Manual de Risco Operacional
Investment Management Business

Maio 2016
Revisado em Janeiro 2019

ARX Investimentos Ltda.

BNY Mellon Alocação de Patrimônio Ltda.

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") e a BNY Mellon Alocação de Patrimônio Ltda. ("BNYM Alocação"), também designadas neste manual como "companhia" ou "companhias", 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 seguintes sistemas proprietários do grupo BNY Mellon, baseados na web: Risk Management Platform ("RMP") e Crisis Management System ("CMS").

4 PROCEDIMENTOS

3.1 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 final 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.

3.1.1. Notificações e reporte de eventos

Conforme estabelecido nas politicas 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 events"* devem ser comunicadas no prazo máximo de 30 dias.
- *"Significant events"* que gerarem perdas ou ganhos superiores a USD 50.000 (cinquenta mil dólares), devem ser reportados no prazo de 5 dias, para uma lista de distribuição definida na política coorporativa I.G.031.
- Eventos classificados como "*Near Miss*" ou quase erro que possam gerar perdas ou ganhos superiores à USD 100 milhões deverão ser reportados à alta administração.
- Relatórios internos de eventos de risco operacional são considerados informação confidencial e devem ser tradados conforme estabelecido nas politicas internas do grupo BNY Mellon.

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

Todos os eventos serão reportados, trimestralmente, no Comitê de Compliance e Risco.

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 será consolidado na plataforma de risco ("RMP").

3.1.2. 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: *F:\Risco Operacional & Controles Internos AM\1 Asset & Wealth Management\OpRisk Events\ano\XX mês*.

Caso trate-se de um "*significant event*", a área de Risco Operacional registrará o evento na plataforma de risco, Risk Management Platform (link disponível na intranet do grupo). Após acessar a plataforma deve-se seguir o seguinte procedimento:

a. Entrar em *Operational Risk Events (OpRisk)*;
b. Entrar em *Create Risk Event*;
c. Preencher o formulário de registro com base nas informações do formulário fornecido pela área que reportou o evento;

d. Clicar em *Save;*
e. Clicar em *Print Event* e salvar o registro (como pdf) no diretório: *F:\Risco Operacional & Controles Internos AM\1 Asset & Wealth Management\OpRisk Events\ano\XX mês.*

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 na política coorporativa I.G.031.

3.1.3. Associação financeira dos eventos

A associação dos eventos com o lançamento contábil é realizada manualmente na plataforma de risco, seguindo o procedimento abaixo:

a. Entrar em *Operational Risk Events (OpRisk)*;
b. Entrar em *View or Modify Risk Events*;
c. Clicar em *Retrieve Risk Events*;
d. Clicar no *Risk Event ID* desejado;
e. Clicar em *Relate G/L Transactions to Event*;
f. Escolher os critérios de busca no campo *G/L Transaction Selection Criteria* e clicar em *Retrieve G/L Transaction*;
g. Selecionar o(s) lançamento(s) contábil (eis) associado (s) e clicar em *Save.*

Para que a associação financeira seja realizada na plataforma de risco, mensalmente, a equipe de Finance Accounting envia para a área de Risco Operacional (via procedimento de Key Risk Indicators, descrito adiante nesse manual) os lançamentos contábeis realizados no mês anterior nas contas de risco operacional associadas às empresas de Investment Management no Brasil.

3.1.4. 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.

Para encerrar o evento na plataforma deve-se seguir o seguinte procedimento:

a. Entrar em *Operational Risk Events (OpRisk)*;
b. Entrar em *View or Modify Risk Events*;
c. Clicar em *Retrieve Risk Events*;
d. Clicar no Risk Event ID desejado;
e. Selecionar a opção "*Closed*" no campo "*Event Status*" e clicar em "*Save*".

3.2 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.

O RCSA é composto de:

a. Resumo do perfil da empresa;
b. Resumo e classificação dos riscos inerentes ao negócio;
c. Resumo dos controles associados a estes riscos;
d. Avaliação da adequação dos controles para mitigar os riscos inerentes;
e. Análise dos riscos residuais;
f. Avaliação da direção dos riscos residuais; e
g. Registro dos planos de ação para os gaps associados aos controles.

O RCSA é atualizado na plataforma de risco ("RMP"). A metodologia utilizada para coleta das informações segue a política corporativa I.G.037.

3.3 High Level Assessment

A avaliação de alto nível ou High Level Assessment ("HLA") é uma avaliação qualitativa realizada pela área de Risco Operacional em conjunto com o negócio que tem por objetivo avaliar a qualidade dos controles existentes, os fatores internos e externos que impactam o negócio e o perfil de risco do negócio.

Periodicamente, o relatório High Level Assessment é atualizado na plataforma de risco, conforme estabelecido na política I.G.036. Esse relatório é composto dos seguintes itens:

a. Análise de risco resumida;
b. Novos riscos e mudanças relevantes no modelo de negócio;
c. Novos produtos desenvolvidos; e
d. Status das atividades/projetos da área de risco operacional.

3.4 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 definidos internamente, através do procedimento indicado abaixo:

1º passo: Solicitar por email aos responsáveis por cada indicador a informação.
2º passo: Salvar as informações no diretório: *F:\Risco Operacional & Controles Internos AM\1 Asset & Wealth Management\KRI\Material Recebido\AAAA\MM.*
3º passo: Consolidar as informações na planilha geral que fica no diretório: *F:\Risco Operacional & Controles Internos AM\1 Asset & Wealth Management\KRI\Material Recebido\AAAA.*
4º passo: Acessar a plataforma "RMP" e incluir as informações dos indicadores no item *Key Indicators (KRI/KPI).*

OBS: Para incluir o KRI na plataforma deve-se seguir o seguinte procedimento:

a. Entrar em *Operational Risk Events (OpRisk)*;
b. Entrar em *View or Modify Risk Events*;
c. Clicar em *Retrieve Risk Events*;
d. Clicar no Risk Event ID desejado;
e. Selecionar a opção "*Closed*" no campo "*Event Status*" e clicar em "*Save*".

Adicionalmente, existem alguns KRIs (chamados de *Risk Metrics*) 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.

3.5 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".

3.5.1 Produtos e/ou serviços novos ou modificados significativamente

Conforme definido na política coorporativa I.G.034:

- 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.

Conforme estabelecido na política corporativa I.G.034, um novo produto/serviço só poderá ser lançado após a aprovação do *Risk Assessment* pela alta administração do negócio, pelo responsável pelo 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.

3.5.2 Processos de Prevenção a 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.

3.6 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.

O apetite de risco do negócio é 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 também considera especificamente a atividade, o ambiente e estratégia da linha de negócio relevante, além da região e do país onde o negócio está localizado.

3.7 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 a politica corporativa I.G. 033. Esta política descreve os

padrões do grupo para a aceitação de novos produtos e serviços, e também descreve os requisitos de documentação, aprovação e de governança do grupo.

Mensalmente, a área de Risco Operacional monitora a entrada, saída e alterações de produtos e serviços. As evidencias desse monitoramento ficam registradas no diretório: *F:\Risco Operacional & Controles Internos AM\1 Asset & Wealth Management\Business Acceptance Committee\Relatórios\AAAA\MM.*

3.8 Comitê de Compliance e Risco

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

A reunião do comitê ocorre trimestralmente, reportando suas atividades aos principais executivos das companhias.

3.9 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 das companhias são desenvolvidos, atualizados e centralizados no sistema de gerenciamento de crise chamado *Crisis Management System*, um sistema de propriedade do BNY Mellon, baseado na web.

3.9.1 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, o mesmo é orientado a notificar o "*Technology Help Desk*" do grupo e 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 "*Computer Security Incident Response*" 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 cliente; 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. As principais responsabilidades da equipe são:

- Avaliar a gravidade do incidente;
- Realizar uma investigação imediata do incidente;
- Controlar e gerenciar o incidente;
- Notificar a gerência sênior; e
- Normalizar imediatamente a atividade principal do negócio afetado.

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

Este documento é revisado anualmente.

3.10 Relatórios e rotinas sob demanda

Alguns relatórios e rotinas são realizados sob demanda, tais como:

Cliente	Report	Periodicidade
IM BNYM	SLA IM EMEA	Mensal
IM BNYM	IM EMEA Management Meeting	Mensal
Diversos	Revisão e aprovação de DDQs	Sob Demanda
IM BNYM	Model Risk Report	Sob Demanda
IM BNYM	Treinamentos	Sob Demanda