4.1. Produtos e/ou serviços novos ou modificados significativamente

Conforme definido nas políticas corporativas:

- Produto e/ou serviço novo é um produto ou serviço que nunca foi oferecido pelo negócio ou que aumente significativamente o perfil de risco do negócio.

- Produto e/ ou serviço modificado significativamente é um produto ou serviço que já existe, mas que foi alterado de forma que o seu perfil de risco tenha sido significativamente alterado.

Desta forma, um novo produto/serviço só poderá ser lançado após a aprovação do *Risk Assessment* pela alta administração do negócio, pelo responsável por Risco Operacional no negócio e pelo Comitê de Compliance e Risco local.

A área responsável pelo produto/serviço e a área de Risco Operacional são responsáveis, respectivamente, pela descrição do produto e pela avaliação de risco.

Serão documentados os riscos significantes associados ao produto, bem como as ações para que os riscos sejam mitigados.

4.4.2. Processos de Prevenção à Lavagem de Dinheiro e Anticorrupção

Periodicamente são realizados os *Risk Assessments* dos processos e procedimentos relacionados à prevenção a lavagem de dinheiro ("AML") e anticorrupção. Essas avaliações de risco são realizadas para cumprimento das normas do grupo e, para registrar a avaliação, utiliza-se um sistema corporativo, baseado na web.

4.5 Risk Appetite

Como uma instituição financeira global e diversificada, o grupo BNY Mellon atua em áreas de negócio onde se precisam assumir riscos. No entanto, ao mesmo tempo em que é inerente ao nosso modelo de negócio assumir riscos, devemos fazê-lo de forma responsável e controlada, considerando o risco associado.

Apetite ao risco ou "*Risk Appetite*" é o nível agregado de risco que uma empresa está disposta a assumir depois de considerar os seus objetivos estratégicos, seu plano de negócios, os principais riscos enfrentados pelo negócio e sua capacidade de risco.

A declaração de apetite de risco do negócio é um documento desenvolvido anualmente pela área de Risco Operacional em conjunto com o negócio. Ele é elaborado em linha com o apetite de risco do grupo, e considera especificamente a atividade, o ambiente e estratégia da linha de negócio, além da região e do país onde o negócio está localizado.

4.6 Business Acceptance Committee

De forma a garantir que os produtos e serviços oferecidos pelo negócio estão dentro de suas capacidades operacionais, tolerâncias de risco e seguiram os processos de aprovação adequados foi implantado um procedimento chamado *Business Acceptance Committee* ("BAC"), que objetiva atender as políticas corporativas do grupo BNY Mellon.

Mensalmente, a área de Risco Operacional monitora a entrada, saída e alterações de produtos e serviços. As evidências desse monitoramento ficam registradas no diretório da área.

4.7 Comitê de Compliance e Risco

O Comitê de Compliance e Risco da ARX tem por objetivo reportar e discutir com a alta administração da companhia a adequação das práticas adotadas na gestão de carteiras de investimento à legislação e regulação vigentes, bem como às políticas internas estabelecidas.

A reunião desse comitê ocorre trimestralmente, conforme estabelecido em seu regimento interno, reportando sua atividade aos principais executivos da companhia.

4.8 Plano de Contingência do Negócio

O Plano de Contingência define quais e quantos funcionários serão necessários durante a ocorrência de qualquer desastre, e quais outros recursos serão indispensáveis para recomeçar as atividades de uma maneira progressiva. O escopo do plano é cobrir um desastre e/ou uma situação de contingência.

Todas as rotinas e premissas do plano de contingência da companhia são desenvolvidos, atualizados e centralizados no sistema de gerenciamento de crise do grupo BNY Mellon, baseado na web.

4.8.1. Controles de Segurança Cibernética

Em conjunto com o Plano de Contingência do Negócio, foi elaborado o Plano de Recuperação Cibernética, que resume os procedimentos e ações implementadas para mitigar os impactos de um ataque cibernético. O escopo desse documento é identificar os riscos potenciais de "*cyber-attacks*", avaliando as ameaças e métodos de ataque, assim como as estratégias de mitigação correspondentes.

Adicionalmente, o plano estabelece o "*Cybersecurity Incident Response*", que é o processo pelo qual o grupo BNY Mellon identifica, investiga, responde, recupera e aprende com uma falha na confidencialidade, integridade e/ou disponibilidade de um ativo relevante. O processo de resposta à incidentes de segurança cibernética é realizado de forma centralizada pelo grupo BNY Mellon.

Caso um funcionário suspeite que um incidente cibernético está ocorrendo, ele é orientado a abrir um evento de registro do incidente. Além disso, ele deve reportar o evento ao seu gerente direto e ao coordenador do Plano de Contingência do Negócio.

A equipe de "*Information Security*" do grupo BNY Mellon trabalha para: (i) limitar os efeitos adversos de ameaças externas ou internas à rede de informações do grupo; (ii) minimizar perdas e/ou danos às informações eletrônicas dos nossos clientes; e (iii) manter a reputação da empresa. Essa equipe é responsável pela supervisão de todos os sistemas e redes de computadores do grupo BNY Mellon. A equipe é acionada sempre que ocorre um incidente de segurança de informação grave e orienta as respostas a todos os incidentes que afetam a capacidade da empresa de fazer negócios ou prejudicam sua reputação.

O plano também estabelece os procedimentos de comunicações corporativas e externas e é revisado anualmente.