1
Introdução

1.1
Contexto e objetivo do trabalho

O estudo proposto avalia a atual relevância conferida ao Risco Operacional, no que tange, em princípio, à atuação da indústria financeira nas pesquisas sobre o tema; e, sobretudo, à dimensão de tais riscos no contexto de outras indústrias, no caso desta pesquisa na indústria Petroleira.

Embora o enfoque dado ao risco operacional, para as instituições financeiras, tenha evoluído consideravelmente, esta pesquisa almeja avaliar a perspectiva do risco operacional para instituições não financeiras, em particular para indústrias de Petróleo, uma vez que a ocorrência de falhas nos processos de negócio, possivelmente, causaria perda exorbitante para qualquer indústria.

O tema em questão vem despertando amplo interesse em inúmeras e variadas instituições mundiais, acelerado pelo avanço exponencial de novas tecnologias, e da crescente complexidade dos processos de negócio e dos sistemas automatizados de informação. Comparativamente ao setor financeiro é notória a carência de metodologias de gestão de riscos difundidas e compartilhadas nas demais indústrias.

O objetivo desta pesquisa é entender, sobretudo, como esse tipo de risco é enfrentado pelas organizações não financeiras; bem como adaptar a literatura existente a uma análise pontual; e ilustrar um pequeno estudo de caso, mais especificamente na área de operações com derivativos para realização de hedge operacional (petróleo e derivados).

Medidas para mensurar os riscos de mercado e crédito foram as principais fontes de pesquisas acadêmicas em finanças até meados dos anos 90. Foi a partir de eventos envolvendo fraudes e erros humanos, que ocasionaram além de perdas catastróficas, também a bancarrota de grandes instituições, surge a necessidade de explorar e entender outro tipo de risco.

É pertinente, neste caso, citar algumas situações clássicas de falência de grandes corporações. Há, por exemplo, o episódio decorrido na *Arthur Andersen* [empresa de auditoria dos Estados Unidos], com escândalos que denegriam a reputação do grupo; no caso *Barings*, [renomada companhia bancária da Inglaterra] – destacam-se as fraudulentas operações em derivativos; e há, também, o caso de uma grande perda do banco suíço de investimento UBS, por consequência do erro de um funcionário, cujo prejuízo totalizou cem milhões de dólares.

Mas, afinal, o que é risco operacional? Como medir os riscos operacionais? Existem mecanismos de controle eficientes contra esses riscos?

Marcelo Cruz, Ph.D. em Matemática Financeira, foi CEO e fundador do RiskMaths, autor de *Modelagem, Avaliação e Proteção para o Risco Operacional*, descreve em sua obra que o Risco Operacional (RO), inicialmente, foi definido com afirmativas – "o risco não comensurável" –; e negativas – "tudo aquilo que não é mercado ou crédito".

A fim de alcançar total compreensão sobre o tema em questão e, com isso, classificar o risco operacional para as outras indústrias, não é possível deixar de voltar os olhos para todos os progressos, relacionados à classificação e mensuração de riscos, realizados por instituições financeiras até o momento.

A definição mais amplamente difundida foi instituída em 2006 pela organização, estabelecida na Basiléia (Suíça), composta por várias autoridades em supervisão bancária dos bancos centrais – O Comitê da Basiléia.

O Comitê da Basiléia é uma organização que congrega autoridades de supervisão bancária, visando fortalecer a solidez e segurança do sistema bancário internacional, estabelecer padrões de conduta e melhorar a qualidade da supervisão bancária. Os acordos definidos por este Comitê são ratificados por mais de 100 países por todo mundo.

O primeiro acordo, Basiléia I, ocorreu em 1988, e teve como objetivo criar exigências mínimas de capital, que deveriam ser respeitadas por bancos comerciais, como precaução contra o risco de crédito.

Diversas críticas foram feitas em relação à Basiléia I por não conseguir evitar inúmeras falências de instituições financeiras na década de 90.

Em junho de 2004, o Comitê divulgou o Novo Acordo de Capital da Basiléia, intitulado "Basiléia II", mais complexo e extenso que o anterior. As

principais mudanças acarretadas pelo Novo Acordo constam no fim da padronização generalizada. Considerando um enfoque mais flexível, ou seja, dando ênfase nas metodologias de gerenciamento de risco dos bancos, na supervisão das autoridades bancárias e no fortalecimento da disciplina de mercado.

É válido mencionar que, pela primeira vez, um acordo da Basiléia introduziu e classificou o risco operacional, devendo este ser classificado e medido isoladamente. Verifica-se que, quase em sua totalidade, as pesquisas e publicações sobre o risco operacional estão voltadas para a indústria financeira, tanto no aspecto regulamentar, quanto nos aspectos de análise e gestão.

O acordo firmado na Basiléia designa uma série de padrões quantitativos que devem ser aplicados nos modelos de mensuração avançadas.

Um desses padrões descreve que qualquer sistema interno de medição do risco operacional deve ser coerente com definições determinadas. As definições limitam o escopo àquele definido pelo Comitê, no Parágrafo nº 644 – "o risco de perdas resultantes de falhas dos processos internos, pessoas, sistemas ou eventos externos" [Fonte: BCBS – *Basel Comittee on Banking Supervision*].

Essa definição inclui o risco legal e, no entanto, exclui o risco estratégico e de reputação. O Acordo de Capital de Basiléia II classifica o risco considerando a causa da perda, que pode pertencer às seguintes categorias:

- Fraude interna;
- Fraude externa;
- Descumprimento de normas para os empregados, e normas de segurança no local de trabalho;
- Descumprimento de normas empresariais, para clientes e para produtos;
- Danos a ativos físicos;
- Interrupção dos negócios, falhas de sistema; e
- Falhas na gerência de processos.

No Brasil, conforme definido pelo Banco Central, o risco operacional é a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas; ou perdas resultantes de eventos externos, o que inclui o risco legal associado à inadequação ou deficiência

em contratos firmados pela instituição, às sanções em razão do descumprimento de dispositivos legais, e às indenizações por danos a terceiros, decorrentes das atividades desenvolvidas pela instituição. Essa definição visa atender aos procedimentos direcionados à implementação da nova estrutura de capital descritos no acordo da Basiléia II.

Em pesquisa realizada pela empresa Deloitte Touche Tohmatsu [empresa prestadora de serviços de consultoria e auditoria. Fundada em 1845, possui mais de 700 escritórios em 150 países contando com 120.000 profissionais], intitulada *Global Risk Management Survey* (2009), retrata o modelo atual de gestão em instituições financeiras – os principais progressos e deficiências –, e apresenta os novos desafios dessas instituições no recente cenário da pós-crise. Para tal análise, avaliaram-se pouco mais de cem instituições financeiras, cujos ativos totais eram superiores a dezenove trilhões de dólares.

Alguns resultados apontam que:

- Somente 36% das instituições participantes relataram ter um programa de *Enterprise Risk Management* (ERM), ou equivalente, implementado. Nenhuma das instituições que se identificavam como banco de investimento possuía esse tipo de programa.

- Aproximadamente 90% dos programas de ERM nas instituições participantes cobriam risco de crédito e de mercado.

O risco operacional, que se tornou foco devido à Basiléia II, foi incluído em praticamente todos os programas de ERM, demonstrando que foi avaliado, quase universalmente, como um risco fundamental a ser gerenciado. Ainda que o estímulo à adoção ao ERM seja baixo, as instituições que o adotaram já perceberam a relevância do risco operacional no contexto em que se insere.

Após vasta pesquisa, não se encontrou nenhuma referência bibliográfica semelhante a essa, que pudesse elucidar o nível de maturidade de gestão de riscos em outros setores. Não foi localizada sequer uma definição, nem classificação dos riscos operacionais para as demais indústrias. Cada indústria tem a sua peculiaridade. O risco ambiental, por exemplo, para algumas indústrias é altamente relevante, pois possivelmente ocasionaria perdas catastróficas; já para as instituições financeiras, não representaria risco significativo.

Para fortalecer ou até mesmo esclarecer alguns conceitos, nos capítulos subsequentes foi realizada uma extensa revisão da bibliografia que caracteriza o risco operacional segundo a indústria financeira. No capítulo 1.2 tratamos de sua definição e classificação, seguindo as diretrizes da Basiléia II. No capítulo 1.3 estão expostas metodologias e padrões de gestão de riscos, e para fechar estes conceitos o capítulo 1.4 trata da gestão de riscos operacionais especificamente. Alguns destes conceitos orientarão a condução do estudo de caso em outras indústrias. O capítulo 1.5 trata de como o tema é abordado por outras indústrias, com ênfase na indústria do Petróleo.

Considerando todo o panorama exposto acima, este trabalho pretende explorar os *frameworks* e metodologias, desenvolvidos pela indústria financeira, por meio de extensa revisão bibliográfica dos métodos qualitativos e quantitativos desenvolvidos para os bancos com a finalidade de avaliar e mensurar os riscos operacionais. O cerne desta análise é a ampliação desses conceitos, a serem aplicados em outras instituições e, neste estudo, em especial, na indústria de Óleo e Gás.

1.2
Definindo o risco operacional

O intuito deste capítulo é explorar como o risco operacional foi estudado e classificado nas instituições financeiras, levantando conceitos e método disponíveis no mercado e na literatura acadêmica. Para isso, foi feita uma prévia seleção da literatura existente, tanto em relação à identificação e classificação, como também sobre as abordagens de mensuração que serão detalhados nos capítulos subseqüentes.

Por ser esta a definição mais difundida, partir-se-á da proposição divulgada pela Basiléia (2004): "o risco operacional é definido como o risco de perdas resultantes de falhas dos processos internos, pessoas, sistemas ou de eventos externos. Essa definição inclui o risco legal, mas exclui o risco estratégico e de reputação". Define-se que o risco legal inclui, mas não está limitado a multas, sanções ou indenizações decorrentes de ações de fiscalização ou por questões privadas.

O acordo da Basiléia é composto por três pilares, ou seja, três alicerces que sustentam os padrões a serem seguidos na gestão de riscos. O primeiro Pilar está relacionado ao requerimento mínimo de capital e os métodos aceitos pela Instituição – parcela mínima exigida dos bancos para cobrir os riscos de crédito, de mercado e de operação. O segundo Pilar relaciona-se ao processo de revisão de supervisão dos órgãos reguladores e como se preparar para ele. E o terceiro abrange aspectos para a disciplina de mercado. Estes pilares incentivam a maior compreensão do risco e seus mecanismos de controle, e por isso serão explorados nesta pesquisa.

O foco central desta proposta de análise será o primeiro pilar, pois nele encontram-se as exigências e incentivos para o cálculo do risco. Esse cálculo tem a intenção de medir o tamanho do risco potencial, que uma instituição estaria exposta em dias de cenários adversos, e desta forma alocar uma determinada quantia de capital que possibilite cobrir esta perda, garantindo assim o equilíbrio no mercado.

A retenção de capital pode ser feita de três formas: através de um Indicador Básico (BIA); do Método Padrão (ASA); e de Métodos de Mensuração Avançada (AMA).

A metodologia mais básica (BIA) utiliza um multiplicador para cada unidade de negócio, definido pelo órgão regulador, o resultado da multiplicação deste fator pela receita financeira desta unidade de negócio resultará no capital a ser alocado. As abordagens mais sofisticadas explicitam o valor real do risco e seu maior entendimento, permitindo a menor alocação de capital, a medida que a instituição seja capaz de comprovar a robustez e confiabilidade no seu método.

Os bancos são incentivados a moverem-se ao longo do espectro de abordagens disponíveis, mas espera-se que os bancos internacionalmente ativos e os bancos com significativa exposição ao risco operacional utilizem uma abordagem mais sofisticada do que o indicador básico.

Carol Alexander [Operational Risk, 2003, p262] afirma que, historicamente, os modelos avançados geram menor alocação de capital. Além disso, apresentam outras vantagens, pois possibilitam um melhor entendimento das perdas operacionais e também fornecem informações e estimativas de perdas futuras.

Contudo, por envolver uma complexidade maior, a autora sugere que os modelos sejam aplicados em processos-chave, que apresentam um histórico de

perda, e, assim, gerem valor para a empresa à medida que os riscos relevantes sejam mais bem administrados. Kessler (2008) complementa que "a modelagem estatística é necessária, mas não suficiente".

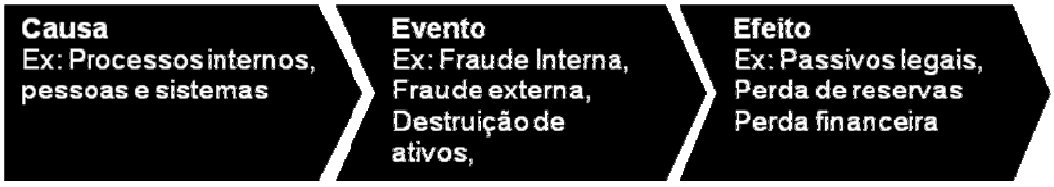
A quantificação é apenas uma das maneiras de medir os riscos, a outra forma é saber que a abordagem qualitativa é, também, uma importante forma de medição e, sob condições de incerteza, é tão útil quanto a quantitativa. O gestor de riscos operacionais deve ser capaz de responder:

- Em que linguagem os resultados devem ser expressos? (Linguagem)
- Em quais objetos e quais ambientes os resultados devem ser aplicados? (Especificação)
- Como os resultados podem ser usados? (Padronização)
- Como a confiança nos resultados é avaliada, e como seu resultado é aproveitado? (Exatidão e Controle)

O *framework* proposto pela Basiléia para a abordagem AMA é, necessariamente, flexível. Entretanto, um elemento essencial, que merece uma discussão aprofundada, é a exigência de dados.

Victor Dowd (2003) afirma que um modelo de mensuração deve conter uma definição clara do que precisa ser medido. O problema é que a definição torna alguns riscos difíceis de serem mensurados. A identificação e a classificação do risco originam um mapa de riscos que fornece informações sobre os riscos que são aplicáveis ao negócio, aos processos ou à unidade organizacional, além de especificar em que grau de intensidade eles estão.

Para auxiliar a resolução desse problema, os órgãos regulatórios e as indústrias desenvolveram um conceito mais complexo de risco operacional, baseado na distinção entre causa, evento, e efeito conforme ilustrado a seguir:



Fonte: Livro - Operational Risk: Regulation, Analysis and Management

Figura 1.1: Análise de Risco Operacional através de causa, evento e efeito

A figura acima estrutura o conceito e a relação entre causa e efeito dos riscos, exemplificando, as falhas nos processos internos (causa), podem provocar a destruição dos ativos (evento), e por conseqüência ocorrer a perda financeira. Esta definição padroniza e facilita a classificação de riscos, além de permitir o entendimento de suas correlações.

Conforme foi visto anteriormente, a Basiléia divide o risco operacional em categorias de eventos. Essa definição já fornece um padrão de classificação. Com a ajuda da indústria, o BCBS (2004), desenvolveu uma matriz com sete categorias, que são definidas e divididas em subcategorias.

As sete categorias em seu nível mais abrangente – nível 1 são: fraude interna; fraude externa; descumprimento de normas para empregados e de segurança no local de trabalho; descumprimento de normas empresariais para clientes e para produtos; danos a ativos físicos; interrupção dos negócios; falhas de sistema; e falhas na gerência de processos. Categorias que funcionam como uma alternativa para que os bancos possam alcançar o escopo de eventos de perda operacional, em sua totalidade.

Nesta matriz, para cada uma das sete categorias há uma definição comum, exemplo, o evento "destruição dos ativos" é definido como: perdas decorrentes de danos aos ativos físicos devido à desastres naturais ou outros eventos. As categorias podem ter dois níveis, de forma que a torne mais específica – a destruição de ativos pode ocorrer em função de desastres ou outros eventos como: Perdas por desastres naturais ou Perdas humanas por fontes externas (terrorismo, vandalismo), além disso, está representada uma série de atividades usadas como exemplo. A matriz supracitada pode ser vista abaixo:

Tabela 1.1: Classificação de RO – Basel II

Categoria do Tipo de Evento (Nível 1)	**Definição**	**Categorias (Nível 2)**	**Exemplos de atividades (Nível 3)**
Fraude interna.	Perdas em função de atos fraudulentos intencionais, apropriação in-devida de bens ou burla de regulamentos, leis ou políticas da companhia, eventos discriminatórios, os quais envolvam, pelo menos, uma parte interna.	Atividade não autorizada.	- Transações não declaradas (intencional); - Tipo de transação não autorizada (com perda monetária); - Posição falsa (intencional).
		Roubo e fraude.	- Fraude / fraude de crédito / depósitos sem valor; - Roubo / extorsão / apropriação indevida; - Apropriação indevida de ativos; - Destruição intencional de ativos; - Falsificação; - Cheques sem fundo; - Contrabando; - Apropriação de contas / falsidade ideológica / etc.; - Fraude tributária / evasão (dolosa); - Suborno / Propina; - Negociação interna (Fora da conta da firma).
Fraude externa.	Perdas em função de atos fraudulentos intencionais, apropriação in-devida de bens ou burla da lei, por parte de terceiros.	Roubo e Fraude.	- Fraude / Roubo; - Falsificação; - Cheques sem fundo.
		Segurança dos sistemas.	- Danos por invasão; - Roubo de informação (com perda monetária).
Práticas trabalhistas e segurança no local de trabalho.	Perdas decorrentes de atos incompatíveis com as leis ou acordos trabalhistas, de saúde e de segurança, através de pagamento de indenizações por danos morais, ou por eventos contra a diversidade/ discrimina-tórios.	Relações trabalhistas.	- Compensação, benefícios, rescisões; - Atividade sindical organizada.
		Ambiente Seguro.	- Responsabilidade geral (quase acidentes, acidentes, etc.); - Saúde dos empregados e eventos de normas de segurança; - Compensação dos trabalhadores.
		Diversidade e discriminação.	- Todos os tipos de discriminação.
Danos aos ativos físicos.	Perdas decorrentes de danos aos ativos físicos devido à desastres naturais ou outros eventos.	Desastres ou outros eventos.	- Perdas por desastres naturais; - Perdas humanas por fontes externas (terrorismo, vandalismo).
Interrupção dos negócios e falhas de sistemas.	Perdas decorrentes da interrupção dos negócios e falhas dos sis-temas.	Sistemas.	- *Hardware;* - *Software;* - Telecomunicações; - Interrupção de serviço.
Clientes,	Perdas decorrentes de uma	Adequação,	- Violações fiduciárias / violação de orientações;

produtos e práticas de negócios	falha não intencional ou devido à negligência no atendimento das obrigações profissionais com clientes específicos (incluindo exigências fiduciárias e de adequação), ou devido ao desenho ou a natureza de um produto.	divulgação e fiduciários.	- Adequação / Questões de sigilo; - Violação do sigilo do cliente de varejo; - Violação de privacidade; - Vendas agressivas; - Contabilização automática; - Uso indevido de informações confidenciais; - Responsabilidade do credor.
		Práticas de mercado ou de negócios impróprias.	- Antitruste; - Comércio impróprio / práticas de mercado; - Manipulação de mercado; - Negociação interna (na conta da firma); - Atividade não licenciada - Lavagem de dinheiro.
		Falhas de produtos.	- Defeitos de produtos (não autorizado, etc.); - Erros de modelagem.
		Seleção, Patrocínio & Exposição.	- Falha na investigação de clientes através das orientações; - Exceder os limites de exposição do cliente.
		Atividades de consultoria.	- Questionamentos sobre o desempenho das atividades de consultoria.
Execução, entrega e gerencia-mento de processos.	Perdas por falhas no processamento de transa-ções ou gerenciamento de processos, por relações com as contrapartes co-merciais e fornecedores.	Captura de transação, execução e manutenção.	- Falha de comunicação; - Erro na entrada, manutenção ou carregamento de dados; - Prazo ou responsabilidade perdida; - Falha de operação do modelo/sistema; - Erro de contabilidade; - Falha no desempenho de outra atividade; - Falha na entrega; - Falha no gerenciamento colateral; - Manutenção dos dados de referência.
		Monitoração e notificação.	- Falha na notificação obrigatória; - Relatórios externos imprecisos (Incorrendo em perdas).
		Admissão e documentaçã o de cliente.	- Permissões de clientes / falta de retratação; - Documentos legais incompletes.
		Gerenciamen to de contas dos clientes.	- Concessão de acesso não autorizado às contas; - Registros de clientes incorretos (incorrendo em perdas); - Perda por negligência ou danos aos ativos dos clientes.
		Contrapartes de comércio.	- Falha no desempenho de uma contraparte que não é cliente; - Disputas diversas com as contrapartes que não são clientes.
		Fornecedores .	- Terceirização; - Disputas entre fornecedores.

Internamente, os bancos estão livres para escolherem estruturas alternativas, desde que tenham sua eficácia avaliada pelo órgão supervisor. Porém, a vantagem de uma definição comum para o risco operacional e para o evento de perda é que sua tipologia será raramente subestimada.

Victor Dowd (2003), disse: "Essa emergente linguagem comum de riscos operacionais, como qualquer outra, deve evoluir com o tempo para sobreviver a um mundo tão complexo e desafiador". Alguns "dialetos" que estão próximos a emergir, principalmente aqueles oriundos de abordagens avançadas (e seus componentes), das variações dos modelos de distribuição de perda de redes bayesianas, e das metodologias baseadas em indicadores, irão enriquecer e não destruir essa linguagem.

Além de um dicionário comum para eventos, recomendado como melhor prática pela Basiléia e pelos órgãos reguladores, encontra-se na literatura existente algumas classificações para o comportamento destes eventos, refletidos em freqüência e severidade. A mais comum delas pode ser vista abaixo:

- HFLS (*High Frequency Low Severity*) - Alta frequência, baixa severidade.
- LFHS (*Low Frequency High Severity*) – Baixa frequência, alta severidade.

Os bancos têm maior interesse no segundo grupo, uma vez o maior interesse sobre risco operacional são os eventos extremos. Porém, para outras indústrias, as duas medidas podem representar o mesmo grau de relevância.

Para Jacques Pézier (2002), o comportamento dos eventos de riscos operacionais podem ser classificados de três formas, e não duas: a forma nominal, ordinária e excepcional.

O risco nominal advém do ramo do gerenciamento da qualidade total, que é uma disciplina bastante estudada e, provavelmente, mais desenvolvida na indústria de manufatura do que na indústria financeira. São riscos que ocorrem repetidas vezes (em média uma vez por semana ou mais), devido, por exemplo, ao erro humano na execução de transações. As perdas oriundas de riscos nominais devem ser consideradas na otimização de processos, não merecendo ser caracterizadas como riscos, uma vez que podem ser informações incorporadas em planos de negócio. Os riscos nominais são excessivamente caros, caso

considerem-se sua frequência; dessa forma, o aprimoramento de procedimentos de gestão e de uma cultura de qualidade geram benefícios, em longo prazo, para clientes e para a imagem da empresa, o que torna válido ponderar o *trade-off* de implementação de controles.

No que concerne aos riscos ordinários, pode-se inferir que são riscos menos frequentes, com perdas demasiadas; entretanto, não apresentam risco de falência para uma instituição. Representam apenas uma entre as várias consequências das escolhas estratégicas, e deveriam ser avaliados em um contexto mais amplo, pois são caracterizados como elementos cruciais para o entendimento da relação entre riscos, custos e receitas.

Os riscos excepcionais justificam a atitude da gestão de risco, pois quando ocorrem podem levar uma empresa à falência.

O referido autor resume sua classificação de riscos e suas fronteiras da seguinte forma:

- Perdas imateriais – perdas esperadas e riscos insignificantes.
- Riscos operacionais nominais – as perdas esperadas são mais importantes do os riscos.
- Riscos operacionais ordinários – riscos e perdas esperadas são igualmente importantes.
- Riscos excepcionais – os riscos são muito mais importantes que as perdas esperadas.

Com um dicionário de riscos e perdas definido, é necessária a escolha do método de avaliação, que pode ser qualitativo, quantitativo ou ambos. Alguns bancos estão integrando metodologias quantitativas e qualitativas, que, antes, eram encaradas como excludentes. Além disso, também estão agregando, no cálculo de seu risco operacional, dados da exposição do risco oriundos de um *score* de riscos e de atividades de controle, por exemplo, auditora interna.

Essas abordagens se complementam, uma vez que a análise qualitativa busca identificar, avaliar e mitigar o nível de RO, enquanto a quantitativa demonstra o poder em unidades monetárias.

Além da combinação de abordagens qualitativa e quantitativa, algumas pesquisas recentes defendem que o risco operacional deve ser encarado através de abordagens sistêmicas.

A abordagem sistêmica, também chamada de abordagem holística, exige conhecimento multidisciplinar. O líder do projeto deve entender o relacionamento entre as áreas, isto é: TI, segurança, transferência de risco e finanças, e como elas interagem.

Em sua tese se doutorado, em 2008, a pesquisadora Anna-Maria Kessler, defende o que ela chama de SAFOR – *Systemic approach framework for operational risk* –, que designa que a meta da administração de RO é gerir e mitigar os riscos em torno das causas das perdas.

O SAFOR utiliza a Teoria Geral dos Sistemas (*General Systems Theory* – GST) como tema central da tese. A vantagem do *framework* exposto nesta pesquisa é que, além de considerar e discutir os modelos para mensurar o RO, também inclui um método de tomada de decisão.

A abordagem sistêmica é fundamental para o entendimento dos processos e da relação de iteração entre eles. Isso representa um papel fundamental na gestão de riscos, uma vez que, para se avaliar o RO, é necessário simular alguns cenários de perda. Esse tipo de conhecimento torna mais consistente a avaliação de cenários.

Seja pelas abordagens qualitativa, quantitativas ou pela abordagem sistêmica, o risco operacional ainda é considerado um grande desafio para a gestão.

Embora o Acordo da Basiléia tenha se tornado uma realidade em diversas partes do mundo, ainda existem muitas diferenças entre as técnicas, no que tange às abordagens mais avançadas.

1.3
Metodologias e padrões de Gestão de Riscos

O impulso para a formação e o desenvolvimento do sistema de gestão de riscos remonta aos desastres financeiros ocorridos nos anos 1990. Tais desastres, aliados à crescente complexidade dos negócios em instituições financeiras, acarretada, principalmente, pelo crescimento da utilização de derivativos, impeliram o comprometimento com a concepção de guias e direcionadores para a gestão de riscos.

Diante de um cenário de incertezas, surgiram novos padrões e melhores práticas de gestão de riscos, nesse contexto, na tentativa de formular um guia capaz de mostrar os procedimentos necessários para uma gestão eficaz de riscos.

O primeiro conjunto de padrões para gestão de risco em bancos foi o relatório de práticas, lançado em 1993, pelo "Group of Thirty" – G30. O relatório fornece vinte e quatro melhores práticas de gestão; e foi, inicialmente, desenvolvido para tratar derivativos. Contudo, refere-se a técnicas muito mais abrangentes e, de fato, se aplicam a qualquer carteira de investimento.

O G-30, grupo estabelecido em 1978, é uma entidade privada, um órgão internacional sem fins lucrativos, composto por representantes de alto nível, tanto dos setores públicos quanto privados, e pelas universidades [Os membros do Grupo dos 30 se organizaram com a finalidade de aprofundar a compreensão das questões econômicas e financeiras].

Os princípios do G-30 foram, rapidamente, incorporados aos procedimentos regulatórios. Dentre as vinte e quatro práticas, convém destacar os itens a seguir:

1. Políticas de gestão de riscos definidas pela alta gerência;
2. Marcação a mercado;
3. Metodologia de valoração do mercado;
4. Identificação das fontes de receita;
5. Mensuração do risco de mercado;
6. Simulações de estresse;
7. Previsões de fluxo de caixa;
8. Gestão independente do risco de mercado;
9. Mensurar exposição de crédito;
10. Consolidação da exposição de risco de crédito;
11. Padronização de acordos;
12. Gestão de risco com função independente;
13. Utilização de reforços de crédito;
14. Experiência profissional;
15. Adequação dos sistemas; e
16. Limites de autoridade claramente definidos.

Em 1995, algo improvável desencadeou-se na Inglaterra. O Banco Barings, um dos mais antigos bancos da Grã-Bretanha, esteve próximo à falência. Um de

seus funcionários – Nick Leeson, 28 anos – perdeu aproximadamente um bilhão e meio de dólares ao fazer especulações em contratos de futuros na área de derivativos. As dívidas originadas dessa ação se acumularam em uma conta secreta, que o autor do desfalque ocultava dos auditores.

Com o intuito de compartilhar as lições aprendidas nesse caso, foi escrito um relatório sobre a quebra do Barings e, de acordo com as estimativas, o Banco havia ignorado grande parte das recomendações do G-30.

O relatório do estabelecimento bancário da Inglaterra mencionou, pela primeira vez, a expressão "risco de reputação", que está intimamente relacionado ao impacto nos lucros, em decorrência de uma opinião pública negativa. Nesse relatório concentravam-se algumas lições sobre a catástrofe e, portanto, ele logo se tornou material de referência, cuja função previa pontuar as ações que um banco, certamente, não deveria realizar. As lições aprendidas com o acontecimento, de forma resumida, estão relacionadas a seguir:

- As equipes gerenciais têm a obrigação de entender, completamente, os negócios que elas administram;
- As responsabilidades de cada atividade de negócio devem ser claramente definidas; e
- A clara segregação de função é fundamental para qualquer sistema de controle eficaz.

Existe, também, o *Bank of International Settlements* (BIS) – órgão regulador criado para bancos que operam em esfera mundial, que visa promover a cooperação entre os bancos centrais e as outras agências, à procura de estabilidade monetária e financeira; e que atenta para a normatização dos procedimentos bancários.

É através do Comitê de Supervisão Bancária da Basiléia (*Basel Committee on Banking Supervision* – BCBS), uma organização que congrega autoridades de supervisão bancária, que o BIS define acordos para fortalecer a solidez dos sistemas financeiros. Esses acordos direcionam os principais aspectos que devem ser contemplados na gestão de riscos.

A primeira reunião do Comitê da Basiléia ocorreu em fevereiro de 1975, sendo que, a partir de 1981, os resultados das reuniões começaram a ser

publicados anualmente, por meio de relatórios sobre os avanços ocorridos na supervisão bancária.

Desde seu surgimento, o BCBS constituiu-se em um fórum de discussão para o aprimoramento das práticas de supervisão bancária, buscando aperfeiçoar as ferramentas de fiscalização internacionalmente.

Dentre as indicações relacionadas à gestão do risco operacional, citam-se dois deles, recomendados pela Basiléia:

- Melhores práticas para gestão e supervisão do Risco Operacional – do inglês *Sound Practices for the Management and Supervision of Operational Risk;*
- Estrutura: Sistemas de Controles Internos em Instituições financeiras – do inglês *Framework: Internal Control Systems in banking organizations.*

Essas melhores práticas fornecem elementos para uma eficaz estrutura de gerenciamento do risco, para os bancos de qualquer tamanho e extensão, por meio dos seguintes itens:

- Forte cultura de risco operacional;
- Cultura de controle interno (incluindo, entre outras coisas, as linhas claras de responsabilidade e segregação de funções);
- Comunicação interna eficaz;
- Estabelecimentos de planos de contingência.

Além das melhores práticas que determinam a gestão de riscos em bancos, outros padrões tiveram suas aplicações desdobradas para as demais indústrias. Essas melhores práticas difundiram-se para outros mercados, impulsionados pelo advento da lei estadunidense *Sarbanes-Oxley*, assinada em 30 de julho de 2002, pelo senador Paul Sarbanes e pelo deputado Michael Oxley.

Essa lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores, ambos os problemas causados pela aparente insegurança a respeito da governança das empresas.

Para isso, é necessário aperfeiçoar os controles financeiros e apresentar eficiência na governança corporativa, a fim de evitar que aconteçam outros escândalos e prejuízos. Com o intuito de melhorar a confiabilidade nos relatórios

financeiros, através da ética, da efetividade dos controles internos e da governança corporativa, foram criados padrões de qualidade e melhores práticas de gestão.

Dentre os mais famosos, encontra-se o padrão elaborado pelo *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, que é uma organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nas demonstrações contábeis da empresa, define a gestão de riscos como um processo, influenciado pelo conselho de diretores da organização, pelos gestores e por outros atores, aplicado na definição de estratégias e por toda a empresa.

Em 1992, o COSO publicou o *Internal Control – Integrated Framework*, com padrões de controles internos a serem seguidos pelas instituições, mas foi em 2004 que surgiu o COSO ERM – *Enterprise Risk Management*, que se propõe a ajudar a administração das empresas a lidar melhor com seus riscos e a atingir seus objetivos.

O COSO ERM foi desenhado para tentar identificar eventos potenciais que poderão afetar a organização; além disso, previa gerenciar os riscos, a fim de que se situem dentro do apetite de riscos da empresa, garantindo uma segurança razoável na busca pelos objetivos definidos.

De acordo com o COSO, a gestão de riscos deve abranger os seguintes aspectos:

1. Ambiente Interno – nesta etapa definem-se as estratégias para gestão de risco dentro das organizações – O apetite ao risco da empresa, a filosofia de gestão de riscos e níveis de autoridade e responsabilidades.
2. Definição de Objetivos – como alcançar os objetivos para seguir a estratégia de riscos;
3. Identificação de Eventos – identificação de como estes eventos pode impactar a estratégia;
4. Avaliação dos Riscos – avaliação e classificação de riscos assim com a utilização de modelos para quantificados;
5. Resposta aos Riscos – definição de estratégias de que incluem evitar, mitigar, dividir ou aceitar o risco.;
6. Atividades de Controle – criação de atividades de controle que minimizem ou até inibam o evento de risco;

7. Informação e Comunicação – garantir que informação é direcionada para as pessoas na forma e tempo necessários para a execução da gestão de riscos e outras responsabilidades; e
8. Monitoramento – feito através de atividades contínuas, ou avaliações independentes, e seus resultados servem para garantir que a estratégia adotada faz sentido para o negócio e as medidas tomadas são assertivas.

Outro padrão amplamente utilizado pelas indústrias é o ISO 31000 – *General guidelines for principles and implementation of risk management* –, que tem como objetivo representar uma norma geral de gestão de riscos, independente da área ou do segmento de atuação; e tende a fornecer diretrizes e princípios para a implementação de gestão de riscos e para a criação de outras normas técnicas específicas. Fundada em 1947, em Genebra, na Suíça, a ISO - *International Organization for Standardization* aprova normas internacionais em todos os campos técnicos, sendo uma entidade que atualmente congrega os grêmios de padronização/normalização de 170 países.

A relação dos alicerces da gestão de riscos da ISO 31000 está dividida em:

- Princípios de Gestão de Riscos;
- Estrutura de Gestão de Riscos; e
- Processos de Gestão de Riscos.

Apesar do indiscutível avanço das melhores práticas de gestão de riscos, tanto para as instituições não financeiras quanto para os bancos (este último já em um estágio mais avançado), esses guias fornecem apenas um direcionamento para a gestão de riscos, mas não uma definição clara de como tratá-los.

Por serem muito abrangentes, dificultam uma linguagem comum de riscos, que já se encontra amplamente difundida e compartilhada pelas organizações. "Além disso, apenas propõem um modelo analítico de tratar riscos que só divide a complexidade em partes". (KESSLER, 2008, pag19)

Nesse aspecto, o setor financeiro está à frente dos demais setores, uma vez que a Basiléia II define e classifica os tipos de riscos em categorias e subcategorias, e, além disso, propõe técnicas mais sofisticadas para a gestão de tais alvos.

Porém, mesmo demonstrando grande especificidade em seu discurso, a Basiléia ainda aparenta ser muito permissiva, e, particularmente, não evidencia quais são as instâncias de cada passo que se deve selecionar.

1.4
Gestão de riscos operacionais

A gestão de riscos deve fazer parte das boas práticas de gestão, e a gestão de riscos operacionais (GRO) é apenas um componente desse processo. Em decorrência disso, determinam-se alguns fatores que impulsionaram as descobertas sobre esse tipo de risco, como:

- Crescimento da preocupação sobre a gestão de riscos;
- Maior esforço para identificar, definir, categorizar, mensurar e quantificar RO;
- O crescimento da atenção dos reguladores, analistas financeiros e gestores de bancos para esse tipo de risco; e
- Crescimento do interesse sobre RO, tanto da parte dos gerentes seniores, quanto do corpo de diretores.

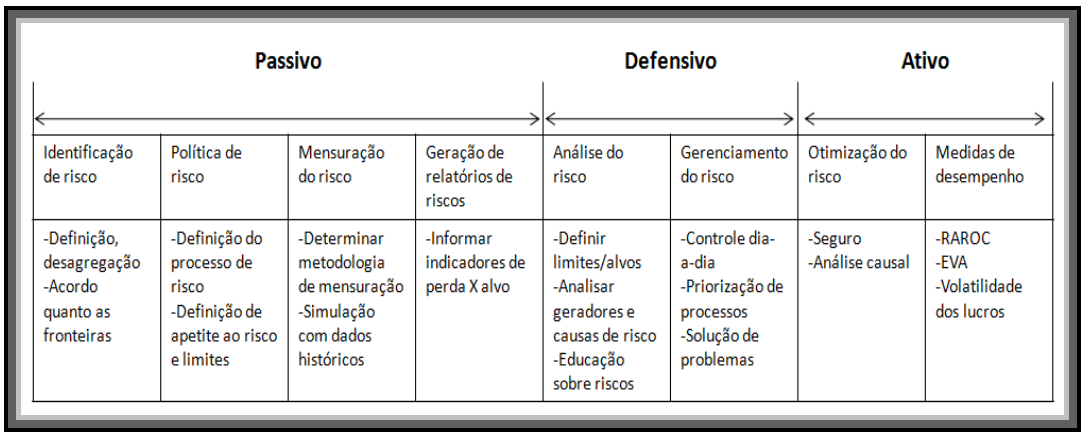
Para a Basiléia II, a gestão de riscos deve abranger risco de crédito, risco de mercado/liquidez, e gestão de risco operacional. Em muitos casos, os riscos de crédito e riscos de mercado são tratados por meio de departamento financeiro, enquanto a gestão de risco operacional pode estar disseminada em diferentes unidades.

A GRO trabalha em função de identificar perdas e conduzi-las a níveis aceitáveis. Implica, também, no estabelecimento de controles para os danos individuais, depois de considerar seus *trade-offs* de segurança e de custos. Esses controles podem estar relacionados a tecnologias e a procedimentos, e devem estar integrados com toda a organização. Para isso, é importante saber o que pode dar errado nos processos de negócio.

Para Jacques Pézier, 2002, não existe diferença entre uma boa gestão e uma boa gestão de riscos, considerando que qualquer resultado, em se tratando de uma importante tomada de decisão, é incerto. Segundo ele, toda gestão de riscos está, indubitavelmente, embasada nos mesmos princípios: geração de alternativas,

quantificação de incertezas e preferências, e modelagem de consequências. Porém, os fatores que compõem um determinado risco divergem de problema para problema.

Marcelo Cruz define que a primeira fase do gerenciamento de riscos costuma ser passiva: os gerentes de risco identificando os riscos, definindo as políticas de riscos (inclusive políticas de mensuração dos mesmos), e começando a coletar os dados. Na segunda fase do gerenciamento, executa-se uma análise mais refinada, para entender as causas e para realizar a primeira tentativa de limitar os riscos, por meio da ação de um processo de controle. Nesta última fase, a instituição já teria um alto grau de confiança nas medidas de risco, portanto, começa-se a usar esses modelos para influenciar os processos de apreçamento, de determinação de preços de seguro e mensuração de desempenho. Nesta linha, um exemplo do exposto acima, ou seja, um processo genérico de desenvolvimento de gestão de riscos pode ser visto, na figura 1.2 da seguinte forma:



Fonte: Livro - Modelagem, avaliação e proteção para Risco Operacional

Figura 1.2: Processos de Gestão de Riscos

Anna Maria Kessler (2008) definiu que o processo de gestão de riscos é composto por seis fases:

1. Identificação de RO;
2. Classificação de RO;
3. Mensuração de RO;
4. Valoração de RO;
5. Cenários/previsões de RO; e
6. Decisão/controle de RO.

Anthony Peccia (2002) define um *framework* para gestão de riscos em instituições financeiras em cuja composição pontuam-se cinco etapas. São elas:

2. Identificação de riscos – Auto-avaliação do risco realizada pelo gerente do negócio e validada pelo gerente de riscos.
3. Mensuração de riscos – Feita pelo grupo de especialistas em riscos. Baseada nas perdas passadas e na análise de cenário, a fim de definir distribuição de frequência e severidade para alcançar a distribuição de perda.
4. Análise, monitoramento e confecção de relatório – Desenvolvidos pelo gerente do negócio e pelo gerente de riscos. Baseados na avaliação quantitativa de riscos, amarrados às características principais do risco, que são: (I) roubo/fraude; (II) exigência de clientes; (III) exigência dos empregados; (IV) exigências legais; e (V) erros em transações.
5. Requerimentos de capital – Através da análise de risco, espera-se saber: (I) quais são os maiores riscos operacionais; (II) quanto de perda espera-se ter com um evento de RO; (III) o quão ruim essas perdas podem ser, em cenários normais ou feitos por testes de stress.
6. Gestão das perdas – Planos de mitigação devem ser elaborados pelo gerente do negócio e pelo grupo de especialistas em riscos, e devem incluir planos de continuidade e seguros.

A maioria dos gestores concorda que "gerir é mais importante do que meramente quantificar". (Tony Blunden, 2003).

De maneira geral, a gestão de riscos operacionais ainda é um assunto recente e apresenta grandes desafios, principalmente porque existem algumas divergências conceituais sobre RO entre instituições financeiras e não financeiras. O próprio perfil do profissional de riscos diverge entre as organizações, e isso faz com que as firmas foquem em práticas diferentes de gestão.

Isso corrobora com a ideia de que os gestores de riscos corporativos geralmente exigem prática em negócios e bons conhecimentos em proteção dos ativos (controles), enquanto os gestores de riscos financeiros exigem

especialização em negociação com derivativos e capacidade para manipular estatisticamente modelos matemáticos.

Essas duas abordagens de gestão de riscos podem ser problemáticas, caso sejam sobrepostas; e podem concluir com uma perspectiva fragmentada da gestão de riscos.

De toda a interpretação sobre esse aspecto, a única coisa passível de intuição é que o profissional de riscos do futuro deve ser capaz de identificar os principais riscos do negócio, e, para isso, é preciso fazer um trabalho em conjunto com o gestor/especialista do negócio; logicamente, sem deixar de saber utilizar com propriedade as ferramentas estatísticas, para o auxílio à tomada de decisão.

1.5
O risco operacional na indústria de Petróleo

Acompanhando a tendência global a indústria de petróleo experimentou uma vastidão de inovações: de natureza tecnológica, especialmente o crescente desenvolvimento da exploração *offshore* – termo utilizado para atividades no mar, dado o inevitável esgotamento futuro da produção onshore (em terra); e também de natureza financeira: uma crescente "comoditização" do petróleo, e a utilização dos modernos mecanismos financeiros de gerenciamento de risco, como operações de hedge e nos mercados futuros, a termo e de opções.

Diante de um cenário mais complexo não restam dúvidas da necessidade de um modelo de gestão de riscos que ajude a estruturar decisões e direcionar estratégias no negócio.

Para enriquecer o trabalho, foram realizadas algumas pesquisas bibliográficas sobre a gestão de riscos operacionais em empresas do mercado de energia – com foco na indústria de petróleo. O objetivo era entender como o setor enxerga e avalia esse tipo de risco e, basicamente, os artigos relacionam o risco operacional, principalmente, com projetos de investimento, segurança no trabalho e meio ambiente.

Quando se comenta sobre projetos de exploração e produção, esses riscos estão relacionados à localização, tecnologia, timing, aspectos legais, aspectos políticos e negócios. Quando se comenta sobre operações de plataforma, fala-se

sobre falhas nas operações, acidentes no trabalho e danos ao meio ambiente relacionadas à falha de processos e procedimentos.

As técnicas utilizadas nesses artigos, descritos ao longo deste capítulo, para a avaliação de riscos operacionais são similares às utilizadas em instituições financeiras, com foco em frequência de eventos e na inclusão de fatores causais.

A importância desta analogia é que a indústria de petróleo pode estender o uso destas técnicas, assim como os bancos, para suas operações financeiras, gestão de projetos, para o controle de contingência jurídica, para gestão de falhas em atividades operacionais das atividades de apoio – Recursos Humanos, Contabilidade, entre outras. Isso tornaria a abordagem da gestão de riscos, na organização como um todo, muito mais completa e integrada, mas sem perder o foco e os esforços no que é efetivamente relevante para o negócio.

O maior impulso para criação de metodologias para gestão de riscos nas empresas foi dado em função dos requisitos de governança corporativa exigidos pela Lei Sarbanes-Oxley, instituições não financeiras vêm sofrendo uma forte pressão para a implementação de metodologias de riscos.

A lei exige, principalmente, a garantia de criação de mecanismos de auditoria e segurança, incluindo ainda algumas regras para a criação de comitês encarregados de supervisionar suas atividades e operações.

Essas ações objetivam mitigar riscos dos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorram, garantindo a transparência na gestão.

De acordo com artigo publicado por David Wood e Scott Randall, o grande impulso para adequação à SOX tem sido conduzido pelos setores de Finanças, Tecnologia da Informação e Jurídico. Porém, os gestores estão utilizando esses instrumentos para gerenciar seus passivos e preencher os *gaps* de sua gestão de riscos.

Os autores citam o COSO como instrumento de gestão de riscos, e enfatizam que os *frameworks* de ERM utilizados pelas empresas focam demasiadamente em atividades de controle e reporte e, raramente, detalham as etapas de avaliação e implementação. Para que se tenha um instrumento de gestão efetivo, todos os componentes do COSO devem estar funcionando de forma satisfatória para todos os setores da empresa.

Muitas empresas de petróleo, *upstrem* - uma expressão utilizada na indústria do petróleo que significa a parte da cadeia produtiva abrangendo atividades de exploração, desenvolvimento, produção, e *downstrem* - o termo utilizado para referir as áreas de negócio que lidam com o refino, distribuição e venda de produtos petrolíferos, conhecem os riscos, mas ainda tomam decisões sem estabelecer critérios bem definidos, abordagens quantitativas e não utilizam técnicas de gestão de riscos em processos para a melhoria de sua *performance*.

O foco do ERM deve ser sistemático e quantitativo, quando possível. Sua utilização deve estender-se, também, para projetos de investimentos específicos e na avaliação de oportunidades. A avaliação e o planejamento das estratégias de gestão de risco, para esses casos, exigem um profundo conhecimento técnico, abrangendo operações, cadeia de fornecimento, geopolítica, segurança, legislação e questões financeiras específicas para a indústria.

Essas necessidades podem ser ilustradas através da natureza dos negócios de projetos de petróleo e gás internacionais para os setores de *upstream* e *midstream*, que, atualmente, recebem grande investimento de capital. Desenvolvimento em águas profundas em difíceis regiões internacionais, liquefação de gás e terminais de recebimento de Gás natural liquefeito, instalações para GTL (*Gas-to-Liquids*) e oleodutos intercontinentais com fronteiras múltiplas ou de difícil conexão necessitam de muito capital durante um longo período, e o retorno vem apenas em longo prazo.

Para os casos acima, o amplo conjunto de habilidades para a avaliação de risco operacional tem mais a oferecer em termos de tomada de decisão do que para os setores de contabilidade, TI e consultoria jurídica. Nesses casos, para ser uma gestão bem sucedida, o ERM deve abraçar a especialização em geologia e atributos de engenharia, instalações, equipamentos, saúde, segurança, meio ambiente, negócios, financeiro, e gestão de tecnologia.

A complexidade dos negócios exige uma gestão de riscos que vai além de exigências regulatórias de governança para prevenir erros ou fraudes. Se a adequação a SOX, for vista apenas como a assinatura de um papel para certificação, as empresas perdem uma grande oportunidade de implementar um *framework* de gestão de riscos para melhoria de *performance* e vantagem competitiva.

David Wood e Scott Randall escreveram uma continuação do artigo supracitado, intitulado *The link of risk management*, no qual apresentam uma proposta de análise de risco holística para projetos de exploração e produção. Os autores argumentam que os modelos de *valuation* devem considerar as várias facetas do risco e os conceitos de ERM podem ajudar nesta identificação.

Dos doze fatores identificados como relevantes pelos autores para a avaliação de riscos em projetos de exploração e produção, seis deles foram classificados como operacionais: localização, tecnologia, *timing*, aspectos legais, aspectos políticos e negócios. Esses fatores podem variar de acordo com o tipo de projeto. É por isso que uma abordagem holística é fundamental, pois essa abordagem considera as características únicas de cada projeto.

A visão desses autores é bem interessante para que se possam elucubrar algumas questões relacionadas à aplicação da gestão de riscos em empresas não financeiras. Um conceito diferente do setor financeiro é a inclusão do risco ambiental.

Recentes escândalos envolvendo riscos ambientais merecem ser citados, como a explosão da plataforma "Deepwater Horizon", controlada pela BP (antiga British Petroleum), no dia 20 de abril na costa da Louisiana matou 11 trabalhadores e, segundo estimativas do governo norte-americano, jogou no mar do golfo do México entre 356 e 697 milhões de litros de petróleo.

A petrolífera aceitou pagar US$ 20 bilhões para formar um fundo independente para custear os estragos reivindicados pela população e empresários atingidos pelo vazamento de petróleo no golfo do México.

Mas será que apenas os riscos relacionados ao núcleo ou atividade fim do negócio são os que realmente importam para as indústrias? Em que proporção estão concentrados cada tipo de risco?

Um evento interessante ocorrido na indústria de papel e celulose, no qual a empresa Aracruz - empresa brasileira sediada no município de Aracruz, no Espírito Santo), quase foi a bancarrota em decorrência de operações com derivativos.

Em 2008, a então maior fabricante de celulose de eucalipto do mundo, anunciou que eliminou 97 por cento de sua exposição a instrumentos derivativos de investimento, sofrendo uma perda total de 2,13 bilhões de dólares. Desde 2004, o uso de derivativos financeiros, além de outros instrumentos de proteção contra a

valorização do real, gerou um ganho acumulado de R$ 630 milhões. Entretanto, fontes do mercado relatam que, desde o final do primeiro trimestre de 2008, a empresa passou a realizar operações bastante agressivas, extrapolando a política de risco da própria companhia.

A empresa estava com uma exposição de US$ 10 bilhões, enquanto as receitas anuais com exportação são da ordem de US$ 2 bilhões. As operações contratadas pela Aracruz previam ganhos limitados com a valorização do real, e perdas ilimitadas no caso de desvalorização – cenário tido como pouco provável até algumas semanas atrás do escândalo. Pelos contratos, quando a cotação ultrapassasse determinado teto fixado entre as partes, as perdas se multiplicariam por dois.

As indústrias devem encarar seus riscos de forma holística e consciente, empresas de petróleo, por exemplo, não se resume em processos de segurança, meio ambiente e saúde, e os avanços e integrações de métodos têm grandes contribuições para consolidação de alguns conceitos.

Além da visão fragmentada, não há uma definição de risco operacional comum, que poderia incluir, por exemplo, o risco ambiental. *Frameworks* de ERM frequentemente utilizados, como o COSO, fornecem apenas um direcionamento para a gestão de riscos, mas não uma definição clara de como tratá-los. Sequer definem um padrão de nomenclatura de riscos, ou especifica como mensurá-los.

Estas metodologias quando utilizadas pelas empresas focam demasiadamente em atividades de controle e reporte e, raramente, detalham as etapas de avaliação e implementação, justamente por terem como maior motivação atender as requisitos da lei SOX. Para que se tenha um instrumento de gestão efetivo, todos os componentes do COSO devem estar funcionando de forma satisfatória para todos os setores da empresa. O foco do ERM deve ser sistemático e quantitativo, quando possível.

Por esta razão, nesta pesquisa, foram explorados métodos mais específicos de avaliação utilizados na indústria financeira. Esta aplicação e suas dificuldades de implementação podem ser vista no próximo capítulo, que trata do estudo de caso.