Este modelo incorpora as medições relativas às variáveis básicas da avaliação do risco de crédito – Probabilidades de *Default* (PD), Perdas em caso de *Default* (LGD) e Factores de Conversão de Crédito Fora de Balanço (CCF), considerando ainda a incerteza associada a estas medidas ao incorporar também a volatilidade destes parâmetros. Para além disso, o modelo também considera efeitos de diversificação/concentração de risco de crédito, entrando em linha de conta com os graus de correlação entre os diversos sectores de actividade económica.

Em Dezembro de 2010, o capital económico associado ao risco de crédito correspondia a 40,6% do capital económico não diversificado total do Grupo, o que se traduz num acréscimo de 5,1 p.p. neste peso face a Dezembro de 2009.

RISCO OPERACIONAL

O risco operacional materializa-se por via das perdas resultantes de falhas ou da inadequação dos processos internos, das pessoas ou dos sistemas ou ainda pela ocorrência de eventos externos.

Para a gestão e controlo deste tipo de risco, o Grupo tem vindo a adoptar, de forma crescente e muito relevante, um conjunto de princípios, práticas e mecanismos de controlo claramente definidos, documentados e implementados, de que são exemplos:

- A segregação de funções;
- As linhas de responsabilidade e respectivas autorizações;
- A definição de limites de tolerância e de exposição aos riscos;
- Os códigos deontológicos e de conduta;
- Os indicadores-chave de risco (*key risk indicators* – KRI);
- Os controlos de acessos, físicos e lógicos;
- As actividades de reconciliação;
- Os relatórios de excepção;
- Os planos de contingência;
- A contratação de seguros;
- A formação interna sobre processos, produtos e sistemas.

Assim, visando-se uma cada vez maior eficiência na identificação, avaliação, controlo e mitigação das exposições ao risco, o Grupo tem vindo, desde 2006, a reforçar o seu sistema de gestão do risco operacional e a alargar a sua abrangência às principais operações no exterior.

A adopção de uma aplicação de suporte comum a todas as subsidiárias e o acompanhamento por parte do Risk Office do Grupo asseguram um elevado nível de uniformidade na gestão do risco entre as várias operações, muito embora se registem estágios de evolução diferenciados, atendendo à implementação faseada do referido sistema de gestão e às prioridades atribuídas em função da materialidade das exposições.

O reconhecimento da política de gestão e controlo de risco operacional delineada resultou na aprovação do Banco de Portugal relativa à utilização do método *Standard* (TSA) para o cálculo dos requisitos de fundos próprios para a cobertura do risco operacional. Esta aprovação foi concedida com efeitos a partir de Março de 2009 (inclusive) ao Grupo, em base consolidada, abrangendo também, em base individual, os Bancos sediados em Portugal.

Em consonância com a evolução futura do *framework* de gestão do risco operacional, o Grupo ambiciona vir a adoptar o Método de Medição Avançada (AMA), cujos requisitos regulamentares são, na sua maioria, comuns aos do método *Standard*.

Em 2010, destacam-se as seguintes concretizações no âmbito da gestão do risco operacional:

- Consolidação da base de dados de eventos de perda operacional nas principais operações do Grupo;
- Realização de novos exercícios de auto-avaliação de riscos em Portugal, na Polónia e na Grécia e o lançamento deste instrumento de gestão de risco na Roménia e em Moçambique;

- Utilização progressiva de indicadores de risco (KRI) na monitorização preventiva dos riscos de processos de Portugal, Polónia, Grécia e Roménia;
- Incorporação mais efectiva da informação proporcionada pelos instrumentos de gestão do risco na identificação de acções de melhoria sobre os processos.

ESTRUTURA DE GESTÃO DO RISCO OPERACIONAL

A gestão do risco operacional assenta numa estrutura de processos *end-to-end*, definida para todas as subsidiárias do Grupo, beneficiando-se, dessa forma, de uma percepção mais abrangente dos riscos, decorrente de uma visão integrada das actividades desenvolvidas ao longo da cadeia de actividades de cada processo.

O conjunto dos processos definidos para cada entidade é dinâmico, sendo ajustado e diferenciado em função das práticas operacionais e de negócio de cada uma, por forma a cobrir todas as actividades relevantes desenvolvidas.

A responsabilidade pela gestão dos processos foi atribuída a *process owners* que têm por missão:

- Caracterizar as perdas operacionais capturadas no contexto dos seus processos;
- Realizar a auto-avaliação dos riscos (*risks self-assessment* – RSA);
- Identificar e implementar as acções adequadas para mitigar exposições ao risco, contribuindo para o reforço do ambiente de controlo interno;
- Monitorizar os indicadores de risco (KRI).

Em Portugal, os *process owners* são designados pelo Comité de Acompanhamento de Processos (CAP), com base no reconhecimento dos seus conhecimentos e experiência no âmbito das actividades dos processos de que são responsáveis, cabendo também a este órgão a responsabilidade por:

- Aprovar a definição dos *dossiers* de processo;
- Aprovar a instituição de novos processos, definindo, caso a caso, a necessidade da respectiva certificação ISO 9001 e identificando os processos que, fora da certificação, devam ter medição de desempenho (*key performance indicators* – KPI);
- Alinhar as práticas da gestão por processos com a realidade das unidades de estrutura intervenientes nos mesmos;
- Assegurar a produção, manutenção e divulgação interna de documentação e informação sobre a gestão por processos;
- Aprovar as alterações a processos já instituídos, bem como o desenho dos novos processos.

Nas restantes geografias, a nomeação dos *process owners* cabe aos respectivos Conselhos de Administração.

AUTO-AVALIAÇÃO DOS RISCOS OPERACIONAIS

O objectivo da auto-avaliação dos riscos é o de promover a identificação e a mitigação (ou mesmo eliminação) de riscos, actuais ou potenciais, no âmbito de cada processo. A classificação de cada risco é obtida através do seu posicionamento numa matriz de tolerância, para três cenários diferentes, o que permite:

- Determinar o risco inerente aos processos, sem considerar os controlos existentes (risco inerente);
- Avaliar a exposição dos vários processos aos riscos, considerando a influência dos controlos existentes (risco residual);
- Identificar o impacto das oportunidades de melhoria na redução das exposições mais significativas (risco objectivo).

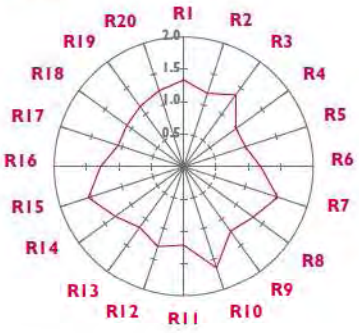
Os exercícios de RSA são baseados em *workshops*, assistidos pelo Risk Office e com a participação dos *process owners* e *process managers* ou em questionários enviados aos *process owners* para actualização dos resultados, em função de critérios de actualização pré-definidos.

Estes exercícios são também utilizados para capturar informação sobre o impacto na reputação que advém da ocorrência dos riscos operacionais avaliados, na medida em que estes são os que mais directamente se relacionam com risco reputacional.

Em 2010, a auto-avaliação de riscos operacionais foi realizada pela primeira vez na Roménia e em Moçambique, tendo sido igualmente concluídos novos exercícios em Portugal, na Grécia e na Polónia. Tal permitiu obter, para cada processo definido nessas operações, resultados relativos à respectiva exposição aos riscos operacionais. As exposições mais significativas serão mitigadas através de medidas correctivas identificadas no próprio exercício de RSA, as quais serão priorizadas em função da magnitude dos riscos em causa, sendo a respectiva implementação monitorizada através da aplicação de suporte à gestão do risco operacional.

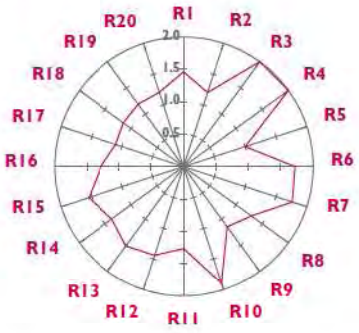
Os gráficos seguintes apresentam os resultados dos RSA realizados em 2010 em Portugal, Polónia e Grécia, relativamente ao *score* médio de cada uma das 20 subtipologias de risco definidas para o risco operacional, no conjunto dos processos avaliados, sendo que a linha exterior representa um *score* de 2,0, numa escala de 0 (menos grave) a 5 (mais grave).

PORTUGAL



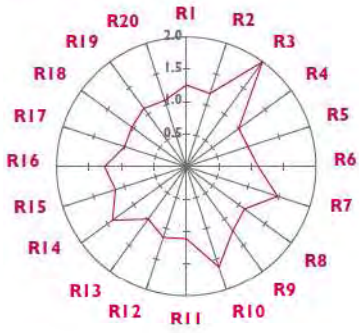
R1 Fraude interna e roubo
R2 Execução de transacções não autorizadas
R3 Relações com Colaboradores
R4 Violação dos regulamentos de higiene e segurança
R5 Discriminação sobre Colaboradores
R6 Perda de Colaboradores-chave
R7 *Hardware* e *software*

POLÓNIA



R8 Infra-estruturas de comunicações
R9 Segurança de sistemas
R10 Execução e manutenção de transacções
R11 Monitorização e reporte
R12 Relações com Clientes
R13 Concepção de produtos/serviços
R14 Fraude externa e roubo
R15 Desastres e danos nos activos

GRÉCIA



R16 Obrigações regulamentares, legais e fiscais
R17 Práticas comerciais ou de mercado incorrectas
R18 *Outsourcing*
R19 Outros problemas de relações com terceiros
R20 Riscos de projectos

PERDAS OPERACIONAIS

A identificação e registo de perdas operacionais é uma responsabilidade de todos os Colaboradores, cabendo aos *process owners* um papel relevante na dinamização da captura de dados sobre as perdas verificadas no âmbito dos seus processos. O Risk Office também procede à identificação e registo de perdas operacionais, a partir da análise de dados oriundos de áreas centrais.

O principal objectivo da captura de dados relativos a eventos de perda operacional é o de reforçar a consciencialização para este tipo de risco e facultar, aos *process owners*, informação relevante que devem incorporar na gestão dos seus processos. Para além disso, a base de dados de perdas operacionais é também um importante instrumento para, no futuro, vir a suportar o cálculo das necessidades de capital regulamentar. Acresce ainda que os dados das perdas operacionais são utilizados para *backtesting* dos resultados dos RSA, possibilitando assim a aferição das classificações atribuídas a cada processo, relativamente às 20 subtipologias de risco operacional.

As perdas operacionais identificadas são relacionadas com um dado processo e registadas na aplicação de gestão do risco operacional do Grupo, sendo caracterizadas pelos respectivos *process owners* e *process managers*. A caracterização completa de uma perda operacional inclui, para além da descrição da respectiva causa-efeito, a sua valorização e, quando aplicável, a descrição da acção de mitigação identificada (a partir da análise da causa da perda), implementada ou a implementar.

TEMAS DO PROGRAMA	DESTINATÁRIOS	ESTADO AVANÇO DA FORMAÇÃO	MÉDIA TESTES DE AVALIAÇÃO	GRAU DE SATISFAÇÃO COM OS CONTEÚDOS
Ética e Responsabilidade	Todos os Colaboradores	Concluídos 2 dos 5 subtemas	90%	79%
Branqueamento de capitais		Não iniciada		
Prevenção e Segurança		Iniciada		
Abertura de Contas	Áreas Comerciais e de Operações	Concluída	95%	79%
Venda de Produtos e Serviços	Áreas Comerciais e de Marketing	Não iniciada		
Crédito	Áreas Comerciais e de Operações Direcção de Crédito Direcção de Recuperação de Crédito	Não iniciada		
Execução de Transacções		Não iniciada		

O Programa iniciou-se em Junho de 2010, com o tema "Ética e Responsabilidade", com um seminário que teve como orador Roberto Carneiro. Para complementar as acções específicas de formação e consolidar os conhecimentos adquiridos, foi criado um *site* na Intranet dedicado apenas ao tema cultura de rigor, onde estão disponibilizados os documentos e filmes que dão suporte ao programa.

Paralelamente, o Compliance Office continuou a publicar comunicações internas na Intranet, designadas "E se um dia acontece …" e "Formação num Minuto", com o objectivo de dar a conhecer situações que envolvem riscos de reputação e de *compliance* e transmitir as melhores práticas de actuação perante as mesmas. Durante o ano de 2010 foram publicadas 30 comunicações.

Foi também mantida a prática de formação permanente em matérias de branqueamento de capitais e financiamento do terrorismo (AML/CTF), controlo interno, abuso de mercado e fraude, técnicas de monitorização de transacções e alterações de legislação (DMIF, publicidade, ética, deveres de informação, entre outros).

NÚMERO DE COLABORADORES FORMADOS (1)

AML/CTF, Abuso de Mercado, Controlo Interno, Monitorização de Transações e Temas Legais

	'10	'09	'08	VAR. % '10/'09
Actividade em Portugal	767	445	n.d.	72,4%
Actividade Internacional (2)	13.515	5.542	n.d.	143,9%
TOTAL	**14.282**	**5.987**	**n.d.**	**138,6%**

(1) O mesmo Colaborador pode ter frequentado diversas formações.
(2) Exclui Angola e Suíça em 2009.

Dos Colaboradores formados em Portugal 33% desempenham funções directivas e 67% desempenham funções técnicas.

PRINCIPAIS ACTUAÇÕES DO COMPLIANCE OFFICE

O Compliance Office tem por missão assegurar que sejam cumpridos os regulamentos e normativos (internos e externos) que pautam a actividade do Banco e das suas associadas, de forma a evitar o risco de a Instituição incorrer em sanções de carácter legal e em prejuízos financeiros ou de ordem reputacional, decorrente do incumprimento das leis, códigos de conduta e regras de "boas práticas" negociais.

A actual estrutura do Compliance Office em Portugal, onde se encontra o Group Head of Compliance, integra as áreas de Compliance Risk Control, Compliance Risk Assessment, Corporate & Legal e uma área de ligação com as unidades de *compliance* das Instituições do BCP no exterior – International Compliance Offices – que garante a transversalidade da função no Grupo BCP no que respeita aos princípios e políticas de *compliance*.