INSTRUTIVO N.º 28/16
de 16 de Novembro

ASSUNTO: Governação do Risco de Operacional

Considerando o estabelecido no Aviso.º 07/2016 de 22 de Junho sobre Governação do Risco, as Instituições financeiras devem adoptar funções, políticas e processos de gestão de risco para a identificação, avaliação, monitorização, controlo e prestação de informação sobre o risco operacional;

Nestes termos, e ao abrigo das disposições combinadas das alíneas d) e f) do artigo 21.º e alínea d) do número 1 do artigo 51.º, ambos da Lei n.º 16/10, de 15 de Julho – Lei do Banco Nacional de Angola e do artigo 90.º da Lei n.º 12/15, de 17 de Junho – Lei de Bases das Instituições Financeiras.

DETERMINO:

1. Definições

Sem prejuízo das definições estabelecidas na Lei de Bases das Instituições Financeiras, para efeitos do presente Instrutivo, entende-se por:

1.1 **Factor de risco**: aspecto ou característica que influencia o risco. Na avaliação dos riscos são relevantes, nomeadamente, as características dos produtos e mercados financeiros, dos mutuários e dos processos em vigor nas Instituições.

1.2 **Posição em risco**: exposição relativa a um activo, um elemento extrapatrimonial ou um instrumento financeiro derivado, acrescido de proveitos de qualquer natureza não recebidos que se encontrem

reflectidos contabilisticamente como valores a receber, independentemente de se encontrarem vincendos ou vencidos, de acordo com os critérios do Manual do Plano Contabilístico das Instituições Financeiras.

2. Identificação

2.1 As Instituições devem compreender os aspectos relevantes do risco operacional, em relação às suas actividades de negócio, sendo necessário garantir a classificação de eventos de risco operacional através de um conjunto de critérios objectivos, devidamente documentados, conforme estabelecido no **Anexo I** que é parte integrante do presente Instrutivo, nomeadamente:

a) fraude interna;
b) fraude externa;
c) práticas em matéria de emprego e segurança no local de trabalho;
d) clientes, produtos e práticas comerciais;
e) danos ocasionados a activos físicos;
f) perturbação das actividades comerciais e falhas do sistema;
g) execução, entrega e gestão de processos.

2.2 As Instituições devem considerar factores internos e externos, incluindo condições macroeconómicas e de mercado, que possam ter um impacto negativo, real ou potencial, nas suas actividades de negócio.

2.3 As Instituições devem considerar a possibilidade das fontes de risco operacional e concentração estarem relacionadas com as características das actividades ou estrutura organizacional.

3. Avaliação

3.1 Os colaboradores responsáveis pelo risco operacional devem estar envolvidos na avaliação do risco operacional e respectiva concentração e, quando aplicável, devem envolver as restantes funções de controlo

interno, sendo que o histórico de perdas deve fazer parte dessa avaliação.

3.2 As Instituições devem ter à sua disposição ferramentas de avaliação do risco operacional, designadamente:

a) observações de auditoria;
b) recolha e análise dos dados de perdas internas;
c) recolha e análise de dados externos, designadamente valores de perdas, datas, recuperações e informações sobre as causas associadas;
d) avaliação do risco, tendo em consideração as categorias do risco operacional referidas no **Anexo I** que é parte integrante do presente Instrutivo;
e) mapeamento dos processos de negócio para identificar os procedimentos, actividades e funções organizacionais, determinando os principais focos de risco;
f) indicadores do risco e desempenho, métricas e/ou estatísticas, que fornecem uma visão interna do risco, particularmente informações em relação a vulnerabilidades, falhas e perdas potenciais;
g) análise de cenários sobre os processos de negócio para identificar potenciais eventos de riscos operacionais e avaliar o seu potencial resultado;
h) comparação dos resultados das várias ferramentas de avaliação para fornecer uma visão mais compreensiva do perfil de risco operacional da Instituição.

4. Requisitos gerais de monitorização e controlo

4.1 Para a monitorização e controlo do risco operacional as Instituições devem considerar os factores de risco relevantes, a capacidade de assumir risco, o apetite ao mesmo, a sua condição financeira e a sua estratégia.

4.2 As Instituições devem assegurar que os métodos internos de fixação de preços e de avaliação de desempenho têm em consideração o risco operacional, por forma a estarem alinhados com o apetite ao risco e capacidade de assumir o mesmo.

4.3 As Instituições devem desenvolver políticas de monitorização de conformidade que incluem, designadamente:

a) acompanhamento do progresso das actividades tendo em conta os objectivos estabelecidos pelo órgão de administração;
b) verificação da conformidade com os controlos de gestão;
c) revisão do tratamento e resolução de situações de não conformidade;
d) avaliação dos processos de aprovação para assegurar a responsabilização de um nível da gestão apropriado;
e) monitorização dos relatórios de excepções e desvios às políticas.

4.4 Os processos e procedimentos de monitorização e controlo devem incluir um sistema para assegurar o cumprimento com as políticas mencionadas no ponto anterior.

4.5 As Instituições devem assegurar o funcionamento e efectividade dos controlos internos destinados à mitigação do risco operacional, designadamente:

a) processos de aprovação;
b) monitorização da aderência aos limites impostos;
c) protecção do acesso à informação da Instituição e sua utilização;
d) processo contínuo para a identificação de linhas de negócio e produtos onde é verificado um desalinhamento entre os retornos verificados e os esperados;
e) regras de verificação e reconciliação de transacções e contas;
f) política que assegure a continuidade das funções dos colaboradores em períodos de ausência.

4.6 Sem prejuízo do ponto anterior, as Instituições devem considerar os mecanismos de mitigação do risco como complementares e não como

substitutos de um completo e efectivo controlo interno do risco operacional, verificando se reduzem realmente o risco, se o transferem para outro sector ou área de negócio ou se criam um novo risco.

4.7 As Instituições devem estabelecer mecanismos de teste e processos sólidos de resolução de problemas identificados.

4.8 As Instituições devem garantir que a abordagem das "três linhas de defesa", disposta no **Anexo II** que é parte integrante do presente Instrutivo, está em funcionamento e, quando solicitado, explicar as acções do órgão de administração e dos colaboradores com responsabilidades de direcção na prossecução desse objectivo.

5. Monitorização e controlo - planos de continuidade de negócio

5.1 As Instituições devem desenvolver e, se necessário, executar planos de continuidade de negócio, para assegurar a capacidade de operar numa base contínua e limitar perdas em casos extremos e diferentes cenários de vulnerabilidade.

5.2 As Instituições devem identificar operações críticas e dependências, internas e externas, assim como a respectiva capacidade de superar os efeitos adversos decorrentes.

5.3 Os planos de continuidade de negócio devem conter os seguintes elementos:

a) estratégias de contingência;
b) procedimentos de recuperação e reinício das actividades;
c) planos de comunicação para informar os colaboradores, as autoridades reguladoras, clientes, fornecedores e, quando apropriado, autoridades civis;
d) prioridades de recuperação.

5.4 As Instituições devem realizar um teste de recuperação de desastre e continuidade de negócio, devendo os resultados ser reportados aos colaboradores com responsabilidades de direcção e ao órgão de

administração, para que possam ser tidos em conta na elaboração e ajustamento dos planos de continuidade de negócio.

5.5 As Instituições devem rever periodicamente os seus planos de continuidade de negócio, de forma a assegurar que a respectiva estratégia de contingência continua alinhada com as operações, riscos e ameaças, e capacidade de enfrentar efeitos adversos.

6. Prestação de informação

6.1 As Instituições devem definir, formalizar, implementar e rever periodicamente políticas e processos para a prestação de informação, que devem ser adequados à sua natureza, dimensão, complexidade e perfil de risco

6.2 Na prestação de informação interna, as Instituições devem fornecer os principais resultados das etapas de identificação, avaliação, monitorização e controlo do risco operacional e respectiva concentração, ao órgão de administração e aos colaboradores com responsabilidades de direcção, que deve incluir, no mínimo:

a) resumos das posições em risco agregadas da Instituição;
b) cumprimento com as políticas, processos e limites de risco operacional, assim como situações em que os limites foram excedidos identificando as razões e os colaboradores responsáveis pela aprovação;
c) detalhes de eventos internos do risco operacional recentes e perdas associadas;
d) eventos externos relevantes e qualquer impacto potencial na Instituição ou nos seus fundos próprios regulamentares;
e) desenvolvimentos em novos produtos ou iniciativas de negócio;
f) resultados dos testes de esforço;
g) informação qualitativa e, quando apropriado, quantitativa das concentrações inter e intra-risco.

6.3 Na prestação de informação externa, as Instituições devem definir, formalizar e implementar políticas e processos para transmitir às partes interessadas informação abrangente, que deve incluir, no mínimo:

a) informação qualitativa, sobre:
   i. estratégias de investimento e respectivos processos;
   ii. estrutura e organização da função de gestão do risco operacional;
   iii. ferramentas utilizadas para a identificação e avaliação do risco operacional;
   iv. âmbito e natureza da prestação de informação e dos sistemas de avaliação do risco;
   v. estratégias e processos para monitorizar a contínua efectividade das posições de cobertura ou de mitigação;
   vi. explicação da abordagem das "três linhas de defesa".

b) informação quantitativa, sobre:
   i. exposição global bruta e a exposição média bruta durante o período em questão, discriminando os principais tipos de posições em risco;
   ii. eventos de risco operacional e respectivas consequências nos resultados da Instituição;
   iii. requisito de fundos próprios para risco operacional, de acordo com o Aviso sobre requisito de fundos próprios regulamentares para risco operacional.

6.4 A periodicidade da prestação de informação deve reflectir a materialidade e natureza das fontes do risco de operacional, especialmente em relação à sua volatilidade, e estar devidamente disposta nas políticas e processos previstos no ponto 8.1 do presente número.

6.5 Os relatórios elaborados numa base extraordinária não podem ser usados como substitutos da prestação de informação regular.

7. Sanções

O incumprimento das normas imperativas estabelecidas no presente Instrutivo constitui contravenção punível nos termos da Lei de Bases das Instituições Financeiras.

8. Disposição transitória

As Instituições devem estar em conformidade com o disposto no presente Instrutivo nos termos das disposições transitórias do Aviso N.º 07/2016 de 22 de Junho, sobre Governação do Risco.

9. Dúvidas e omissões

As dúvidas e omissões resultantes da interpretação e aplicação do presente Instrutivo são resolvidas pelo Banco Nacional de Angola.

10. Entrada em vigor

O presente Instrutivo entra em vigor na data da sua publicação

PUBLIQUE-SE

Luanda, 16 de Novembro de 2016

O GOVERNADOR

VALTER FILIPE DUARTE DA SILVA

ANEXO I - Categorias do Risco Operacional

Categoria do risco operacional (nível 1)	Eventos do risco operacional	Categorias (nível 2)	Exemplos (nível 3)
Fraude interna	Perdas decorrentes de actos destinados intencionalmente à prática de fraudes, à apropriação indevida de activos ou a contornar legislação, regulamentação ou políticas empresariais, com excepção de actos relacionados com a diferenciação/discriminação, que envolvam, pelo menos, uma parte interna da empresa	Actividades não autorizadas	Transacções não reportadas de forma intencional Transacções não autorizadas, com perdas materiais Falha intencional em assumir posições
		Furto e fraude	Fraude / fraude de crédito / depósitos sem valor Roubo / extorsão / desfalque Apropriação indevida de activos Destruição maliciosa de activos Falsificação Contrabando Tomada de contas / Personificação / etc. Evasão fiscal Subornos / Corrupção Negociação com informação privilegiada
Fraude externa	Perdas decorrentes de actos destinados intencionalmente à prática de fraudes, à apropriação indevida de activos ou a contornar legislação por parte de um terceiro	Furto e fraude	Roubo Suborno
		Segurança dos sistemas	Danos de *hacking* Roubo de informação, com perdas materiais
Práticas em matéria de emprego e segurança no local de trabalho	Perdas decorrentes de actos que não se encontram em conformidade com legislação ou acordos de trabalho, saúde ou segurança, bem como do pagamento de danos pessoais ou de actos relacionados com a diferenciação/discriminação	Relações com os colaboradores	Compensação, benefícios, assuntos de terminação Sindicatos laborais
		Segurança no trabalho	Responsabilidade geral Saúde dos colaboradores e regras de segurança Compensação dos colaboradores
		Diversidade e discriminação	Todos os tipos de discriminação
Clientes, produtos e práticas comerciais	Perdas decorrentes do incumprimento intencional ou por negligência de uma obrigação profissional relativamente a clientes específicos (incluindo requisitos fiduciários e de adequação) ou da natureza ou concepção de um produto	Adequação, divulgação e fiduciário	Quebras de fiduciariedade / violação de orientações Adequação / problemas de divulgação Violação da divulgação de clientes de retalho Violação de privacidade Práticas de venda agressivas Uso indevido de conta de clientes Uso impróprio de informação confidencial Responsabilidades do mutuante
		Práticas de negócio ou de mercado impróprias	*Antitrust* Negociação imprópria / práticas de mercado Negociação com informação privilegiada, por conta da instituição Actividade não licenciada Lavagem de dinheiro
		Falha no produto	Defeitos nos produtos
		Selecção, patrocínio e exposição	Erros nos modelos
		Actividades de consultoria	Disputas para a execução das actividades de consultoria
Danos ocasionados a activos físicos	Perdas decorrentes de danos ou prejuízos causados a activos físicos por catástrofes naturais ou outros acontecimentos	Desastres e outros eventos	Perdas associadas a desastres naturais
Perturbação das actividades comerciais e falhas do sistema	Perdas decorrentes da perturbação das actividades comerciais ou de falhas do sistema	Sistemas	Hardware Software Telecomunicações Disrupções de energia
Execução, entrega e gestão de processos	Perdas decorrentes de falhas no processamento de operações ou na gestão de processos, bem como das relações com contrapartes comerciais e vendedores	Captação de transacções, execução e manutenção	Falhas na comunicação Processamento de dados, manutenção e erro de carregamento Incumprimentos de prazo ou responsabilidades Falhas no modelo / sistema Erro contabilístico / Erro de atribuição de entidade Eerro de atribuição de entidade Falhas no desempenho de outras tarefas Falha na entrega Falha na gestão de garantias reais Manutenção de Dados de Referência
		Monitorização e prestação de informação	Falha na prestação de informação obrigatória Imprecisão de prestação de informação externa
		Aceitação de clientes e documentação	Falta de permissões dos clientes Falta ou incompletude de documentos legais
		Gestão das contas cliente	Acesso a contas não aprovado Registos de contas de clientes incorrectos Danificação negligente dos activos dos clientes
		Contrapartes de transacções	Incumprimento de uma contraparte não clientes Disputas de contrapartes não clientes
		Prestadores de serviços e fornecedores	Subcontratação Disputas de prestadores de serviço

Anexo II – Abordagem das "Três Linhas de Defesa"

1. A primeira linha de defesa é a gestão das unidades de negócio. Significa isto que uma sólida governação do risco operacional reconhece que a gestão das unidades de negócio é responsável pela identificação e gestão dos riscos inerentes a produtos, actividades, processos e sistemas pelos quais são responsabilizáveis.

2. A segunda linha de defesa corresponde à função corporativa do risco operacional independente, complementando as actividades de gestão do risco operacional das unidades de negócio. O nível de independência da função corporativa do risco operacional pode variar entre Instituições. Para Instituições de menor dimensão, a independência pode ser alcançada através da segregação de funções e da revisão independente de processos e funções. Para Instituições de maior dimensão, a função corporativa do risco operacional deve ter uma estrutura de prestação de informação independente das linhas de negócio que aceitam o risco, e deve ainda ser responsável pelo estabelecimento, manutenção e o desenvolvimento contínuo do enquadramento do risco operacional dentro da Instituição. Adicionalmente, a função corporativa do risco operacional pode ainda ser responsável pela avaliação do risco operacional, pelos processos de prestação de informação, comités do risco e responsabilidades para a prestação de informação ao órgão de administração. Uma das responsabilidades chave da função corporativa do risco operacional é o desafiar a informação fornecida pelas unidades de negócio e as avaliações da gestão do risco. Para o desempenho efectivo das suas funções, a função corporativa do risco operacional deve ser composta por um número suficiente de colaboradores com a formação e experiência adequadas.

3. Finalmente, a terceira linha de defesa corresponde a uma revisão e desafio independente aos controlos, processos e sistemas da gestão do risco operacional da instituição.

Os colaboradores responsáveis pelas revisões devem ter a formação e competências adequadas, e não devem estar envolvidos no desenvolvimento, implementação e operacionalização do enquadramento para a gestão do risco operacional.