



Instituto Politécnico de Coimbra

Instituto Superior de Contabilidade e Administração de Coimbra

Dissertação

Mestrado em Auditoria Empresarial e Pública

*Risk Management e Ambiente Controlo Mitigadores
Negócio da Banca*

Realizado: Rui Mendes Santos

Orientador: Nuno Miguel Caeiro Castanheira

*Coimbra
Outubro 2013*

«Recomeça... Se puderes, sem angústia e sem pressa e os passos que deres nesse caminho duro do futuro, dá-os em liberdade, enquanto não alcances não descanses, de nenhum fruto queiras só metade.»

Miguel Torga

*... Para a princesa Mariana,
... Miminho Tomás
... a ti, Maria João*

Resumo

A identidade de uma Instituição é a imagem que lhe é associada pelo mercado e sociedade em geral, é o resultado do conjunto de princípios, valores e comportamentos exercidos pelos seus colaboradores e clientes, devendo aderir a elevados padrões de ética profissional e evitar situações suscetíveis de originar conflitos de interesse e fraude. Nos últimos anos várias situações têm vindo a público de posições menos claras por parte das organizações e dos seus colaboradores. Tal realidade pode ter diversas justificações, nomeadamente a atual crise económica e a crescente crise de valores existente na sociedade em geral. A necessidade de eficácia no cumprimento de objetivos extremamente exigentes com a maior eficiência dos cada vez mais reduzidos recursos exige dos responsáveis, ou de quem tem que tomar decisões, um maior conhecimento e saber no desempenho das suas atividades. A informação constitui, na atual realidade económica, um poderoso ativo para o exercício das suas funções, e em particular, para o apoio à sua tomada de decisão. As organizações com elevado grau de descentralização têm na Auditoria Interna um complemento indispensável, na medida em que pode ajudar na eliminação de desperdícios, simplificar tarefas, reduzir custos e minimizar riscos, constituindo uma função de apoio á gestão, sendo capaz de auxiliar em diversas áreas tais como: “*corporate governance*”, ética, gestão de risco, controlo interno e “*compliance*”, tecnologias de informação, qualidade e ambiente. Os procedimentos de auditoria são processados por pessoas, daí a importância do comportamento humano e da própria cultura organizacional. A essência de qualquer negócio são as pessoas, suas características, integridade moral, ética e competências pessoais e profissionais, no entanto os objetivos delineados regulam todo o seu “*modus operandi*”, com definição clara do “*core business*”.

Palavras-chave: *Corporate Governance*, Gestão Riscos, Ética, Conflitos de Interesse Fraude, *Core Business*

Abstract

The identity of an institution is the image by which an institution is associated by the market and society in general, is the result of the set of principles, values and behaviors used by their employees and customers, adhering to high standards of professional ethics and avoiding situations that are likely to create conflicts of interest and Fraud. On the last few years several situations have become public, exposing organizations and their employees. Such reality may have several explanations, in particular the current economic crisis and the decaying of values in society. The need for efficiency achieving objectives while demanding efficiency with dwindling resources requiring from the decisions makers greater knowledge and wisdom in carrying out its activities. The Information is, in the current economic reality, becomes then a powerful asset, in the performance of their duties and, in particular, to support their decision-making. Decentralized organizations have, then in their Internal Audit department an indispensable complement, as it can help them to eliminate overspends, simplify tasks, reduce costs and minimize risks, providing a support function to management, being able to additionally assist in various areas such as: corporate governance, ethics, risk management, internal control and compliance, information technology, quality and environment, among other areas. The audit procedures are conducted by people, hence the importance of human behavior and organizational culture in those roles, people are after all the essence of any business, providing their characteristics, moral integrity, ethics and personal and professional skills, however the objectives outlined shall regulate their "modus operandi" in an organization, with clear definition of the "core business".

Keywords: Corporate Governance, Risk Management, Ethics, Conflict of Interests, fraud, Core Business

Índice

Resumo	3
Abstract	4
Índice	5
Índice de Figuras, Quadros e Gráficos	7
Lista de Siglas	9
1. Introdução.....	11
2. Governo das Sociedades	13
2.1 Governo das Sociedades nos Estados Unidos da América	16
2.2 Governo das Sociedades na Europa	17
2.3 Governo das Sociedades em Portugal	18
3. Ética.....	23
3.1 Ética e Transparência Empresarial	24
4. Risco.....	29
4.1 O COSO ERM	38
4.2 Limitações da Gestão de Risco Empresarial	42
5. Sistema Financeiro.....	48
5.1 Sistema Financeiro Português	49
5.2 Modelo de Supervisão Português	52
5.3 Banco de Portugal – Aviso nº 5/2008 de 25 de Junho	54
5.3.1 Objetivos da publicação do Aviso nº 5/2008	55
5.4 Componentes do Controlo Interno	57
5.4.1 Ambiente de Controlo	58

5.4.2	Identificação e Avaliação de Riscos.....	60
5.4.3	Informação e Comunicação	60
5.4.4	Atividades de Controlo	61
5.4.5	Processo de Monitorização de Controlo	62
5.5	Categorias de Controlo	63
5.6	Categorias de Riscos	65
5.7	Gestão Risco Operacional nas Instituições Financeiras.....	67
5.8	Regulamentação para a gestão de risco operacional.....	73
5.8.1	Decreto-lei nº298/92 de 31 de Dezembro.....	74
5.8.2	Acordos Basileia.....	74
5.8.3	Sarbanes-Oxley.....	81
6.	Conflito Interesses.....	83
6.1	Sociedades Financeiras	85
7.	Fraude Bancária	88
7.1	Fraude e Abuso Ocupacional.....	91
7.2	O Triângulo da Fraude de Donald R. Cressey.....	93
7.3	A Balança da Fraude de W. Steve Albrecht.....	97
7.4	Gestão de Risco de Fraude no Sistema Bancário	99
7.5	Avaliação e Prevenção da Fraude	102
7.6	Risco e Probabilidade de Ocorrência.....	105
7.7	Construção de Perfil de Risco.....	105
7.8.	Procedimentos e Prevenção da Fraude no Sistema Bancário	106
8.	Auditoria e Compliance	108
9.	Investigação	115
10.	Conclusões.....	135
11.	Referências Bibliográficas.....	140
12.	Anexos.....	147

Índice de Figuras, Quadros e Gráficos

Figuras

Figura 1	Ideograma Chinês	30
Figura 2	Risco e Principais Interessados	32
Figura 3	Fontes de Incerteza	35
Figura 4	Cubo do COSO ERM	40
Figura 5	Matriz de Risco – Impacto x Probabilidade	47
Figura 6	Sistema Financeiro	48
Figura 7	Componentes fundamentais do SCI	58
Figura 8	Risco - Definições, Tipos, Medição e Recomendações para a sua Gestão	66
Figura 9	Estado de maturação da investigação na área de Risco	70
Figura 10	Arquitetura de um Sistema de Informação para risco Operacional	82
Figura 11	Distribuição de Perdas Operacionais	83
Figura 12	Triângulo da Fraude	94
Figura 13	A Balança da Fraude	98
Figura 14	Estratégia de Gestão de risco	100
Figura 15	Protagonistas na Gestão de Risco	101
Figura 16	Construção de Perfil de Risco	106
Figura 17	Exemplos de Modelos alternativos de Supervisão de Compliance	110

Quadros

Quadro 1	Instituições de Credito (Banco Portugal)	51
Quadro 2	O Modelo de Supervisão Português (BP)	53
Quadro 3	Matriz de Risco Standard	105

Gráficos

Gráfico 1	A entidade possui Auditoria interna	117
Gráfico 2	Utilização Auditoria externa pelas Entidades	118
Gráfico 3	Periodicidade trabalhos auditoria nas Sucursais	120
Gráfico 4	Áreas de Conhecimento Auditor das Organizações aquando dos trabalhos a executar	120
Gráfico 5	Processos Pedagógicos versus satisfação Colaboradores	122
Gráfico 6	Temas de Trabalho e sua Prioridade	124
Gráfico 7	Tipos de fraude mais frequentes	124
Gráfico 8	Detenção Fraude nas Instituições Financeiras	128
Gráfico 9	Características Auditor	128
Gráfico 10	Deteção Fraude – Relação entre Auditoria Interna/Externa	129
Gráfico 11	Trabalho de auditoria junto das sucursais	130
Gráfico 12	Objetivo dos trabalhos desenvolvidos Sucursais	131

Lista de Siglas

- ABE** - Associação Europeia Bancos
- AICPA** - American Institute of Certified Public Accountants
- APB** - Associação Portuguesa Bancos
- BCBS** - Comité de Basileia de Supervisão Bancária
- BCP** - Banco Comercial Português
- BdP** - Banco de Portugal
- CAATs** - Técnicas de Auditoria assistidas por Computador
- CEBS** - Comitê de Supervisão Bancária Europeia
- CMVM** - Comissão do Mercado de Valores Mobiliários
- CNSA** - Conselho Nacional de supervisão de Auditoria
- COBIT** - Control Objectives for Information and Related Technology
- COSO** - Committee of Sponsoring Organizations
- CSA** - Control Self Assessment
- CTT** - Correios de Portugal
- DAI** - Direção Auditoria Interna
- DMIF** - Diretiva dos Mercados de Instrumentos Financeiros
- DL** - Decreto-lei
- ERM** - Enterprise Risk Management
- EUA** - Estados Unidos da América
- IC** - Instituição Credito
- IIA** - Institute of Internal Auditors
- IPAI** - Instituto Português de Auditoria Interna
- IPCG** - Instituto Português de Corporate Governance
- ISO** - International Organization for Standardization
- ISP** - Instituto Seguros Portugal

KRI – Key Performance Indicators

MAR – Modelo Avaliação Riscos

OCDE - Organização para a Cooperação e Desenvolvimento Económico

OECD - Organisation for Economic Co-operation and Development

OROC - Ordem dos Revisores Oficiais de Contas

RGICSF - Regime Geral das Instituições de Crédito e Sociedades Financeiras

SCI - Sistema Controlo Interno

SEC - Securities and Exchange Commission

SOX - Sarbanes Oxley

TUAC - Trade Union Advisory Committee

1. Introdução

Nos últimos anos, em consequência da globalização, do acréscimo de concorrência e de exigências de simplificação processual e operativa, levou a que as condições de funcionamento dos Bancos tenham mudado de forma significativa.

Na atualidade as organizações precisam estar em conformidade com uma série de normativos legais bem como metodologias que representam as melhores práticas. Para tal, toda a organização necessita ter formas de controlo e políticas de melhoria contínua. A procura da excelência operacional resulta em iniciativas cada vez mais complexas que envolvem o negócio, as TI¹, as infraestruturas e as pessoas.

Neste contexto de mudança, torna-se ainda mais necessário que os Bancos disponham de Auditores Internos persistentes, preparados, objetivos e imparciais. Acima de tudo, torna-se necessário que a Auditoria Interna seja atuante e que seja capaz de desenvolver atividade nos domínios da verificação Processual do Aconselhamento e da consultoria.

A Auditoria Interna é parte integrante do processo contínuo de monitorização do Sistema de Controlo Interno dos Bancos e assiste a Gestão de Topo e Administração no eficiente e eficaz desempenho das suas responsabilidades, dado que fornece uma avaliação independente da adequação e conformidade das políticas e procedimentos em vigor.

Contudo aos Auditores Internos são exigidos desempenhos cada vez mais alargados, preparados e consistentes, para que possam corresponder ao que deles se espera, torna-se exigível que os Auditores Internos se questionem regularmente, sobre as áreas de atuação, os métodos de trabalho e as formas de intervenção tradicionais. Neste contexto estar preparado significa garantir desempenhos mais equilibrados e competentes, como forma de acrescentar valor à organização.

As instituições financeiras estão incluídas num sistema financeiro com uma regulação e quadro legislativo próprios. Portugal, pelo facto de ser membro da União Europeia, tem integrado no seu direito interno as “Diretivas” que conduzem à aplicação dos chamados “Acordos de Basileia”.

¹ Tecnologias de Informação

Estes Acordos, emitidos pelo Comité de Basileia de Supervisão Bancária, visam estabelecer os princípios fundamentais e recomendações importantes para a supervisão do sistema bancário e integram a problemática da gestão do risco.

A agenda regulatória internacional do Setor Financeiro tem vindo a ganhar importância ao longo do tempo, com ênfase nas últimas duas décadas. O Acordo de Basileia (*International Convergence of Capital Measurement and Capital Standards*) firmado em 1988 e ratificado por mais de 100 países foi apenas um primeiro passo no sentido de dotar os bancos de níveis de capitais suficientemente robustos para fazer face às incertezas dos mercados.

Os posteriores acontecimentos mundiais precipitaram diversas necessidades de “afinação”/calibragem que levaram os bancos a ter de repensar a forma de atuação e, inclusivamente, o modo como encaram a rentabilidade e as respetivas medidas. “*Basileia II*”, “*Basileia III*”, “*CRD IV*”, “*FinRep*”, “*CoRep*” e muitos outros termos circulam diariamente nos meios financeiros e na comunicação social e nem sempre são entendidos de uma forma coerente e totalmente exata.

A gestão do risco nas instituições financeiras é um tema de investigação pertinente e atual. A gestão do risco é uma das atividades fundamentais para a sobrevivência de qualquer organização. A crise financeira, a instabilidade e a volatilidade que caracterizam o atual momento tornam a gestão do risco essencial. O crescimento do mercado, a que se associa o aparecimento de novos produtos e a maior possibilidade de acesso ao crédito por parte das economias, produziu a necessidade de contar com sistemas informáticos e ferramentas que permitam a gestão dos riscos de modo mais eficiente. Segundo Castanheira et al. (2006:61) nas “instituições financeiras a gestão de risco não é alheia ao incremento do risco operacional, o que motivou a que o Comité de Basileia publicasse recentemente um documento formal com normas específicas de gestão do risco operacional, que deverão ser atendidas pela atividade bancária e que vêm incentivar os Bancos a fortalecer os sistemas de controlo e gestão de risco. Adicionalmente, a regulação tem um papel de extrema importância na maturidade de gestão de risco”.

Os riscos que as instituições financeiras enfrentam mudam rapidamente, os métodos utilizados para os gerir também mudam, pelo que é previsível que incorporem progressivamente a gestão de riscos na sua organização até chegarem a uma gestão centralizada e integral, questões como a estratégia, o “*Core Business*” do negócio, a cultura da instituição, “*Risk Appetite*” e recursos disponíveis, são fundamentais no “*Corporate Governance*” institucional.

2. Governo das Sociedades

O controlo de qualidade é o elemento central em qualquer estrutura empresarial, sendo nas empresas de prestação de serviços, fulcral e imprescindível. No setor de atividade em análise (setor financeiro), veremos mais a frente será de extrema importância devido ao englobar de áreas e processos bastante sensíveis para todos os intervenientes.

Assim e embora o conceito de “governo das sociedades”, internacionalmente conhecido por “*Corporate Governance*”, seja relativamente novo, o seu estudo não é assim tão recente. Segundo Moreira et al (2004), a origem deste estudo deve-se ao trabalho realizado por Adolph Berle e Gardiner Means designado “*The Modern Corporation and Private Property*”, publicado em 1932. Este trabalho terá surgido na sequência da grande crise de 1929, acabou por ser considerado uma referência para a legislação norte-americana que foi entretanto aprovada.

Depois da sua criação, o conceito de “governo das sociedades” tem vindo a acompanhar as grandes mudanças e oscilações do mundo financeiro, sofrendo ele próprio uma forte evolução. No entanto, este conceito não reúne consenso, talvez pelo facto dos autores terem diferentes perspetivas criando, inevitavelmente, diferentes definições. Segundo alguns autores o “governo das sociedades” deve ter uma perspetiva mais limitada e essencialmente relacionada com o objetivo de eficiência económica. No entanto, existem opiniões discordantes, segundo as quais este conceito deve ser visto e pensado numa perspetiva mais vasta onde se inclui, por exemplo, o conhecimento da organização da atividade económica; neste caso pretende-se que sejam igualmente atingidos objetivos sociais relativos (Marques, 2003).

Embora não haja uma definição unânime alguns organismos desenvolveram as suas definições, TUAC (2004) refere que em 1999 a OECD² (*Organisation for Economic Cooperation and Development*) define o “governo das sociedades” como sendo um sistema através do qual as organizações são dirigidas e controladas. A estrutura do “governo das sociedades” especifica a distribuição dos direitos e das responsabilidades ao longo dos diferentes participantes na empresa – o conselho de administração, os gestores, os acionistas e outros intervenientes – e dita as regras e

² Organisation for Economic Co-operation and Development

os procedimentos para a tomada de decisões nas questões empresariais. Ao fazê-lo, fornece também a estrutura através da qual a empresa estabelece os seus objetivos e as formas de atingi-los e monitorizar a sua performance. Muitas outras definições de “governo das sociedades” têm sido emanadas pelas mais diversas organizações todas elas com um conceito chave que se foca na melhoria da confiança dos *stakeholders*, assim como na maior responsabilização da administração por atos de gestão menos cuidados. Outro dos fatores sempre implícito no conceito de “governo das sociedades” foca-se na adoção de boas práticas de governação por parte da administração. As “*best practices*” como são comumente conhecidas estão intimamente relacionadas com *Benchmarking*, que também é considerado na essência do conceito em apreço. A utilização desta técnica consiste na identificação dos resultados das melhores práticas utilizadas nos diferentes processos de negócio e funções empresariais, com especial destaque para aqueles cujo impacto no desempenho permita assegurar e sustentar vantagens competitivas para a empresa.

Em 2005, a Comissão do Mercado de Valores Mobiliários referia-se ao “governo das sociedades”, “como sendo um sistema de regras e condutas relativo ao exercício da direção e controlo das sociedades emitentes de ações admitidas à negociação em mercado regulamentado” (CMVM, 2005, pp. 1). Segundo Almeida (2005), “os objetivos do “governo das sociedades” passam por apoiar o desempenho da organização de modo a que esta obtenha os melhores resultados, para tal, existe a tentativa de prevenir e detetar comportamentos fraudulentos”.

Pretende-se ainda que a reputação das organizações cresça, ao apostar-se na transparência e relato da informação. Pinheiro (2008 b) expõe de modo sucinto que o governo das sociedades tenta:

- ✓ Assegurar a confiança e integridade da informação;
- ✓ Assegurar o cumprimento das políticas, planos, procedimentos e legislação em vigor;
- ✓ Assegurar e proteger os ativos
- ✓ Assegurar a realização dos objetivos e metas fixadas para as operações
- ✓ Acrescentar valor acionista
- ✓ Avaliar e responsabilizar a gestão pelos atos praticados
- ✓ Incentivar a gestão pela responsabilidade social

A adoção dos princípios de “*governo das sociedades*” associados a um bom desempenho da DAI³ poderá fazer com que muitos dos riscos inerentes à própria atividade sejam mais facilmente detetados, reportados e desde logo mitigados, conferindo assim valor acrescentado à empresa que opta pela implementação destes princípios cada vez mais em voga. Os princípios referenciados estão intimamente relacionados com a implementação de um eficaz Controlo Interno, para assim promover uma maior agilidade na gestão de todos os riscos inerentes à própria atividade, com vista a evitar situações de falência como as que já foram vivenciadas por muitas empresas um pouco por todo o mundo. Os princípios de “*governo das sociedades*” não constituem o garante de uma eficaz gestão de riscos, para isso será necessária a existência de sólidos SCI⁴, para que em aliança confirmam valor acrescentado à organização, poupando-a de correr alguns riscos, ou pelo menos ter um maior controlo sobre os mesmos, fato esse que ao não se verificar poderá por em causa a sua continuidade.

O conceito de “*governo das sociedades*” rege-se por um conjunto de princípios basilares que têm por finalidade acrescentar valor à empresa, fazendo com que esta se possa destacar dos mais diretos concorrentes visando assim a melhoria da sua *performance* e consequente continuidade.

A nível externo, o elemento de referência é a supervisão da Ordem Profissional e outras entidades como sejam a CMVM⁵ e o Banco de Portugal. Em 2008 foi aprovada a criação do Conselho Nacional de Supervisão de Auditoria (CNSA)⁶ – Decreto – Lei n.º 224/2008, tendo sido aprovado os respetivos estatutos, procedendo à transposição parcial da Diretiva n.º 2006/43/CE, do Parlamento Europeu e do Conselho, de 17 de Maio de 2006, relativa à revisão legal das contas anuais e consolidadas, visando regular o exercício da atividade de auditoria para a promoção da qualidade e a confiança dos mercados nas funções de auditoria. Deste modo, foi introduzido um novo modelo de supervisão da profissão, com a criação do CNSA, ao qual é atribuída a responsabilidade final pela supervisão do exercício da atividade.

³ Direção Auditoria Interna

⁴ Sistema de Controlo Interno

⁵ Comissão do Mercado de Valores Mobiliários

⁶ O CNSA (Conselho Nacional de supervisão de Auditoria), tem por missão reforçar a confiança e a credibilidade na atividade de auditoria exercida pelos revisores oficiais de contas e sociedades de revisores oficiais de contas em Portugal, assegurando assim que estes contribuam para o rigor, correção, fiabilidade e transparência dos documentos de prestação de contas

O sistema de supervisão pública caracteriza-se por uma gestão independente, atribuída ao Banco de Portugal, à Comissão do Mercado de Valores Mobiliários, ao Instituto de Seguros de Portugal, à Ordem dos Revisores Oficiais de Contas e à Inspeção-Geral de Finanças (Autoridade Tributária). No cerne das atribuições do CNSA encontram-se a emissão de parecer prévio relativamente às normas do sistema de controlo de qualidade, deontológicas e de auditoria e a avaliação do plano anual de controlo de qualidade proposto pela OROC, bem como o acompanhamento da sua execução⁷. No que concerne às instituições financeiras, muito do controlo de qualidade, alicerçada em condutas éticas, bem como a gestão do risco se baseiam em estruturas sólidas das instituições, bem como nas políticas internas de governo das sociedades.

2.1 Governo das Sociedades nos Estados Unidos da América

A problemática sobre “*Corporate Governance*” iniciou-se nos EUA nos anos 70⁸ mas, é com a criação da “*Comissão Treadway*” no ano de 1985 que esta temática ganha destaque. A “*Comissão Treadway*” foi criada pelo Congresso Americano com o intuito de aumentar o combate à fraude, tendo posteriormente, evoluído para a realização de estudos sobre o controlo interno, considerando que este deve oferecer uma garantia razoável de que os objetivos das entidades são alcançados. Dando igualmente relevância à existência da auditoria interna e a que os auditores sejam devidamente independentes (Pinheiro, 2008 a).

Segundo Pires (2008), “o Relatório de *Treadway* defendia a criação de um controlo interno adequado, graças a uma auditoria interna objetiva e eficaz e à criação de um comité de auditoria independente”. Deste modo as organizações teriam mais condições para assegurar e supervisionar os processos de preparação de documentos, as contas, os controlos internos e os códigos de conduta.

Como refere Gonçalves (2008) este relatório pretende que os responsáveis pela gestão concebam um sistema de controlo interno eficaz, graças à existência de um código de conduta e de uma comissão de auditoria que integre profissionais competentes e com conhecimento adequado da atividade desenvolvida.

⁷ Informação institucional CNSA

⁸ Devido aos escândalos de corrupção financeira de várias empresas como a Enron e Parmalat

Neste relatório o controlo interno foi definido como um processo, efetuado pela direção, gerentes e demais colaboradores com o objetivo de assegurar a eficácia e eficiência das operações e se estas cumprem com os regulamentos e as leis previstas. Foi esta comissão que criou o tão falado “*Committee of Sponsoring Organizations*” (COSO). As suas diretrizes foram publicadas em 1991, diretrizes estas, que foram sofrendo algumas revisões e atualizações ao longo dos últimos tempos. Segundo Flaherty e Maki em COSO 2004⁹, “desde a criação da referida estrutura esta tem sido incorporada em políticas, normas e regulamentos adotadas por inúmeras organizações, levando a que esta estrutura seja a escolhida pela maior parte das organizações”.

2.2 Governo das Sociedades na Europa

A problemática do “governo das sociedades” desenvolve-se fortemente na Europa quando em 1992 surge na Inglaterra o “*Relatório de Cadbury*”, que à semelhança do que aconteceu nos EUA, aparece na sequência de grandes escândalos financeiros ocorridos em várias empresas do Reino Unido. Este documento trouxe um importante desenvolvimento ao nível do “governo das sociedades” e por sua vez um reconhecimento significativo da auditoria interna. Segundo Câmara (2008), “o relatório britânico pretendia que os administradores elaborassem, anualmente, uma declaração sobre a eficácia do sistema de controlo interno, a qual por seu turno seria apreciada pelo auditor”. Esquemáticamente, o relatório “*Cadbury*” prevê (Mattedi, 2006):

- ✓ Que as informações devem ser apresentadas frequentemente e com clareza;
- ✓ Elucidar sobre as responsabilidades dos administradores executivos e não executivos dentro da entidade;
- ✓ Responsabilizar os executivos sobre a análise e apresentação de informações para os acionistas;
- ✓ Elucidar sobre as responsabilidades dos auditores e a extensão das suas atribuições;
- ✓ A constituição e o papel dos conselhos,
- ✓ As ligações entre acionistas, conselhos e auditores.

⁹ Enterprise Risk Management — Integrated Framework Executive Summary

Posteriormente, mais propriamente no ano de 1995 surge o “*Relatório Greenbury*” que, e de acordo, com Pires (2008), caracteriza-se por recomendar o reforço da relação existente entre a remuneração e o desempenho do conselho de administração. Recomendando a divulgação das remunerações nos relatórios anuais e a criação de um comité de remunerações, composto por administradores não executivos. Ainda em 1995 surge o “*Relatório Hampe*” que segundo Cunha e Martins (2007) “tenta desenvolver *Standards* elevados de governo das sociedades destacando a proteção dos investidores e a tentativa em garantir o bom desempenho das empresas inglesas cotadas em bolsa”. Este relatório vem apoiar os pressupostos dos relatórios de *Cadbury* e de *Greenbury* reforçando, alguns aspetos. Em 1999 aparece um novo relatório, o “*Relatório Turnbull*” que acaba por juntar o que de melhor há nos relatórios já aqui mencionados. O principal objetivo é assegurar uma boa gestão das empresas centrando a atenção nos aspetos relativos ao controlo interno e na gestão do risco.

2.3 Governo das Sociedades em Portugal

Como vimos o “governo das sociedades” tem conhecido uma difusão em todos os mercados internacionais e Portugal não é exceção. Aliás, a vivida internacionalização das sociedades e globalização dos mercados leva a que seja importante nivelar parâmetros de segurança da organização e dos agentes dos mercados, sendo impossível que Portugal se desvie desta problemática. Em território nacional, dispomos de algumas disposições ou recomendações que se assemelham às disposições previstas pela lei SOX¹⁰, nomeadamente as recomendações da CMVM¹¹, alguns artigos previstos no Código das Sociedades Comerciais, algumas disposições do regulamento dos Revisores Oficiais de Contas, e mais recentemente através do Instituto Português de *Corporate Governance* (IPCG), que neste momento apresenta um projeto de Código de Bom “governo das Sociedades”¹².

¹⁰ A lei Sarbanes Oxley Act (SOX) tenta restabelecer a confiança dos investidores no mercado de capitais Americano transformando as boas práticas de governo das sociedades em leis. Torna a gestão responsável por estabelecer, avaliar e monitorizar a eficiência e eficácia do controlo e procedimentos internos. Visto que esta lei não é de aplicação obrigatória em Portugal, a maioria das empresas têm vindo a seguir as recomendações e regulamentos emitidos pela CMVM sobre o governo das sociedades. No entanto, e porque algumas empresas portuguesas estiveram ou estão cotadas na bolsa americana, existem empresas que possuem estas duas estruturas.

¹¹ Comissão do Mercado de Valores Mobiliários

¹² Prevê-se que o novo regulamento só seja aplicável ao exercício de 2014, mantendo-se em vigor até 31 de Dezembro de 2013 o atual Regulamento da CMVM n.º 1/2010.

No entanto, e embora não seja a única entidade a fazê-lo, a CMVM tem desempenhado um papel fundamental na implementação das boas práticas do “governo das sociedades” em Portugal, uma vez que é da sua responsabilidades a elaboração de recomendações e aprovação de regulamentos sobre o governo das sociedades das entidades cotadas.

Segundo Moreira et all (2004, ap.) “uma adequada política de “governo das sociedades” deve: garantir a transparência; assegurar a defesa dos acionistas e dos credores; responsabilizar os gestores pelos incumprimentos de objetivos e pelas violações à lei; não impedir a maximização de performance; ser conforme aos *standards* internacionais e ser ajustada à realidade do país”.

As recomendações da CMVM que têm conhecido uma evolução significativa, quer quanto ao seu conteúdo, quer quanto à sua envolvência. A primeira edição destas recomendações surge no ano de 1999, e “ limitava-se a procurar que os emitentes de ações admitidas à negociação em mercado regulamentado informassem o mercado sobre o grau de cumprimento das recomendações” (Pereira e Branco 2005, pp. 1)

Dois anos mais tarde, o Regulamento n.º 7/2001¹³ da CMVM aderiu ao princípio “cumpra ou explica” e propõe que “as sociedades emissoras de ações admitidas à negociação em mercado regulamentado devem divulgar anualmente informações sobre diversos aspetos ligados ao governo societário. Sendo de salientar aquelas relativas ao cumprimento ou incumprimento das recomendações, sempre acompanhadas da respetiva fundamentação” (CMVM, 2005). Pereira e Branco (2005) salientam o facto de este regulamento “obrigar as sociedades emissoras de ações a elaborar um relatório sobre o governo da sociedade, em anexo ao relatório anual de gestão, ou num capítulo separado”.

Em 2003, ocorreu uma nova revisão de forma a tornar mais completo o relatório anual sobre o “governo das sociedades” mantendo-se contudo as linhas fundamentais do Regulamento n.º 7/2001, e em especial a filosofia “cumpra ou explica” que continuou a crescer. Esta revisão que foi precedida de discussão pública, valorizou o conceito de “administrador independente” e criou novos deveres de informação das sociedades, incluindo informação sobre os honorários pagos aos auditores e divulgação de informação obrigatória através de *Site* na *internet* (Pereira e Branco, 2005).

¹³ Governo Sociedades Cotadas

Por sua vez em 2005 surgem novas modificações que estão relacionadas com o aperfeiçoamento do sistema de fiscalização interna e o reforço da transparência das sociedades, o que se traduz, na prática, numa maior exigência informativa ao nível do relatório anual sobre o “governo das sociedades” (CMVM, 2007 b).

Sumariamente, as novas recomendações da CMVM passam por sugerir (Tavares, 2006):

- ✓ A criação de um gabinete de apoio ao investidor;
- ✓ A eliminação das limitações ao exercício do voto, diretamente, por correspondência, ou por procuração;
- ✓ A criação de um sistema interno de controlo para a deteção eficaz de riscos ligados à atividade da empresa, em salvaguarda do seu património e em benefício da transparência do seu governo societário;
- ✓ A adoção de medidas para impedir o êxito de ofertas públicas de aquisição deve respeitar os interesses da sociedade e dos seus acionistas;
- ✓ A existência de um número suficiente de administradores não executivos e de administradores independentes;
- ✓ A existência de uma política interna de comunicação das irregularidades ocorridas na sociedade;
- ✓ A criação, pelo órgão de administração de comissões internas de controlo com atribuição de competências na avaliação da estrutura e governo societários;
- ✓ A divulgação das remunerações individuais dos administradores e aprovação pela assembleia-geral de uma política de remuneração dos órgãos da administração;
- ✓ A independência dos membros da comissão de remunerações ou equivalentes relativamente aos membros do órgão de administração;
- ✓ A submissão à assembleia-geral da proposta relativa à aprovação de planos de atribuição de ações, e/ou de opções de aquisição de ações ou com base nas variações do preço das ações, a membros do órgão de administração e/ou trabalhadores.

Em 2007 faz-se uma nova revisão em que um conjunto de recomendações conhece uma nova arrumação sistemática e passa a ser designado por “*Código do Governo das Sociedades da CMVM*”.

No mesmo ano de 2007, a CMVM aprovou o Regulamento n.º 1/2007, com conseqüente revogação do Regulamento n.º 7/2001. “A revisão bienal do texto das “Recomendações da CMVM sobre governo das sociedades”, levou a sucessivas modificações do Regulamento n.º 7/2001 (Regulamentos da CMVM n.ºs 11/2003, 10/2005 e 3/2006), com o propósito de adequar o enquadramento regulamentar e recomendatório à evolução do padrão regulatório, ditada pela aprovação de textos relevantes tais como as recomendação da Comissão Europeia sobre independência dos auditores, sobre o papel dos administradores não executivos e sobre a remuneração dos administradores, o plano de ação da Comissão Europeia sobre direito das sociedades e a revisão dos princípios da OCDE sobre o governo das sociedades” (CMVM, 2007 a).

Neste sentido a CMVM, tem como principal objetivo melhorar as estruturas de “governo das sociedades” português e “importar” para o contexto nacional as melhores práticas de “governo das sociedades” cotadas. Ou seja, pretende recuperar a confiança dos investidores no mercado de capitais português e nos modelos de governo societário existentes (CMVM, 2001).

“No entanto, a adoção do Regulamento n.º 1/2007 insere-se numa linha de continuidade sendo que as grandes diferenças surgem no conteúdo do relatório anual de governação, nos deveres de transparência a cargo da sociedade e nos deveres informativos dos membros dos respetivos órgãos sociais” (CMVM, 2007 a).

Assim, quanto às modificações surgidas, destacam-se as alterações na estrutura do relatório sobre a estrutura e a prática do “governo das sociedades”, a divulgar por sociedades emittentes de ações admitidas à negociação em mercado regulamentado e sujeitas a lei portuguesa, de modo a alinhar o teor do relatório com a nova sistematização das recomendações, agora convertidas no “código sobre o governo das sociedades da CMVM”. Contudo, a CMVM renova a instrução principal quanto ao modo de elaboração do documento, prevendo que o “relatório não deve ser elaborado como se um inquérito de preenchimento mecânico se tratasse, mas antes deve ser entendido enquanto exercício de reflexão crítica e tomada de posição, pela sociedade, sobre as sãs práticas do governo das sociedades” (CMVM, 2007 a).

Deste modo, e graças às novas recomendações e ao novo regulamento sobre o “governo das sociedades” aprovado pela CMVM, podemos considerar que o ano de 2008 pode ser visto como o ano de viragem para o “governo das sociedades” cotadas, em Portugal.

No entanto, mais alterações se processaram durante os anos, estando em vigor o Regulamento n.º 4/2013 que enquadra os termos em que as sociedades emitentes devem elaborar o relatório anual sobre a estrutura e as práticas do “governo societário”. Não obstante a CMVM continuar a proporcionar um Código de Governo apto a promover a implementação das melhores práticas societárias, o juízo quanto ao mérito da escolha pelo Código a que cada sociedade se submete deixa de ser feito pela CMVM, impendendo, ao invés, exclusivamente sobre esta. Serão os órgãos decisórios desta sociedade que deverão justificar de forma fundamentada a opção tomada, constituindo esta a única contrapartida para o maior grau de liberdade que esta opção proporciona. Não obstante a entrada em vigor deste dispositivo estar fixada em 1 de Janeiro de 2014, admite-se no preâmbulo do documento “ a possibilidade (*rectius*, o dever) de, ainda no decurso de 2013, as sociedades conformarem as suas práticas de governo com as recomendações decorrentes de qualquer Código de Governo. “O regime relativo ao “governo das sociedades” encontra-se hoje, entre nós, predominantemente estruturado de acordo com um modelo de regulação pela CMVM assente na imposição às sociedades emitentes de ações admitidas à negociação em mercado regulamentado, situado ou a funcionar em Portugal, do dever de prestação e divulgação de informação por via da elaboração de um relatório sobre a estrutura e as práticas de governo societário (“*relatório de governo societário*”), cujo conteúdo é o resultado da convocação de normas legais, regulamentares e da descrição quanto ao grau de adoção de Códigos de Governo de natureza recomendatória.”¹⁴

No âmbito do conteúdo informativo de prestação obrigatória são reformuladas as exigências de fonte regulamentar, centrando-as na prestação das informações tidas por essenciais para garantia de um conhecimento adequado das práticas de governo adotadas por cada sociedade. Diz o referido regulamento que ““No que respeita à vertente recomendatória passa a admitir-se o recurso a Códigos de Governo distintos do Código da CMVM (art. 2.º, n.º 1), sem que tal possibilidade dependa de qualquer apreciação prévia por parte desta entidade”. A revisão do regime empreendida incide sobre o conteúdo do referido relatório, sistematizando as exigências informativas cuja prestação é obrigatória, possibilitando que as sociedades recorram a um Código de Governo das sociedades distinto daquele divulgado pela CMVM e reformulando o próprio Código de Governo das Sociedades disponibilizado pela CMVM, cuja última versão remonta já a 2010.

¹⁴ Regulamento n.º 4/2013 CMVM

3. *Ética*

Uma avaliação ou juízo sobre uma pessoa ou entidade é sempre o resultado inspirado nas impressões e análises de carácter pessoal, social, ou perfil do sujeito avaliado. A mesma é materializada sob a forma de notícias, comunicações, comentários, ou opiniões sobre o sujeito em causa. Toda a informação colocada a disposição dos utentes independentemente da fonte informativa ser essa entidade, devera ter a capacidade de gerar impressões sobre o seu carácter ou perfil, aos seus utentes/analistas.

O modo mais seguro de uma entidade controlar a boa reputação, a imagem e até uma interação mais profunda com as sociedades será garantir que o relacionamento com os seus parceiros e demais interessados se desenvolva de forma justa e correta. A justiça confunde-se muitas vezes com a ética, pois ambos personificam os valores positivos para uma melhor sociedade. Na atualidade, muitas das existentes ameaças globais são efeitos da crise financeira mundial, consequência de governações empresariais goradas, questões de agência e praticas legalmente duvidosas, apresentação de informações deturpadas/manipuladas contendo erros e omissões relevantes.

Com a evolução do fenómeno mundial das crises financeiras, surgem as primeiras debilidades e incapacidades de resposta empresarial como fruto da mentira e sustentadas polémicas governativas. Dai surgirem verdadeiros e inevitáveis escândalos em prejuízo da confiança depositada nas organizações e nos sistemas económicos. “Faliu a Mentira”, agora impera o medo e a desconfiança entre as organizações, *stakeholders*, e *demais interessados*, com acentuados prejuízos causados pela ausência da reciprocidade ou relacionamentos proveitosos.

Só uma gestão ética e socialmente responsável encorajada na sustentabilidade e desempenho com práticas diárias e contínuas poderão garantir, com mérito, o *feedback* ou recompensa da sociedade. A confiança dos utentes na empresa/organização é um privilégio, e conquista-se trabalhando por merece-la, agindo honestamente e respeitando os valores éticos e morais. Em capítulos seguintes iremos também abordar temas como, conflitos de interesse e fraude no sistema financeiro.

Práticas responsáveis e corretas são as que mais capitalizam em favor das instituições para o sucesso e realização dos objetivos, e missão das mesmas. Mais ainda, a importância do compromisso empresarial na implementação de regras ou condutas de funcionamento condizentes com os valores mais apreciados na sociedade e sobretudo com sucessivas formações e práticas continuadas com os colaboradores. Dai, também os gestores ou administradores de topo devem ser exemplares nas práticas que moldam a boa cultura empresarial.

3.1 Ética e Transparência Empresarial

Ética está associada a valores positivos, comportamentos ou práticas de convivência socialmente aceites – A Sociedade. Fundamentalmente ser ético ou agir eticamente é segundo a doutrina fazer algo que nos beneficie e, no mínimo, não prejudicar “outro”. Numa óptica empresarial podemos definir como uma prática de gestão ou administração empresarial transparente e socialmente responsável obtendo benefícios, cumprindo a missão e objeto social com satisfação da globalidade os utentes da empresa (*stakeholders* e/ou partes interessadas).

Porem, nem tudo é simples e genérico. A doutrina da ética tem questões ou dilemas naturais resultantes de múltiplas identidades culturais que influenciam e fazem repercutir diferentes valores éticos e morais. É também inequívoca a abertura das sociedades pelos fenómenos da globalização e mundialização, pelo que há uma evolução natural que permite a aceitação de novas práticas e costumes de outros povos e/ou sociedades, digna de um verdadeiro processo de socialização, mas também há barreiras que correspondem a diferentes princípios éticos entre o todo social.

Toda esta realidade não só afeta o ser social, como também se repercute nas instituições e/ou organizações inseridas no meio social. Logo, os ambientes empresariais que atuam num mercado globalizado, aberto e competitivo, estão sujeitos a necessidade de mudança pela conexão e interação com o meio social (ambiente global).

“Observando novas exigências regulamentares e as melhores práticas internacionais, a prestação de contas desenvolve-se este ano, pela primeira vez, ao longo de três volumes estruturados segundo temas distintos: o Relatório de Atividades e Análise Financeira; o Relatório de Governo de Sociedade e Contas e Notas às Demonstrações Financeiras; e o Relatório de Sustentabilidade”¹⁵

Qualquer organização que se prestigie tem os seus objetivos, missão e visão, cultura empresarial, valores e princípios empresariais divulgados, publicados e incutidos na própria organização.

*“É conhecido que comportamentos menos éticos têm prejudicado gravemente algumas organizações e os seus colaboradores. As suas consequências traduzem-se genericamente na perda de clientes, de trabalhadores, de vendas e da reputação, a qual leva anos a construir. Várias empresas não recuperam mais”*¹⁶

Em toda a estrutura organizacional existem regras e condutas comportamentais formais ou informais que podem ser mais ou menos complexas, e representam princípios e valores que garantem o bom funcionamento das organizações. Até nas micro-organizações existem regras e princípios que disciplinam as ações dos colaboradores, mesmo que não existam formalismos que regulem essas condutas comportamentais. Para implementar com seriedade, regras, princípios ou valores numa organização, que visem as boas praticas, e impreterivelmente necessária a criação de um código de valores com suporte físico ou digital, acessível a todos colaboradores. O código definira as responsabilidades, rigor e disciplina laboral ao qual os colaboradores devem respeito.

“No exercício das suas funções, os membros do órgão de administração e os colaboradores deverão pautar o seu desempenho pelos mais elevados padrões de integridade e honestidade pessoais, cumprindo todas as disposições legais e regulamentares em vigor aplicáveis as atividades a que se encontram adstritos, bem como todas as normas de deontologia previstas neste código ou nos códigos de conduta específicos aplicáveis a essas atividades”¹⁷

Para melhorar as formas de integração e implementação da ética na organização, deve-se aos colaboradores, instruí-los, testá-los, controlar ou fiscalizar em benefício da boa conduta ou práticas laborais. Se necessário tomar medidas proactivas, preventivas e ate corretivas consoante as circunstâncias.

¹⁵ Paulo Teixeira Pinto; Millennium BCP - Relatório e Contas 2005; pag. 5.

¹⁶ Conselho de Administração; Código de Ética, Grupo CTT

¹⁷ Informação institucional BCP (código deontológico)

A qualidade e justiça garantida nos relacionamentos com os interessados vão gerar e estimular confiança destes para com a organização. Toda a organização tem um perfil de identidade e uma imagem reconhecida pelo mercado, sendo fator decisivo no sucesso da mesma. A “nossa civilização e o mercado em geral não aceitam a falta de ética, e valorizam a responsabilidade social” (Conselho de Administração CTT)

“A imagem e a identidade das Organizações resultam cada vez mais, para além do seu desempenho económico e financeiro, dos princípios, valores e comportamentos que assumem.” (Idem)

Quando conjugando as palavras honestidade, responsabilidade, confiança e reputação, ambas são predicados que se seguem mesmo antes do sucesso de negócio ou empresarial. *Eamonn Butler* (2008) defende que “a construção de um negócio e conquista de clientes e outras partes interessadas, resulta da postura ética e honestidade do negociante”. O setor que estudamos assenta em pilares como a confiança e a responsabilidade, pelo que a Ética será um dos fatores mais importantes do negócio. O mesmo só é compensatório se existir uma relação de confiança que garanta justiça, verdade e certeza nos acordos celebrados entre a parte vendedora e compradora. Quem vende, tem palavra de seriedade e garante qualidades que resultam na confiança e satisfação do comprador, que por sua vez sabe o que compra e no mínimo deixara boas impressões do vendedor (fundamental no negocio).

Para *Eleri Hamer* (2008), “a relação de confiança, de como a empresa é vista por outras empresas, inicia-se na própria relação com os seus colaboradores, e isso acaba sendo propagado por estes aos seus parceiros comerciais de diversas formas.” E “desse modo, a confiança e a reputação terão peso cada vez maior nas relações comerciais e segundo alguns, são os que na prática, num futuro muito próximo, moverão as organizações, como um novo e grande diferencial competitivo.”

Para *Gómez Pérez* (1990), existem cinco motivos que podem justificar a necessidade da ética nos negócios:

- ✓ A consciência de solidariedade, pois “o mal que se faz redonda sempre em prejuízo de alguém”.
- ✓ A consciência de alteridade na medida em que “não faça ao outro o que não quer que te façam”.
- ✓ Medo das consequências da má imagem para a organização
- ✓ Medo das sanções legais que poderiam ocorrer
- ✓ Continuidade negócio

Conclui-se assim que os princípios éticos devem estar acima dos interesses particulares, mas deve haver um código de ética e conduta empresarial que sucessivamente promova a formação dos colaboradores e sensibilize para práticas corretas e aceitáveis na sociedade. Hoje há provas inequívocas de que o rigor e a responsabilidade assumem dentro das organizações posturas de conquista no mercado e sociedade. As organizações sem este tipo de valores, independente dos resultados apresentados, correm sérios riscos quanto a continuidade e futuro da entidade.

É no âmago desta cultura de responsabilidade e excelência que se insere o Código Deontológico, com o objetivo principal de permitir a cada destinatário conhecer os princípios e as regras que devem enquadrar toda a sua atuação. Estes princípios e regras deverão ser conhecidos, compreendidos, assimilados e escrupulosamente cumpridos, constituindo padrão de conduta dos membros dos órgãos sociais e de todos os Colaboradores.

A entidade deve ter consciência de que o desempenho da instituição e o cumprimento da sua missão dependem de cada profissional, prezando uma cultura de liberdade e responsabilidade, no entanto estes deverão pautar o seu desempenho pelos mais elevados padrões de integridade e honestidade pessoais, cumprindo todas as disposições legais e regulamentares em vigor aplicáveis às atividades a que se encontram adstritos, bem como todas as normas de deontologia profissional previstas no Código deontológico, ou nos Códigos de Conduta específicos aplicáveis a essas atividades. Todos os profissionais deverão tomar as medidas adequadas e que estejam ao seu alcance para frustrar práticas de que tenham conhecimento e que integrem utilização abusiva de informação ou consubstanciem infração às normas vigentes.

- ✓ Dever de integridade e honestidade
- ✓ Dever de competência
- ✓ Dever de cooperação e transparência
- ✓ Dever de diligência
- ✓ Dever de segredo
- ✓ Dever de comunicar irregularidades

“O sistema de controlo interno, devera abranger o conjunto das estratégias, sistemas, processos, políticas e procedimentos definidos pelo órgão de administração, bem como das ações empreendidas por este órgão e pelos restantes Colaboradores da instituição, com o objetivo de garantir”:¹⁸

- ✓ Um desempenho eficiente e rentável da atividade, no médio e longo prazo que assegure a utilização eficaz dos ativos e recursos, a continuidade do negócio e a própria sobrevivência da Instituição, através nomeadamente, de uma adequada gestão e controlo dos riscos da atividade, de uma prudente e adequada avaliação dos ativos e responsabilidades, bem como da implementação de mecanismos de proteção contra utilizações não autorizadas, intencionais ou negligentes;
- ✓ A existência de informação financeira e de gestão, completa, pertinente, fiável e tempestiva, que suporte as tomadas de decisão e processos de controlo, tanto a nível interno como externo;
- ✓ O respeito pelas disposições legais e regulamentares aplicáveis, incluindo as relativas à prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como das normas e usos profissionais e deontológicos, das regras internas e estatutárias, das regras de conduta e de relacionamento com os Clientes, das orientações dos órgãos sociais e das recomendações do Comité de Supervisão Bancária (CEBS), de modo a proteger a reputação da Instituição e a evitar que esta seja alvo de sanções.

“Sendo o controlo interno de fulcral importância numa organização todos os Colaboradores deverão contribuir para o seu bom desempenho, devendo para o efeito compreender o seu papel no sistema implementado. Para atingir, de forma eficaz, os objetivos do Sistema de Controlo Interno, as instituições financeiras deverão assegurar que as áreas de Auditoria Interna, *Compliance* e Gestão do Risco, deverão ser dotadas da autonomia, liberdade e poderes necessários ao correto desempenho das suas funções”.¹⁹

¹⁸ Informação Institucional BCP

¹⁹ Idem

a) A Direção de Auditoria deverá exercer as suas funções, desenvolvendo ações de verificação e avaliação permanentes do Sistema de Controlo Interno;

b) O *Compliance Office*, de forma independente, permanente e efetiva, controlar o cumprimento das obrigações legais e dos deveres a que se encontram sujeitas, de modo a proteger a reputação das Instituições e a evitar que estas sejam alvo de sanções;

c) O *Risk Office*, assegurar a aplicação efetiva do Sistema de Gestão de Riscos, através do acompanhamento contínuo da sua adequação e eficácia, bem como da adequação e eficácia das medidas tomadas para corrigir eventuais deficiências desse sistema.

4. Risco

O mercado global em que a sociedade se encontra, o crescendo de expectativas dos consumidores, a agressividade da concorrência, as consequências que podem advir de falta de informação e do seu controlo devido a rápida evolução tecnológica e a crise económica mundial a que assistimos, está a afetar as organizações, expondo-as a uma grande variedade de riscos, que podem afetar a concretização dos seus intentos. Deste modo, as organizações devem conhecer os riscos que ameaçam a sua organização, de modo a implementar medidas adequadas que mitiguem estes mesmos riscos e assim não coloquem em causa a estratégia delineada.

O risco constitui um dado indissociável do negócio. Embora o Homem seja avesso à Incerteza, e consequentemente ao risco, a história demonstra que a espécie humana foi desenvolvendo uma longa aprendizagem no sentido de compreender a ocorrência de situações imprevistas e de prever e gerir os impactes delas decorrentes. Controlo e informação, são os dois elementos desde sempre utilizados para minimizar as repercussões negativas e otimizar os efeitos positivos. A noção de risco nem sempre é pacífica, no entanto, está sempre relacionada com os efeitos possíveis da ocorrência de um evento.

Em regra, está associado ao efeito negativo dessa ocorrência. Assim, o risco é a possibilidade de um evento ocorrer e afetar negativamente a concretização de um objetivo planeado, seja por uma pessoa ou por uma empresa. Assim neste sentido temos Borge (2001), citado por Beja (2004a:81) que considera que “Risco significa estar exposto à possibilidade de um resultado negativo”.

“O risco pode ser definido como uma possibilidade de que algum acontecimento desfavorável venha a ocorrer e que possa afetar um grande número de ativos da empresa” (Cruz:2008).

O COSO²⁰ define risco como sendo “a possibilidade de um evento ocorrer e afetar negativamente a realização dos objetivos”. Contudo, os eventos podem resultar de fontes internas ou externas à organização e podem causar impactos positivos e ou impactos negativos. Neste sentido, o COSO refere o seguinte:

“Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização de objetivos”(COSOa, 2004:28)

Na sequência do impacto poder ser negativo ou positivo encontramos o ideograma chinês que apresenta Risco/Crise através de dois símbolos



Figura 1 – Ideograma chinês

²⁰ Committee of Sponsoring Organizations

O ideograma chinês para "Crise/Risco" é a combinação de dois símbolos. Um significa a "Ameaça", o outro pode ser traduzido como "Oportunidade". Apesar dos riscos e ameaças, podemos estar diante de uma grande oportunidade de negócio. Por vezes, os riscos tornam-se em oportunidades. Desta forma, curiosamente os chineses na noção de risco têm os dois conceitos associados, ameaça (negativo) e oportunidade (positivo). Correr riscos é um facto inerente à própria existência de uma empresa, pressupondo, contudo, que esta tenha uma capacidade e vontade de inovar e gerar riqueza, aproveitando assim as oportunidades que lhe vão surgindo de todo o meio envolvente. Essa capacidade fará com que a empresa possa tirar proveito de uma situação de risco, transformando um risco numa oportunidade de acordo com a lógica da análise *SWOT* – ferramenta utilizada para fazer análises de cenários, nomeadamente na gestão e planeamento estratégico. **SWOT** é um termo inglês, acrónimo de Forças (**Strengths**), Fraquezas (**Weaknesses**), Oportunidades (**Opportunities**) e Ameaças (**Threats**). A metodologia de gestão de risco deve assentar nos processos de negócio. Através da forma de funcionamento da organização é efetuada a definição dos *accountables* pelos processos e a descrição dos procedimentos e regras instituídas na organização, após os quais se definem os indicadores de risco desses mesmos processos.

Porém, apesar de existirem vários modelos processuais de referência, todas as empresas são diferentes, e neste contexto, também os indicadores de risco variam de entidade para entidade. As áreas de risco dispõem também de vários modelos e várias metodologias de referência no mercado a nível mundial e neste âmbito, destacamos a metodologia COSO. É a metodologia mais adotada a nível mundial e que tem sido também frequentemente implementada nas organizações em Portugal.

O COSO (2004, p. 4) considera que Gestão de Risco é:

“Um processo desenvolvido pela administração, gestão e outras pessoas, aplicado na definição estratégica ao longo da organização, desenhado para identificar potencia eventos que podem afetar a entidade, e gerir os riscos para níveis aceitáveis, fornecendo uma garantia razoável de que os objetivos da organização serão alcançados.”²¹

²¹ Enterprise Risk Management Framework – COSO I

Ambientes instáveis e fortemente competitivos com tecnologias sofisticadas e com ciclos de vida cada vez mais curtos, com acesso à informação global generalizado, fazem crescer exponencialmente o risco nas organizações, daí a necessidade de um Ambiente de controlo que privilegie o desempenho e a competição, em contraste com os controlos de conformidade existentes no passado, sendo o seu principal objetivo assegurar a eficiente utilização dos recursos e a eficácia das organizações, processos onde mais se fazem sentir os efeitos dos impactos dos novos fatores de risco.



Figura 2 – Risco e principais Interessados (Fonte: produção própria)

O risco está no centro das atenções de toda a organização, desde o Conselho de Administração, Gestores de Topo, Gestores Operacionais, Auditores e Reguladores Externos, Auditoria Interna e Comité de Auditoria (quando existe), como podemos observar na figura (2).

A Auditoria Interna reporta diretamente ao Comité de Auditoria, caso a empresa disponha deste órgão, se não existir deve reportar à Administração, sendo independente de qualquer outro órgão dentro da organização. Assim sendo a decisão da Auditoria Interna focar o seu trabalho na identificação e avaliação dos riscos parte de instruções dadas pelo Comité de Auditoria, conforme se apresenta na figura anterior, ou da Administração.

Por outro lado, cada entidade deve adotar uma metodologia específica para implantar o seu processo de gestão de risco, adaptando a sua cultura, filosofia de gestão e objetivos de negócio. Deve ser concebido segundo a natureza das suas atividades e dependendo do seu tamanho e complexidade, o processo pode ser formal ou informal,

quantitativo ou subjetivo descentralizado a unidades de negócio ou centralizado a entidade. De acordo com Beja (2004a), “o conceito de Gestão de Risco que representa o conjunto de meios utilizados na identificação, avaliação e relato do risco empresarial, surgiu nos Estados Unidos da América, e foi referido pela primeira vez num artigo publicado no “*Harvard Business Review*” no ano de 1956”.

No entanto, só nos finais do Século XX, é que a Gestão de Risco foi considerada como um elemento importante e essencial no governo empresarial. A Gestão de Risco Empresarial passou a fazer parte das boas práticas de gestão, apoiando a tomada de decisão. A gestão de risco envolve um conjunto muito diversificado de atividades e ações, que vão desde as que se relacionam com os riscos dos negócios, até às que dizem respeito aos riscos dos processos operacionais da empresa.

“Esta gestão deve ser integrada e unificadora, dado que as decisões tomadas por uma determinada área para reduzir os seus riscos poderão criar ou aumentá-los noutra área” (Azevedo, 2005).

A Gestão de Risco, de acordo com o Instituto de Gestão de Risco (IRM) de Londres, conforme citado por Willsher (2007:45), “é o processo que pretende ajudar as organizações a compreender, avaliar e atuar sobre todos os seus riscos, para aumentar a probabilidade de sucesso e reduzir a de fracasso”.

De acordo com Azevedo (2005:14) “criar valor implica assumir riscos, conhecê-los e geri-los dá-nos uma força necessária para a fabulosa “aventura” que é de criar riqueza e emprego”.

Segundo o COSO ERM, Gestão de Risco Empresarial é “um processo, desenvolvido pelo Conselho de Administração, Órgãos de Gestão e outros elementos da organização, aplicado na definição da estratégia e que deve abranger toda a organização. Este processo tem como objetivo a identificação dos eventos que podem afetar a organização e a gestão dos riscos, alinhados com o perfil de exposição definido, com vista a providenciar uma segurança aceitável com vista ao cumprimento dos objetivos definidos pela organização” COSO (2004a:16). A gestão de risco é um meio para atingir um fim e, não um fim em si mesmo. É um processo educativo que nos consciencializa que de facto existem riscos, e que aos gestores cabe a responsabilidade de os gerir.

De acordo com Ferma “a gestão de risco deve ser um processo contínuo e em constante desenvolvimento aplicado à estratégia da organização e à implementação dessa mesma estratégia. Deve analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e, em especial, futuras de uma organização” (Ferma, 2003).

Ainda no âmbito da definição de risco há que caracterizar dois conceitos distintos mas bastante relacionados – Risco e Incerteza. Segundo David McNamee, “risco é a quantificação da incerteza”. No processo de negócio a incerteza está associada a concretização dos objetivos organizacionais. As consequências podem ser positivas (oportunidades) ou negativas (apenas riscos).

Cruz (2008), apresenta uma perspetiva sobre o assunto tendo sido feita por este autor uma interessante distinção entre estes dois conceitos:

1. O risco está associado à probabilidade de ocorrência de perda - acontecimentos incertos. Ainda na sua perspetiva, os acontecimentos incertos podem classifica-se em duas categorias distintas, sendo elas:
 - ✓ Acontecimento cuja probabilidade de ocorrência se pode determinar à priori ou tentando seguir um padrão já ocorrido no passado;
 - ✓ Acontecimentos sem probabilidade associada – Considerados imprevisíveis, quer por não existir um padrão definido que permita o cálculo da probabilidade para a sua ocorrência, querem por serem considerados acontecimentos únicos.
2. A incerteza consubstancia-se na falta de conhecimento *à priori* referente ao resultado de uma ação ou ao efeito de uma determinada condição. Esta pode aplicar-se à dificuldade em prever eventos futuros, ou referir-se ainda a eventuais erros ocorridos em procedimentos já realizados.

A tentativa de redução da incerteza é a origem da gestão profissional de riscos, de acordo com *Veja* (2003). O mesmo autor refere, ainda, que “a gestão de riscos, nomeadamente, os operacionais e os de cumprimento, servirá para melhorar o Controlo Interno e, portanto, como medida para potenciar o bom governo corporativo”.

Nestes últimos anos, a gestão de riscos, de um modo geral, tem procurado aproveitar as oportunidades de ganho e minimizar os impactos negativos. A "nova" gestão de risco é parte integrante das boas práticas de gestão empresarial e é um elemento essencial do governo empresarial.

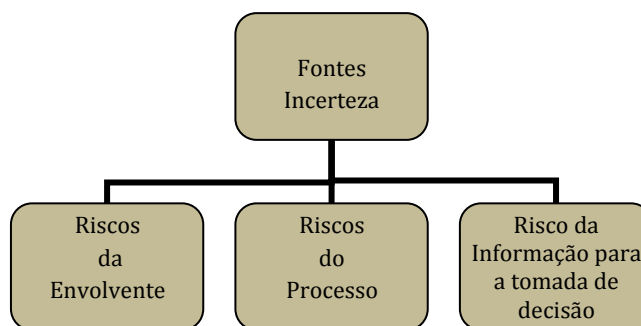


Figura 3 - Fontes de Incerteza
Fonte: Protiviti, 2006

De acordo com Ferma (2003) "o risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências (ISO/IEC Guide 73)". De acordo com Beja (2004b) "o risco constitui uma componente intrínseca do negócio e a informação sobre os riscos do negócio assume-se como um dos principais temas do moderno governo empresarial". A nova norma internacional sobre Gestão de Risco, ISO 31000:2009, segundo Simões (2009), define que o Risco "é o efeito da incerteza nos objetivos".

No mesmo sentido, Morais e Martins (2007), defendem que o risco é importante e interfere no trabalho dos auditores internos, já que a necessidade de controlo é tanto maior quanto maior for o risco. No círculo da gestão de riscos, a incerteza é um fator que deverá ser mantido sob controlo, pois num ambiente empresarial há que tomar decisões, muitas das vezes, tão repentinas e sem as informações mais detalhadas quanto seria desejável, o que fará com que essas situações se revistam de uma enorme incerteza, situação esta que não permitirá controlar as consequências da decisão tomada, podendo estas ser danosas para a organização.

Uma estratégia global e adequada de gestão dos riscos do negócio releva de um escrutínio prévio e completo das situações de risco potencial, obedecendo a três Itens:

- ✓ **Categorias do risco** (análise vertical de âmbito global) – implicam a elaboração de uma lista em que, para cada categoria, se indiquem as situações de risco mais suscetíveis de ter impacte significativo naquela empresa em concreto

- ✓ **Identificação do risco** (análise horizontal por cadeias de valor e/ou processos de negócio) – implica que cada categoria / situação de risco seja analisada numa perspetiva do efeito que pode resultar do respetivo impacto transversal em cada uma das principais atividades ou processos, nomeadamente: gestão global; aquisições; tecnologias; investigação, produção; comercialização; distribuição; finanças; operações; e recursos humanos

- ✓ **Prioridades de atuação** – implicam uma primeira estimativa de graduação dos riscos, de forma a concentrar esforços nas situações materialmente relevantes. Como elemento auxiliar para este diagnóstico pode ser utilizada uma matriz simples, que cruze o nível de probabilidade de consumação do risco com a dimensão previsível do respetivo impacte no negócio. A atuação será priorizada em função do resultado obtido através do referido cruzamento destas duas variáveis.

Na gestão de riscos devem ser utilizadas metodologias adequadas, senso comum, conhecimento da cultura organizacional e, ainda, sensibilidade pessoal.

A principal diferença entre o processo de ERM²² e as outras formas tradicionais de gestão de risco é que o processo de ERM adota uma perspetiva que coordena a gestão de risco ao longo de toda a organização, em vez de cada área da organização gerir os seus próprios riscos” (Banham, 2004) citado por Castanheira e Rodrigues (2006b:58).

²² Enterprise Risk Management

De acordo com Hussein (2008), o “*American Institute of Certified Public Accountants*” (AICPA), classificou os riscos em três grupos, a saber:

- ✓ Riscos relacionados com o ambiente empresarial – ameaças do ambiente empresarial em que a entidade opera, como riscos decorrentes da atuação da concorrência, políticos, legais ou decorrentes da ação de órgãos reguladores e fiscalizadores, financeiros e de procura;
- ✓ Riscos relacionados com o processo de negócio e dos seus ativos – ameaças ao negócio da organização pelos concorrentes e perdas de ativos, sejam físicos ou financeiros; e,
- ✓ Riscos relacionados com as informações – ocorrência de ameaças decorrentes de má qualidade das informações para o processo de tomada de decisão e, fornecimento de informações a terceiros.

O risco, assumido como uma componente intrínseca ao negócio, implica o domínio de estratégias apropriadas²³:

- ✓ ***Prevenir riscos*** – *é a estratégia mais óbvia. Nunca se deve correr um risco que não tenha potencial de contribuição positiva. Quanto melhor preparados para identificar e quantificar riscos, maior sucesso teremos no prevenir ou evitar riscos indesejáveis;*
- ✓ ***Criar riscos*** – *corresponde ao aproveitamento de oportunidades atrativas em que o ganho potencial justifica o risco. O objetivo de gestão do risco não é eliminá-lo mas exercê-lo controladamente;*
- ✓ ***Comprar ou vender riscos*** – *pode ser vantajoso adquirir uma posição de risco com elevado potencial de ganho, como se pode alienar um risco não desejado assumindo uma perda imediata de valor;*
- ✓ ***Diversificar riscos*** – *é uma forma poderosa de gerir riscos, utilizada ao longo dos séculos, de uma ou outra forma. Corresponde ao aforismo popular: não pôr todos os ovos no mesmo cesto;*

²³ Borge, Dan, *The Book of Risk* (p. 65-82), John Wiley & Sons, New York, 2001 (tradução do autor)

- ✓ **Concentrar riscos** – pode ser indicado quando existe capacidade para exercer influência sobre o resultado a obter, especialmente quando tal depender de uma também elevada concentração de atenção e de esforços;
- ✓ **Compensar riscos** – pratica-se quando para não se correr um risco elevado, se adquire um risco correspondente de sentido contrário. Trata-se de uma opção com algum perigo, pela dificuldade em encontrar uma compensação perfeita e sem custos, e que tem conduzido algumas instituições a assumir riscos elevados que acabam por se mostrar desastrosos;
- ✓ **Impulsionar riscos** – tem a expressão mais comum no efeito de alavanca produzido pela obtenção de financiamento externo para desenvolvimento de um projeto ou compra de um ativo. O efeito de impulso (ou alavanca) aumenta o potencial de ganho proveniente do investimento mas aumenta igualmente o risco de percas

4.1 O COSO ERM

Em 2001, o COSO iniciou um projeto, em parceria com a *PricewaterhouseCoopers* com vista ao desenvolvimento de um modelo que permitisse ajudar os gestores na avaliação e melhoria da gestão de risco das suas organizações. Os escândalos financeiros das empresas que manipularam as informações financeiras como a Enron e outras empresas, afetaram de forma significativa a confiança dos investidores, funcionários e outros “*Stakeholders*”, vindo reforçar a necessidade de maior transparência e fiabilidade na realização e divulgação de informação contabilística e financeira e introdução de medidas de melhoria e reforço de competências ao nível da governação corporativa e da gestão de risco, através de novas leis e regulamentações.

Estes factos vieram reforçar a necessidade do desenvolvimento de um modelo de gestão de risco que fornecesse princípios e conceitos chave, uma linguagem comum e que constituísse um guia para a Gestão de Risco nas organizações.

O modelo de Gestão de Risco (publicado em Setembro de 2004), designado Gestão de Riscos Corporativos – Estrutura Integrada, emitido pelo “*Committee of Sponsoring Organizations of the Treadway Commission*” (COSO) com a colaboração da *PriceWaterHouseCoopers* expande-se para além do sistema de Controlo Interno, promovendo uma focalização mais forte e abrangente na gestão de risco empresarial.

Não substitui o modelo de controlo interno desenvolvido pelo COSO em 1992, mas incorpora-o, permitindo que as organizações adotem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno, progredindo para um processo de gestão de risco.

De salientar que todos os dias, as organizações enfrentam incertezas, desafios e uma diversidade de riscos, sendo o grande desafio da Gestão determinar qual é o nível de incerteza para o qual a empresa está preparada para aceitar.

O COSO define ERM²⁴ como um “processo efetuado pelo Conselho de Administração, a Direção e restante pessoal de uma entidade, aplicado a definição da estratégia de toda a entidade e concebido para identificar potenciais acontecimentos que possam afetar a entidade e gerir os riscos dentro do risco aceitável, assegurando razoavelmente a concretização dos objetivos”

Nem todos os riscos apresentam o mesmo nível de importância. A gestão de riscos corporativos permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos cujo impacto seja maior – quer seja positivo quer seja negativo, com o objetivo de criar valor para os acionistas.

O modelo de Gestão de Risco proposto pelo COSO-ERM é apresentado como um modelo de referência, não só a nível internacional como também a nível nacional. O modelo proposto está assente em 8 componentes que são afetados de acordo com os objetivos da organização. Estes objetivos podem ser classificados em:

- ✓ Estratégicos
- ✓ Táticos
- ✓ Comunicação
- ✓ Regulação e Conformidade Legal.

²⁴ COSO- Enterprise Risk management Integrated Framework, www.coso.org, 2004

Existe uma relação direta entre objetivos e componentes, uma vez que os objetivos são metas que a entidade pretende alcançar e os componentes são os meios necessários para atingir esses objetivos. Esta relação é representada através de uma matriz tridimensional, com o aspeto de um cubo, conforme figura a seguir:



Figura 4 - Cubo do COSO ERM (Fonte: COSO, 2004b)
The Committee of sponsoring Organizations of the Treadway Commission

O modelo deverá ser avaliado e implementado de uma forma abrangente a toda a organização, partindo de um nível mais elevado (Entidade) até chegar ao nível mais básico (Atividades). De acordo com este modelo, os componentes da gestão do risco estão identificados como sendo os seguintes:

- ✓ Ambiente Interno, ou seja, contexto ou ambiente onde as organizações funcionam com objetivos a atingir e meios a serem utilizados para esse fim. Abrange a cultura da organização, a base como o risco é visto e dirigido por uma entidade, incluindo a gestão do risco, a consciência interna sobre risco, a integridade, os valores éticos e o ambiente em que a empresa opera.
- ✓ Definição de Objetivos, é uma pré-condição para a identificação dos riscos, para a sua avaliação e formulação das respostas possíveis de serem implementadas.
- ✓ Identificação de Eventos/Acontecimentos, trata-se de identificar os fatores internos e externos, com capacidade de influenciar a estratégia e os seus objetivos. Os fatores externos compreendem a conjuntura económica/financeira, fatores sociais, políticos, tecnológicos e de natureza ambiental. Os fatores internos estão ligados às infraestruturas, aos ativos humanos, aos processos de trabalho e à tecnologia aplicada.

- ✓ Avaliação dos Riscos, a gestão avalia a situação potencial subdividindo o conceito de risco em risco inerente (aquele em que a organização incorre na ausência de medidas preventivas ou de correção) e risco residual (risco que permanece mesmo depois de tomadas as ações preventivas e/ou corretivas de comportamentos). Os riscos são valorizados mediante a probabilidade de ocorrência do acontecimento e das suas consequências ou impactos.

Na análise dos riscos, pode-se recorrer a análises qualitativas ou quantitativas dos mesmos. A análise qualitativa faz a priorização dos riscos através da avaliação e combinação da probabilidade de ocorrência e impacto. Já a análise quantitativa faz a análise numérica do efeito dos riscos identificados nos objetivos gerais.

- ✓ Resposta aos Riscos - depois de identificados e avaliados os riscos, a gestão deve preparar respostas que obedecem inevitavelmente às seguintes possibilidades: evitar o risco, reduzir o risco, partilhar o risco ou aceitar o risco. A resposta ao risco é o processo de desenvolver e determinar ações para mitigar os riscos, reduzindo as ameaças dos objetivos da organização. A administração avalia a probabilidade e o impacto da ocorrência do risco, os custos e benefícios, a prioridade das ações a implementar e seleciona a resposta que melhor se adequar dentro dos limites de tolerância do risco aceite.
- ✓ Controlo das atividades, este controlo deve ser efetuado através do vetor risco. Como tal deve ser enquadrado/identificado com as políticas (o que deve ser feito) e os procedimentos (a forma como se deve fazer) que garantem a resposta aos riscos.
- ✓ Informação e comunicação, torna-se particularmente importante com vista a facilitar a criação de valor acrescentado, formalizar na organização um sistema de informação estratégico.
- ✓ Monitorização, pode revestir-se de duas formas. A primeira prende-se com o conhecimento (em tempo real) do desenvolvimento das atividades, sendo a monitorização, neste caso, parte integrante das atividades operacionais definidas numa organização. A segunda consiste em atividades de avaliação, que o departamento de Auditoria Interna e outras entidades desenvolvem, em função do perfil e frequência dos riscos, da dificuldade ou importância das respostas aos riscos e dos seus controlos de gestão.

4.2 Limitações da Gestão de Risco Empresarial

A Gestão de Risco Empresarial, qualquer que seja o modelo que se aplique, não garante que os objetivos de uma organização sejam todos atingidos, apenas dá uma segurança razoável de que tais objetivos possam ser alcançados. Não nos podemos esquecer que o risco pertence ao futuro, logo é um acontecimento que não é possível prever com segurança e muitos deles não dependem da própria organização, são externos à organização, o que os torna ainda mais difíceis de prever.

A gestão de riscos é feita por pessoas, logo, existe a possibilidade de ocorrer um erro humano, como por exemplo uma informação mal entendida pode dar origem a uma decisão ou um juízo de valor menos correta, podendo afetar a concretização de determinado objetivo. Por outro lado, e tendo em consideração os dias de hoje, em que os recursos são escassos, as organizações devem ter em consideração os custos/benefícios da implementação de controlos para a mitigação de riscos, ou até mesmo ponderar se é vantajoso para determinada organização implementar um modelo de gestão de risco. De acordo com o COSO ERM, o conceito de segurança razoável, não quer dizer que a gestão de riscos corporativa vá fracassar frequentemente. Contudo, pode ocorrer um erro, um evento incontrolável ou uma informação falsa. Uma segurança razoável não constitui uma segurança absoluta. Embora as metodologias utilizadas como instrumento para exercer a Auditoria, tenham vindo a ser diferentes ao longo do tempo, as mesmas têm algo em comum:

- Enquanto na abordagem conceptual do controlo interno, o ambiente de controlo consiste na análise articulada dos elementos chave seguintes:
 - ✓ Comunicação e enfoque na integridade e valores éticos;
 - ✓ Compromisso com a competência;
 - ✓ Filosofia de gestão;
 - ✓ Estrutura organizacional;
 - ✓ Atribuição de autoridade responsabilidades;
 - ✓ Políticas e procedimentos relativos aos recursos humanos;

- Na abordagem conceptual da gestão do risco empresarial (ERM) o topo das componentes do risco relevam os aspetos da:
- ✓ Filosofia de gestão do risco;
 - ✓ Apetência ao risco;
 - ✓ Atitude dos gestores de topo, dos responsáveis da governação e gestão;
 - ✓ Integridade e valores éticos;
 - ✓ Compromisso com a competência;
 - ✓ Estrutura organizacional;
 - ✓ Atribuição de autoridade responsabilidades;
 - ✓ Políticas e procedimentos relativos aos recursos humanos;

Qualquer um dos modelos conceptuais referidos reconhece, que na base de qualquer sistema de controlo interno, ou de gestão do risco empresarial, o papel desempenhado pelos responsáveis da governação e gestão é essencial. Os sistemas não existem e evoluem por si, são concebidos, implementados e monitorizados pelas pessoas, pelo que a ênfase na avaliação, quer do sistema de controlo interno quer no sistema de gestão do risco empresarial, deverá estar centrado no individuo e na organização, no seu “*corporate governance*”, ao mais alto nível da entidade. Esta evolução da Auditoria requer um acompanhamento das competências dos Auditores com conhecimentos técnicos e especializados mais aprofundados (formações técnicas, académicas, certificações, entre outras) mas cada vez mais, também, com conhecimentos mais abrangentes (gestão, comunicação, etc.), levando a um *improvement* das duas vertentes de competências fundamentais do auditor: as técnicas e as de gestão e comunicação.

Deste modo, a utilização destas tecnologias e metodologias, colocam à Auditoria e ao Auditor um desafio muito significativo, quer no que concerne à eficácia e eficiência do desempenho da função, quer na necessidade de incorporar novas competências, bem como na necessidade de alterar e potenciar novos métodos de trabalho, áreas de análise e monitorização permanente de fatores e vertentes fundamentais para o *core business* das organizações.

A importância de se preservar a integridade e a confiabilidade das informações geradas pelos processos corporativos da empresa, implica que o auditor interno deva estar habilitado a avaliar o nível de segurança das informações necessárias a todas as rotinas decisórias e propor ações que agreguem mais-valia aos novos processos corporativos. Para que essa tarefa possa ser realizada de forma eficaz, é necessário que a auditoria interna possua, além de uma visão sistémica da empresa, uma ação cada vez mais pró-ativa, o que aumenta a sua contribuição na realização dos desafios de hoje e na construção do caminho a percorrer amanhã. A auditoria interna, em função dos objetivos pretendidos, utiliza frequentemente as diferentes metodologias referidas:

- ✓ Auditoria baseada nos controlos (*Controls-Base Audit*) - Relativamente às diferentes áreas da organização com preocupação da *check list* do *Compliance* a ser elaborada face à regulamentação específica, visando garantir o cumprimento das normas aplicáveis.
- ✓ Auditoria baseada nos Processos (*Process-Base Audit*) – com a utilização de técnicas substantivas, de modo a que a entidade possa garantir ao nível dos seus principais processos a adoção das melhores práticas (*Benchmark*), permitindo uma mais-valia efetiva para o negócio, ao nível da eficácia e eficiência;
- ✓ Auditoria baseada no Risco (*Risk-Base Audit*) – com o objetivo de levar a efeito atuações direcionadas às áreas, processos e situações que relevam um risco mais significativo para o negócio. Baseando-se nos conceitos da gestão do risco empresarial (ERM) - como forma do Departamento de Auditoria Interna abordar os objetivos estratégicos e verificar da adequação dos procedimentos de gestão do risco implementados e das medidas em concreto decorrentes do seu funcionamento, de modo a permitir aos responsáveis da governação, auditores externos e aos detentores do capital terem uma segurança adicional de que o processo de gestão do risco empresarial é efetivo.

A abordagem de Auditoria Interna atualmente, está muito direcionada para a focalização no risco, daí que Castanheira e Rodrigues (2006 b:11) refira que “a atual orientação da Auditoria Interna aponta para uma abordagem baseada nos principais riscos do negócio, pelo que o planeamento de auditoria deverá estar alinhado com a estratégia da organização e o plano de negócio”.

A Auditoria Interna tem um papel importante na avaliação da eficácia da gestão de risco na organização. Deve avaliar com regularidade a eficácia dos controlos internos relativos à quantificação, informação e limitação dos riscos. A avaliação dos diferentes riscos ajudam a Auditoria Interna a definir o seu plano de trabalho, uma vez que lhe permite determinar quais são as áreas de maior risco, isto é, as áreas prioritárias e sobre as quais devem recair todas as atenções, portanto, as que devem ser analisadas primeiro.

De acordo com Cicco (2006), “a auditoria, identifica, avalia e prioriza os riscos para se focalizar nas áreas mais importantes a auditar. A avaliação de riscos permite ao auditor delinear um programa de auditoria capaz de testar os controlos mais importantes ou com maior nível de profundidade”.

Brasiliano (2003), afirma que “após a identificação e descrição dos processos e recursos operacionais, há a necessidade de verificar quais os riscos suscetíveis de afetar o desempenho dos mesmos. Para isso é necessário o conhecimento de cada tipo de risco, verificando qual o seu impacto para uma organização”.

Nesta fase é fundamental ter um bom conhecimento do setor de atividade em que a empresa opera, para assim ter uma maior capacidade de avaliar quais os riscos mais comuns para assim se verificar, com maior exatidão, quais são os que a afetam de fato a operacionalidade e continuidade da entidade. Pois conforme já foi referido, cada empresa tem uma forma diferente de reagir ao risco, mesmo que integrada no mesmo setor de atividade, daí a importância de conhecer bem os riscos antes de os tentar “combater” e mitigar.

Segundo o COSO (2004a), “a avaliação de riscos é uma responsabilidade da Administração, mas cabe à Auditoria Interna fazer uma avaliação própria dos riscos, confrontando-a com a avaliação feita pelos administradores”. Assistimos a uma mudança nos focos da auditoria, ou seja, deixou de se preocupar só com a análise de avaliação de controlos, para se preocupar também com a análise e avaliação do risco (financeiro, operacional, etc.), deste modo a Auditoria Interna gera mais valor para a empresa. Considera-se pertinente apresentar uma classificação de risco alternativa, ligada às consequências da sua ocorrência para a organização e não à “fonte” do risco. Trata-se da perspetiva de *Cruz* (2008) que elenca os riscos segundo três classes distintas, sendo elas:

- ✓ **Classe I** – Constituída pelos riscos que não afetam a economia da empresa. São os riscos que podem ser assumidos, isto é, a empresa ou entidade tem capacidade e está preparada para aceitar e assumir as consequências que esses riscos podem acarretar, pois neste caso serão imateriais;
- ✓ **Classe II** – Constituída pelos riscos que provocam dívidas ou a necessidade de reforço do capital social da empresa – Estes riscos podem ser assumidos apenas em algumas situações, pois nestes casos as suas consequências podem ser incomportáveis caso esses riscos se materializem, é considerado essencial promover uma adequada avaliação.
- ✓ **Classe III** – Constituída pelos riscos que podem conduzir à quebra, isto é, insolvência da empresa – No caso destes riscos se concretizarem as suas consequências serão incomportáveis para a empresa, será aconselhável a transferência, isto é, passar para uma seguradora a responsabilidade do risco em causa.

Após a identificação, classificação e análise dos riscos, será necessário avaliar cada um em termos da sua ocorrência potencial, e quais os seus impactos tanto Estratégicos e Operacionais como Financeiros. Esta avaliação far-se-á nos seguintes moldes:

Impacto – Alto, Médio ou Baixo

Probabilidade – Alta, Média ou Baixa

De referir que se considerou de extrema importância, nesta fase da análise e avaliação dos riscos, a divisão por classes sugerida por *Cruz (2008)*, feita de acordo com as consequências da ocorrência de cada risco. Através da análise do binómio Impacto/Probabilidade, será possível obter informações que darão um importante auxílio nas decisões a tomar relativamente à gestão desses mesmos riscos. Assim se destaca o fato de em cada quadrado da figura seguinte se poderem posicionar diversos tipos de risco aos quais uma determinada organização está sujeita, a título de exemplo - Impacto e Probabilidade de ocorrência baixa, corresponde a um risco baixo, situando-se este num dos quadrados com a cor verde.

A mesma análise poderá ser feita para diversos riscos sendo estes posicionados no quadrado correspondente, permitindo assim que seja feita uma rápida análise visual dos riscos que estão subjacentes à atividade de uma determinada empresa.

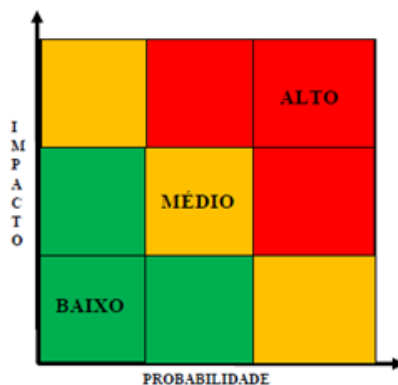


Figura 5 – Matriz de Risco – Impacto x Probabilidade
Fonte: Adaptado de Bezerra, Juliana

Fazendo uma análise crítica a esta matriz facilmente se deduz que para qualquer entidade os riscos a serem prioritariamente tratados serão os de impacto alto e probabilidade também alta. Isto porque o impacto terá grandes consequências para a empresa, podendo mesmo por em causa a sua continuidade, o que acrescido ao fato de ter também uma probabilidade de ocorrência alta o torna num dos riscos mais sensíveis para uma entidade, como tal deverá ser tratado delicada e eficazmente.

Contudo é de referir que todos os outros riscos, não apenas os de impacto e probabilidade alta, não deverão, de forma alguma, ser descurados por parte das entidades, pois representam também eles riscos e como tal deverão sempre ser acompanhados e monitorizados pelas empresas para assim estas não serem surpreendidas. A ISO 31000:2009 é a norma mundial lançada sobre gestão de riscos, que fornece princípios e diretrizes para a implementação eficaz da gestão de riscos nas organizações, encontrando-se alinhada com a visão integrada da gestão de risco empresarial (ERM). A norma pode ser aplicada em qualquer tipo de empresa, mas não é destinada para fins de certificação. Trata-se de uma norma abrangente e que tem como principal objetivo ajudar os responsáveis pelo desenvolvimento da política de gestão de riscos nas organizações a assegurar que os riscos são eficazmente geridos. Hoje em dia verificamos que cada área das empresas avalia os seus riscos, utilizando os meios que considera mais adequados, não existe uma gestão integrada do risco.

Deste modo, esta norma vem ajudar as organizações a desenvolver, programar e melhorar continuamente uma estrutura com a finalidade de integrar o processo de gestão de riscos no governo, na estratégia, na gestão, nos processos e na cultura de toda a organização. A norma inclui princípios de gestão e a importância do risco na consolidação da mesma. O risco é definido como o efeito da incerteza sobre os objetivos, e não apenas como um evento. Cada organização tem objetivos estratégicos, táticos e operacionais para alcançar e para isso vai ter de saber gerir o efeito da incerteza sobre os objetivos.

5. Sistema Financeiro

O sistema financeiro compreende o conjunto de instituições financeiras que asseguram, essencialmente, a canalização da poupança para o investimento nos mercados financeiros, através da compra e venda de produtos financeiros²⁵.

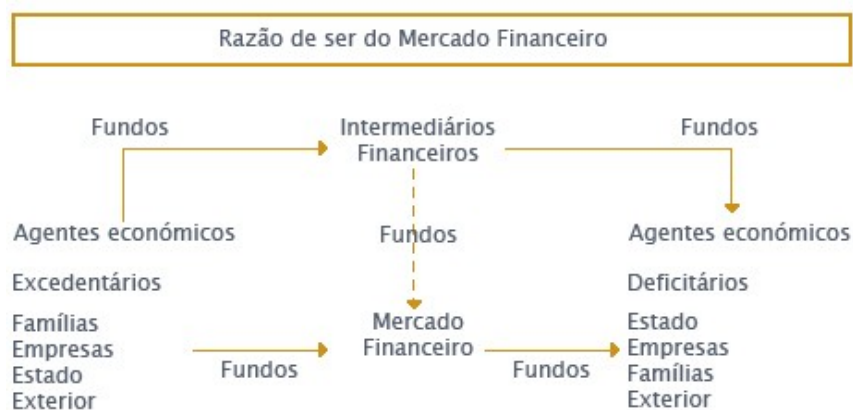


Figura 6 – Sistema Financeiro
Fonte: Associação Portuguesa Bancos (APB)

Estas instituições asseguram um papel de intermediação entre os agentes económicos que, num dado momento, se podem assumir como aforradores e, noutros momentos, como investidores. Para tal, os Bancos procedem à captação da poupança disponível em poder dos aforradores, pagando-lhe o respetivo juro, e depois canalizam-na para os investidores, recebendo destes um determinado rendimento.

²⁵ Associação Portuguesa Bancos (2011b)

A diferença entre o valor do juro cobrado na aplicação da poupança e o valor pago aos seus legítimos donos denomina-se de Margem Financeira. Na perspetiva empresarial, o montante que assume a margem financeira deve ser suficiente para fazer face às seguintes finalidades:

- ✓ Encargos de Funcionamento
- ✓ Risco e desgaste das imobilizações
- ✓ Tributação sobre os lucros
- ✓ Constituição de reservas
- ✓ Pagamento de dividendos aos acionistas

A inexistência de um sistema bancário bem estruturado não permitiria a circulação da moeda, sendo também mais difícil a criação de mercados de bens e serviços, bem como a circulação de pessoas e bens. Por outro lado podemos definir os agentes económicos intervenientes no processo como todos os indivíduos, instituições ou conjunto de instituições, que através das suas decisões e ações (tomadas racionalmente), intervêm num qualquer circuito económico. Apesar de terem funções diferenciadas no circuito económico, de produção, de consumo ou de investimento, estabelecem entre si relações económicas. Temos assim como agentes económicos, o Estado, as Famílias e as Empresas. Estes três agentes, em conjunto com as instituições financeiras, fazem parte de uma Economia Fechada. Contudo, e cada vez mais, deve considerar-se um quarto agente, O Exterior, com os quais os restantes agentes económicos nacionais estabelecem, num quadro de Economia Aberta, relações económicas intensas.

5.1 Sistema Financeiro Português

“O sistema bancário português engloba as instituições de crédito e empresas financeiras a operar em Portugal sob a supervisão do Banco de Portugal, o qual exerce funções de supervisão comportamental, regulando e fiscalizando a atuação das instituições de crédito na comercialização de produtos e serviços bancários, e é responsável pela promoção de ações e de iniciativas de informação e de formação nas áreas que assim o exigem” (Banco de Portugal, 2010).

Em Portugal, a estrutura do sistema financeiro é constituída basicamente pelos intermediários financeiros e outras instituições financeiras (Bancos, caixas agrícolas e outras instituições financeiras), pelos ativos e instrumentos financeiros (credito ao investimento, tesouraria e outros fins), pelos mercados (monetário, de capital e de divisas), pelos investidores finais e pelas entidades reguladoras e supervisoras (Ministério das Finanças, Banco de Portugal, Instituto de Seguros de Portugal e Comissão do Mercado de valores Mobiliários).

A atividade das instituições de crédito e das sociedades financeiras está definida no Decreto-lei nº 298/92, de 31 de Dezembro, designado por “Regime Geral das instituições de Credito e Sociedades Financeiras”, com varias alterações posteriores²⁶. O “Regime Geral das Instituições de Crédito e Sociedades Financeiras” (RGICSF) divide as entidades financeiras em dois grupos principais:

- ✓ Instituições de Crédito;
- ✓ Sociedades Financeiras.

O RGICSF classifica como Instituições de Crédito (IC):

- ✓ As empresas cuja atividade consiste em receber do público depósitos ou outros fundos reembolsáveis, a fim de os aplicarem por conta própria mediante a concessão de crédito;
- ✓ As empresas que tenham por objeto a emissão de meios de pagamento sob a forma de moeda eletrónica.

²⁶ Aprovado pelo Decreto-Lei nº 298/92, de 31 de Dezembro, Alterações: Decretos-Leis nº 246/95, de 14 de Setembro, nº 232/96, de 5 de Dezembro, nº 222/99, de 22 de Junho, nº 250/2000, de 13 de Outubro, nº 285/2001, de 3 de Novembro, nº 201/2002, de 26 de Setembro, nº 319/2002, de 28 de Dezembro, nº 252/2003, de 17 de Outubro, nº 145/2006, de 31 de Julho, nº 104/2007, de 3 de Abril, nº 357-A/2007, de 31 de Outubro, nº 1/2008, de 3 de Janeiro, nº 126/2008, de 21 de Julho, nº 211-A/2008, de 3 de Novembro, pela Lei nº 28/2009, de 19 de Junho, pelo Decreto-Lei nº 162/2009, de 20 de Julho, pela Lei nº 94/2009, de 1 de Setembro, pelos Decretos-Leis nº 317/2009, de 30 de Outubro, nº 52/2010, de 26 de Maio, nº 71/2010, de 18 de Junho e pela Lei nº 36/2010, de 2 de Setembro, pelo Decreto-Lei nº 140-A/2010, de 30 de Dezembro, pela Lei nº 46/2011, de 24 de Junho e pelo Decreto-Lei nº 88/2011, de 20 de Julho, 119/2011, de 26 de Dezembro, 31-A/2012, de 10 de Fevereiro, 242/2012, de 7 de Novembro, pela Lei nº 64/2012, de 24 de Dezembro e pelo Decreto-Lei nº 18/2013, de 6 Fevereiro.)

Instituições de Crédito	
Bancos	Instituições Financeiras de crédito
Caixas de Crédito Agrícola Mútuo	Instituições de Crédito Hipotecário
Caixa Central de Crédito Agrícola Mútuo	Sociedades de Investimento
Caixas Económicas	Sociedades de locação Financeira
Instituições Financeiras (criam moeda)	Sociedades de Factoring
	Sociedades Financeiras para Aquisição a crédito
	Sociedades de Garantia Mútua
	Instituições de Moeda Eletrónica

Quadro 1 – Instituições de Credito (Banco Portugal)

RGICSF classifica como Sociedades Financeiras, as empresas que não sejam instituições de crédito e cuja atividade principal consista em exercer uma ou mais das seguintes atividades:

- ✓ Operações de crédito, incluindo concessão de garantias e outros compromissos;
- ✓ Emissão e gestão de outros meios de pagamento;
- ✓ Transações, por conta própria ou da clientela, sobre instrumentos do mercado monetário e cambial, instrumentos financeiros a prazo, opções e operações sobre divisas, taxas de juro, mercadorias e valores mobiliários;
- ✓ Participações em emissões e colocações de valores mobiliários e prestação de serviços correlativos;
- ✓ Atuação nos mercados interbancários;
- ✓ Consultoria, guarda, administração e gestão de carteiras de valores mobiliários;
- ✓ Gestão e consultoria em gestão de outros patrimónios.

São Sociedades Financeiras, entre outras:

- ✓ As sociedades financeiras de corretagem;
- ✓ As sociedades corretoras;
- ✓ As sociedades mediadoras dos mercados monetário ou de câmbios;
- ✓ As sociedades gestoras de fundos de investimento;
- ✓ As sociedades gestoras de patrimónios;
- ✓ As sociedades de desenvolvimento regional;
- ✓ As agências de câmbios;
- ✓ As sociedades gestoras de fundos de titularização de créditos.

5.2 Modelo de Supervisão Português

Se a Supervisão tem o intuito de garantir a estabilidade e a solidez do sistema financeiro e a eficiência do seu funcionamento, a regulação pretende prevenir o risco sistémico, ou seja, a possibilidade de ocorrência de um evento não antecipado ou repentino que possa afetar o sistema financeiro como um todo.

O fato de existir um conjunto de normas e regulamentos implica o controlo da sua observância pelas instituições financeiras a elas sujeitas e, desta forma, garantir a confiança no sistema financeiro.

O Sistema Financeiro Português assenta num modelo de Supervisão Institucional com uma clara distinção entre os três segmentos de mercado existentes - o Bancário, o Financeiro e o Segurador.

O atual modelo de Supervisão do Sistema Financeiro Português está dividido da seguinte forma:

O Modelo de Supervisão Português			
Autoridade de Supervisão	Comissão do mercado de Valores Mobiliários	Banco de Portugal	Instituto de Seguros de Portugal
Âmbito de Supervisão	Mercado de valores mobiliários e instrumentos financeiros derivados de atividade dos que neles atuam	Instituições de crédito e Sociedades Financeiras	Atividade Seguradora e Resseguradora
Segmento de Mercado	Financeiro	Bancário	Segurador
	Supervisão Horizontal	Supervisão vertical	Supervisão vertical

Quadro 2 - O Modelo de Supervisão Português (BP)

O modelo de Supervisão do Sistema Financeiro Português atualmente em vigor encontra-se em fase de revisão, estando prevista a sua evolução para um modelo com apenas duas autoridades de supervisão – Modelo “*Twin Peaks*”, ou seja, a intenção de reforçar as competências do Banco de Portugal e criar um novo supervisor dedicado ao comportamento dos agentes nos mercados financeiros. Será assim substituído o atual modelo de tripartido de supervisão financeira - Banco de Portugal, CMVM e Instituto de Seguros de Portugal - por uma estrutura com apenas dois supervisores, conhecida por “*twin-peaks*”.

"O Banco de Portugal ficará encarregue de todas a supervisão prudencial das instituições e mercados financeiros, implicando a extensão das suas competências à supervisão prudencial na área dos seguros, resseguros e fundos de pensões, bem como na área da gestão de mercados e de sistemas de negociação"²⁷.

²⁷ Versão preliminar da proposta do Orçamento do Estado para 2010

No âmbito deste processo "será criada uma nova autoridade de supervisão, que substituirá as existentes, permitindo uma gestão mais eficiente dos recursos disponíveis, fomentando sinergias e eliminando sobreposições e redundâncias"²⁸. Este novo órgão ficará responsável pela supervisão comportamental, ou seja, o acompanhamento do comportamento de todos os agentes nos mercados financeiros, tendo em vista assegurar a proteção dos investidores e consumidores de produtos e serviços financeiros.

5.3 Banco de Portugal – Aviso nº 5/2008 de 25 de Junho

Com a entrada em vigor deste normativo, em 2008 (Aviso nº 5/2008 revogou o Aviso nº 3/2006), é exigido às Instituições Financeiras a existência de um sistema de controlo interno efetivo e são estabelecidos um conjunto de requisitos mínimos no SCI²⁹, de cumprimento imperativo. O Aviso nº 3/2006 apenas obrigava a entrega à entidade supervisora de um relatório anual com a descrição do SCI. Atualmente são exigidos relatórios com uma descrição clara e concisa dos desvios encontrados no SCI da instituição, por comparação com os requisitos obrigatórios da norma.

O Aviso nº 5/2008 do Banco de Portugal define três grandes objetivos para as instituições:

- ✓ Garantir a sua sustentabilidade a longo prazo, gerando níveis de rendibilidade suficientes – objetivo da rendibilidade;
- ✓ Manter sistemas de informação que permitam a tomada de decisões de forma fiável e consistente – objetivo da informação
- ✓ Cumprir em permanência as normas, as regras e os deveres aplicáveis à instituição – o objetivo de *compliance*.³⁰

²⁸ Proposta do Orçamento do Estado para 2010

²⁹ Sistema Controlo Interno

³⁰ Revista do Instituto de Formação Bancária, "Inforbanca" nº 90, de Out. – Dez. de 2011

Segundo o Aviso nº 5/2008 o objetivo do “*Compliance*” que está presente em todas as áreas / departamentos da instituição é o respeito pelas recomendações do Comité de Basileia, pelas recomendações da ABE³¹, pelos códigos de conduta, pelos códigos deontológicos profissionais, pelas disposições legais e regulamentares. Ao cumprir as referidas regulamentações, códigos, e condutas, a instituição diminui o risco de “sofrer” sanções ou de “destruir” a sua reputação. Pelo documento em análise constatamos que o “*compliance*” tem dois níveis de responsabilidade:

- ✓ O nível de implementação da função – cuja responsabilidade é do órgão de administração, segundo o art.º 18º do Aviso 5/2008.
- ✓ O nível da execução dos deveres correspondentes – este nível é da responsabilidade de todos funcionários, pois devem reger-se sempre, no exercício das suas funções, pelos respetivos códigos de conduta da instituição e dos códigos profissionais.

5.3.1 Objetivos da publicação do Aviso nº 5/2008

Este aviso tem dois objetivos. Primeiro a harmonização das normas e requisitos do SCI entre as entidades supervisoras em Portugal – O Banco de Portugal, a CMVM e o ISP³². O segundo objetivo é assegurar que as instituições supervisionadas cumprem as suas obrigações legais e que possuem uma gestão de riscos que garante a sua estabilidade financeira, assim como a estabilidade do sistema financeiro. O aviso do Banco de Portugal³³ reconhece as componentes fundamentais do SCI e define os requisitos obrigatórios a cumprir por cada componente, de forma a assegurar um SCI forte.

³¹ Associação Europeia de Bancos

³² Instituto de Seguros de Portugal

³³ Aviso nº 5/2008 de 25 de Junho – Banco de Portugal

O Aviso n.º 5/2008 do Banco de Portugal define o sistema (ou função) de gestão de riscos enquanto parte integrante do sistema de controlo interno das instituições financeiras, destinando-se a identificar, avaliar, acompanhar e controlar todos os riscos que possam influenciar a estratégia e os objetivos definidos pela instituição, assegurando o seu cumprimento bem como as ações necessárias para responder adequadamente a desvios não desejados, nomeadamente:

- ✓ Risco de crédito;
- ✓ Riscos de mercado (nos quais se inclui a gestão e controlo do risco de mercado, do risco de taxa de juro e do risco de taxa de câmbio);
- ✓ Risco de liquidez;
- ✓ Risco operacional (no qual se inclui a gestão e controlo do risco de sistemas de informação e o risco de *compliance*);
- ✓ Outros riscos (risco de estratégia, risco de reputação).

A política e a gestão de riscos devem desenvolver-se através de um modelo funcional de controlo transversal, cabendo a responsabilidade pelo seu governo ao Conselho de Administração, o qual delega na Comissão de Risco o acompanhamento, avaliação e controlo de cada tipo de risco.

A Comissão de Risco (se existir) é responsável por monitorizar os níveis globais de risco incorridos, assegurando que os mesmos são compatíveis com os objetivos e estratégias aprovados para o desenvolvimento da atividade.

Os objetivos de desempenho destinam-se não só a garantir a utilização eficaz dos ativos e recursos, mas também a assegurar a própria sobrevivência da instituição.

Para tal, é indispensável que os colaboradores da instituição trabalhem, em sintonia, para atingir os objetivos definidos pelos órgãos de administração e de gestão, colocando os interesses da instituição à frente dos seus próprios interesses ou dos interesses de terceiros (*v.g.*, fornecedores ou consumidores). Quanto aos objetivos de informação, estes destinam-se a garantir que as tomadas de decisão e processos de controlo, tanto a nível interno (órgãos de administração, de gestão e auditoria interna), como externo (investidores, autoridades de supervisão, auditores externos, acionistas), são executadas com base em elementos (por exemplo, relatórios e demonstrações financeiras) pertinentes, completos, fiáveis e tempestivos.

Por seu lado, os objetivos de "*compliance*" visam assegurar o cumprimento de todas as disposições legais e regulamentares aplicáveis, das normas profissionais e deontológicas e das regras internas e orientações dos órgãos sociais, de modo a proteger a reputação da instituição e a evitar a aplicação de penalidades e sanções.

5.4 Componentes do Controlo Interno

Para atingir eficazmente os objetivos anteriormente definidos, um sistema de controlo interno deve estar alicerçado, segundo o COSO³⁴, nos cinco componentes seguintes, interligados entre si:

- ✓ O **ambiente de controlo** da instituição, que reflete a atitude, a consciência e os atos dos órgãos de administração e de gestão e dos restantes colaboradores da instituição, relativamente aos objetivos definidos. Refletindo ainda a ênfase posta no controlo pelas políticas, procedimentos, métodos e estrutura organizativa, o ambiente de controlo constitui o suporte dos restantes componentes do sistema de controlo interno, estabelecendo a sua disciplina e a estrutura;
- ✓ O sistema de **avaliação de riscos**, destinado a identificar, analisar e gerir todos os riscos que possam influenciar a estratégia e os objetivos definidos pela instituição, bem como a adotar as ações necessárias para responder a desvios não desejados
- ✓ O sistema de **informação e comunicação**, instituído para garantir a captação, tratamento e troca de dados relevantes, abrangentes e consistentes, num tempo e numa forma que permita o desempenho eficaz e tempestivo das funções de administração, gestão e controlo da atividade e dos riscos da instituição;

³⁴ COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) publicou, em 1985, o relatório "*Internal Control - Integrated Framework*", que passou a constituir uma das principais referências em matéria de controlo interno

- ✓ As **atividades de controlo**, composto pelo conjunto de políticas e procedimentos implementados com vista a assegurar que os objetivos da instituição são atingidos e que são tomadas as ações necessárias para responder adequadamente aos riscos previamente identificados;
- ✓ Os processos de **monitorização de controlo**, executados com vista a assegurar a qualidade e eficácia do próprio sistema de controlo interno ao longo do tempo.



Figura 7: Componentes fundamentais do SCI
Fonte: COSO

5.4.1 Ambiente de Controlo

O ambiente de controlo é influenciado, designadamente, pelo padrão de valores éticos seguido pela instituição, pela exigência de níveis adequados de competência para os recursos humanos em função das responsabilidades atribuídas, pelo grau de transparência da estrutura organizativa e da sua adequação face à complexidade e dimensão da atividade da instituição, pela clareza da cadeia hierárquica e das responsabilidades e competências atribuídas a cada função, pela atitude face ao risco e pelo grau de envolvimento dos órgãos de administração e de gestão de topo na atividade.

Para garantir um ambiente de controlo sólido, a adoção de padrões elevados de ética e de integridade deve ser diretamente assumida pelos órgãos de administração e de gestão de topo e demonstrada através das suas ações, atitudes e palavras. Devem ser evitadas políticas ou práticas que possam inadvertidamente incentivar comportamentos inapropriados, tal como, por exemplo, a atribuição de prémios em função de objetivos de curto prazo que ignorem os riscos de longo prazo.

Os órgãos de administração e de gestão de topo devem, igualmente, enfatizar a importância dos controlos internos e envolver todos os colaboradores no processo de controlo, promovendo a comunicação de todos os problemas ocorridos na execução das operações, das falhas ou insuficiências detetadas no sistema de controlo, bem como das violações às regras internas e externas. O órgão de administração deve, também, assumir a responsabilidade pela aprovação e revisão periódica da estratégia global da instituição e de todas as políticas relevantes; conhecer e compreender os principais riscos incorridos na atividade desenvolvida, definir níveis aceitáveis para esses riscos e assegurar que são instituídos os mecanismos necessários para os identificar, medir, acompanhar e controlar; bem como aprovar a estrutura organizativa da instituição e assegurar que o sistema de controlo interno é objeto de avaliação contínua.

Por seu lado, o órgão de gestão de topo deverá assegurar a implementação da estratégia e das políticas aprovadas pela administração; desenvolver os mecanismos necessários para identificar, medir, acompanhar e controlar os riscos; promover a existência de uma estrutura organizativa com linhas de autoridade e reporte e um quadro de competências e responsabilidades, transparentes e objetivas; delegar as responsabilidades necessárias para a execução das operações; implementar as políticas e procedimentos de controlo internos adequados; e avaliar a eficácia do sistema de controlo interno.

O órgão de gestão de topo deve ainda assegurar que os recursos humanos da instituição possuem níveis de competência (conhecimentos, experiência e aptidão) elevados e adequados às funções a desempenhar e que são objeto de remuneração apropriada. Para o efeito, devem ser incentivadas as ações de formação regulares e promovidas políticas remunerativas que recompensem os comportamentos positivos e minimizem os incentivos para violar o sistema de controlo instituído.

5.4.2 Identificação e Avaliação de Riscos

Atendendo a que o negócio financeiro, independentemente da sua dimensão e natureza, implica a assunção natural de riscos, é fundamental que o sistema de controlo interno incorpore mecanismos que permitam identificar e medir todos os riscos que possam afetar de forma adversa os objetivos definidos pela instituição, em termos de impacto e probabilidade. De facto, a capacidade de uma instituição para identificar e avaliar os seus riscos condiciona o seu desempenho, a sua competitividade, a sua situação financeira, bem como a qualidade dos seus produtos e serviços. No entanto, a existência desta capacidade não pressupõe a eliminação total dos riscos, mas sim a sua aceitação consciente, dentro de limites predefinidos pela instituição.

Os procedimentos de identificação e avaliação deverão abranger todos os riscos emergentes da atividade desenvolvida pela instituição e ter em consideração tanto os fatores externos (incluindo, por exemplo, as alterações na conjuntura económica ou inovações tecnológicas) como os fatores internos (nomeadamente, a complexidade da estrutura organizativa, a natureza do negócio ou o grau de rotação do pessoal) que possa influenciar negativamente os objetivos estabelecidos.

De modo a manter a eficácia do sistema de controlo interno, o órgão de gestão de topo deve promover a introdução contínua dos ajustamentos necessários para acomodar eventuais alterações nos fatores internos e externos que influenciem o processo de medição e avaliação de riscos e abranger os riscos gerados pela introdução de novos produtos ou pelo desenvolvimento de novas áreas de negócio.

5.4.3 Informação e Comunicação

A qualidade da informação sobre a atividade e os riscos existentes, bem como sobre a evolução de condicionantes externos que sejam pertinentes para a tomada de decisão e para a realização do controlo, afeta a capacidade da instituição para agir adequada e tempestivamente.

Como tal, o sistema de controlo interno deve garantir a existência de informação substantiva, atual, compreensível, consistente, tempestiva e fiável, que abranja toda a atividade da instituição (incluindo dados financeiros, operacionais e de "compliance") e

dados sobre o comportamento e evolução de mercado relevante. Para o efeito, é fundamental que seja criado e mantido um sistema contabilístico que registe, classifique, associe e archive, tempestivamente e de forma sistematizada e consistente, todas as operações realizadas pela instituição.

Para garantir que a informação chega ao seu destinatário, a instituição deve estabelecer canais e formatos (relatórios, memorandos, atas, etc.) de comunicação, formais e transparentes. A própria estrutura organizativa deve promover o fluxo vertical e horizontal da informação e clarificar quais os deveres e responsabilidades de cada colaborador no processo de informação e comunicação.

5.4.4 Atividades de Controlo

Para garantir que os objetivos da instituição são atingidos e que são tomadas as ações necessárias para responder adequadamente aos riscos previamente identificados é essencial que sejam definidas políticas e procedimentos, que sistematizem, de forma clara e objetiva, o que fazer e como fazer.

Estas políticas e procedimentos devem ser definidos pelo órgão de gestão de topo e aprovados pelo órgão de administração, encontrar-se reduzidos a escrito e ser devidamente divulgados a todos os colaboradores da instituição.

Os procedimentos de controlo podem ser agrupados em duas categorias: de prevenção ou de deteção. Os primeiros consistem em mecanismos destinados a evitar a ocorrência de situações não desejadas ou não autorizadas, enquanto os segundos visam permitir a identificação destas situações quando, não obstante os procedimentos de prevenção, ocorram de facto, de modo a permitir a adoção imediata de medidas corretivas. Entre os procedimentos de controlo mais comuns encontram-se os seguintes:

- ✓ Exigência de recolha e manutenção de evidências que documentem de forma substantiva as decisões tomadas e as operações realizadas, num formato que seja facilmente acessível e se encontre devidamente sistematizado por ordem cronológica;

- ✓ A definição de formulários estandardizados e tipificação clara e objetiva de todos os elementos necessários para o processamento das operações;
- ✓ Definição de requisitos para aprovar e autorizar as operações, devidamente ajustados ao risco existente, com a identificação clara das condições que devem ser previamente verificadas e a atribuição de competências inequívocas para a aprovação e autorização;
- ✓ Existência de um grau de segregação das funções que envolvam responsabilidades conflitantes, nomeadamente, nas operações de crédito e de mercado, entre a autorização, a execução, o registo, a guarda de valores e outra documentação e o respetivo controlo;
- ✓ Imposição de restrições no acesso a ativos e recursos e à informação, através de barreiras físicas ou informáticas;
- ✓ Criação de obrigações de reporte, quer através da elaboração de relatórios de evolução da atividade e dos riscos, como de relatos com os principais desvios, erros, fraudes, incumprimentos e outras situações de exceção;
- ✓ Definição de limites objetivos e prudentes para cada um dos riscos incorridos na atividade desenvolvida;
- ✓ Realização de verificações e reconciliações periódicas, devidamente consubstanciadas, à exatidão, autenticidade e validade das operações registadas.

5.4.5 Processo de Monitorização de Controlo

O processo de monitorização de controlo compreende todas as ações desenvolvidas pela instituição de modo a garantir a eficácia e qualidade do sistema de controlo interno. Estas ações devem ser desenvolvidas de forma contínua e como parte das tarefas diárias da instituição, devendo incluir avaliações autónomas e periódicas a realizar pelo órgão de auditoria interna.

Todos os colaboradores da instituição devem participar nas ações de controlo, nomeadamente através da execução de procedimentos de revisão das tarefas executadas, previamente à sua formalização ou transmissão a terceiros, e da comunicação de todas as irregularidades e falhas de que tomem conhecimento. Por seu lado, os órgãos de gestão intermédia devem desenvolver ações de controlo sobre as áreas da sua responsabilidade, verificando se os colaboradores desempenham adequadamente as responsabilidades que lhe estão atribuídas, analisando eventuais desvios face aos objetivos estabelecidos, mantendo um ambiente e controlo e canais de comunicação apropriados e suficientes e assegurando que os riscos se encontram devidamente identificados.

As ações de controlo devem ser também realizadas pelos órgãos de gestão de topo, ainda que focalizadas nas áreas de negócio principais e na evolução dos objetivos globais da instituição, bem como nas alterações internas e externas que possam comprometer a execução do plano estratégico aprovado.

Para garantir a eficácia e qualidade das avaliações efetuadas ao sistema de controlo interno, a instituição deve dotar-se de um órgão de auditoria interna independente, que reporte diretamente ao órgão de administração e ao órgão de gestão de topo, dotado de recursos materiais e financeiros suficientes e constituído por pessoal com níveis de experiência, formação e competência adequados. Todas as deficiências ou insuficiências detetadas no âmbito das ações de controlo ao sistema de controlo interno devem ser objeto de reporte imediato ao órgão adequado, de modo a possibilitar a adoção tempestiva de medidas corretivas. Periodicamente, devem ainda ser reportados aos órgãos de administração e de gestão de topo relatórios com a síntese dos principais aspetos detetados nas ações de controlo, os quais, ainda que sejam imateriais quando considerados isoladamente, podem evidenciar tendências de deterioração do sistema de controlo interno.

5.5 Categorias de Controlo

Para avaliar a qualidade e abrangência dos controlos da entidade supervisionada, o MAR³⁵ define três categorias (organização, gestão e controlos específicos do risco), cada uma composta por diversas rubricas de referência, que no seu conjunto

³⁵ Modelo de Avaliação Riscos – Banco de Portugal – Supervisão bancária, 2007

incorporam os cinco componentes do sistema de controlo interno referidos anteriormente. As categorias referentes à organização e à gestão avaliam três das referidas componentes: o ambiente de controlo da instituição, o sistema de informação e comunicação e o processo de monitorização de controlo. Estas categorias agregam os mecanismos de controlo com uma natureza transversal a toda a instituição, que funcionam como mitigadores gerais para o conjunto de riscos intrínsecos à atividade desenvolvida por cada área funcional e não apenas de uma categoria de risco em particular. Enquanto a categoria referente à organização concentra os aspetos de carácter mais formal e objetivos (a estrutura organizativa, a estrutura de reporte, as relações entre áreas funcionais, o sistema de informação de gestão e o processo de auditoria), a categoria referente à gestão abarca os aspetos mais qualitativos e que implicam um maior grau de subjetividade no juízo de valor a exercer pelo supervisor (estrutura e qualidade da gestão, processo de decisão e de planeamento estratégico e a atitude face ao risco). A categoria dos controlos específicos do risco avalia o restante componente do controlo interno, ou seja, os aspetos referentes à identificação e avaliação dos riscos e os processos de controlo. A análise autónoma destas componentes destina-se a isolar os procedimentos específicos desenvolvidos pela instituição para identificar, avaliar, acompanhar e controlar cada um dos riscos, de modo a concluir sobre o seu efeito mitigador ao nível de cada categoria de risco intrínseco.

Os controlos específicos dos riscos compreendem o conjunto de políticas, sistemas, procedimentos, métodos e práticas implementados e utilizados pela instituição com vista a identificar, avaliar, acompanhar e controlar, adequada e tempestivamente, cada um dos riscos intrínsecos à atividade desenvolvida em particular.

Para atribuir uma notação aos controlos específicos, o supervisor deverá avaliar a qualidade dos processos de (i) identificação, (ii) avaliação, (iii) acompanhamento (iv) e controlo, existentes para cada categoria de risco.

(I) Identificação

Determinar a qualidade do processo de identificação dos fatores, internos e externos, que, em relação a cada categoria de risco, que possam afetar a capacidade da instituição para implementar a sua estratégia ou atingir os objetivos definidos.

(II) Avaliação

Analisar a qualidade do processo de avaliação/medição da probabilidade de ocorrência de perdas e da respetiva magnitude, em relação a cada categoria de risco.

(III) Acompanhamento

Verificar a qualidade do processo de acompanhamento da exposição a cada categoria de risco.

(IV) Controlo

Avaliar a qualidade do processo de mitigação dos níveis de exposição ao risco, nomeadamente face a determinados limites instituídos, bem como do próprio processo de controlo do risco, tal como aqui descrito.

5.6 Categorias de Riscos

Ao longo das décadas, os lucros associados à indústria bancária têm sido comprometidos por inúmeros fatores, sendo que, comparativamente a outras entidades de caráter financeiro, os bancos continuam sujeitos a um elevado nível de regulamentação, precisamente, pelas suas atividades. Para além disso, os bancos têm vindo a assumir novas atividades, no que diz respeito, por exemplo, ao leque de oferta e à sua área de atuação e, conseqüentemente, novos riscos.

Na década de 70, por exemplo, os países menos desenvolvidos representavam um potencial mercado de atuação para a atividade bancária, no entanto, existia risco inerente à exploração desses mercados.

“O conceito de risco de desagregação, isto é, divisão do risco nas suas componentes específicas, provocou alterações nos métodos através dos quais os bancos medem, assumem e administram os riscos inerentes às suas atividades” (Lastra, 2000).

“Os bancos sólidos e seguros baseiam-se primeiro, sobre uma boa administração do risco e, em segundo lugar, sobre um bom controlo do risco por reguladores e por entidades reguladoras. Os bancos enfrentam problemas particulares associados ao efeito sistémico do risco, uma vez que qualquer risco pode crescer em proporções

sistémicas, quando o seu impacto tem implicações para além da instituição individual, afetando ou ameaçando afetar outras instituições e, eventualmente, a própria economia” (Lastra, 2000). As categorias de riscos identificadas pelo Banco de Portugal no Aviso nº 5/2008 baseiam-se no Modelo de Avaliação de Riscos (MAR), As categorias de riscos, cuja gestão deve cumprir um conjunto de requisitos obrigatórios, podem ser sistematizadas de acordo com as respetivas especificidades, ou seja:

- 1) Riscos financeiros, intrínsecos ao negócio bancário, que sempre foram e são geridos pelas instituições bancárias, como, por exemplo: o risco de crédito, o risco de mercado, o risco de taxa de juro, o risco de taxa de câmbio e o risco de liquidez;
- 2) Riscos de outras naturezas, que apesar de “recentes” são riscos muito debatidos a nível internacional e nacional, são exemplos desta categoria o risco de *compliance*, o risco operacional e o risco de sistemas de informação;
- 3) Riscos de natureza transversal que são:
 - ✓ Risco de estratégia – surge devido a decisões estratégicas inadequadas, ou da sua deficiente implementação, ou ainda da incapacidade de resposta a alterações no meio envolvente ou no ambiente de negócios da instituição;
 - ✓ Risco de reputação – surge devido a uma perceção negativa sobre a imagem pública da instituição, fundamentada ou não, por clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral.

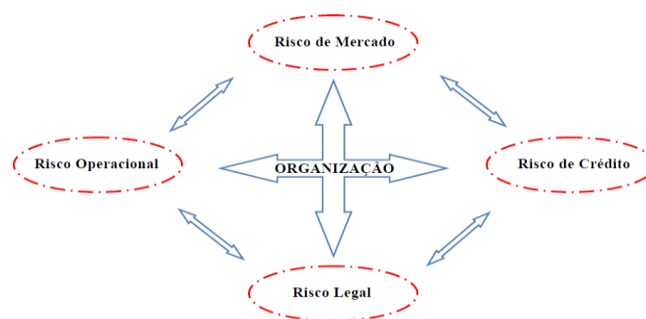


Figura 8 – Risco - Definições, Tipos, Medição e Recomendações para a sua gestão
Fonte: Adaptado – JÚNIOR, António Marcos Duarte

5.7 Gestão Risco Operacional nas Instituições Financeiras

O papel da gestão de risco nas instituições financeiras evoluiu muito para além da simples mitigação dos riscos identificados, caminhando para uma disciplina que concentra modelos financeiros e econométricos complexos. Buchelt e Unteregger (2004) argumentam que, “muito antes do advento do Acordo Basileia II, as instituições financeiras já tinham posto em prática vários mecanismos e procedimentos de controlo, defendendo que a gestão de risco operacional é mais antiga do que a gestão de risco de crédito ao mercado”.

No entanto, continua a ser uma realidade que a gestão de risco operacional tem sido um conjunto de atividades fragmentadas, desenhadas para lidar com uma vasta variedade de riscos operacionais. Uma vez que o conceito de risco operacional era desconhecido até há aproximadamente dez anos atrás – o termo “risco operacional” recebeu o reconhecimento geral em 1995, após a famosa falência do Banco Barings – não se afigura surpreendente que a gestão de risco operacional não perfaça ainda um processo integrado como o é no caso do risco de crédito ou de mercado. As áreas de risco de mercado e de crédito são alvo de análises sofisticadas desde há vários anos por parte das instituições financeiras, mas estas só recentemente se aperceberam da importância do risco operacional.

O risco operacional não constitui novidade: é o mais antigo risco que as instituições financeiras enfrentam. Apesar da sua constante presença em todas as actividades de uma instituição financeira, têm sido as áreas de risco de mercado e de crédito os alvos principais de análises sofisticadas e robustas desde há vários anos.

“Só recentemente as instituições financeiras se aperceberam da relevância do risco operacional” (Bessis 2002). “Razões como a sua difícil identificação e medição e a ausência da devida atenção por parte do mercado e reguladores concorreram para que o foco na sua análise e gestão tenha sido negligenciado até ao final da década de 90. No entanto, vários determinantes vêm contribuindo para a crescente importância concedida ao risco operacional” (Geiger 2000):

- a) A perceção do crescimento do impacto dos riscos operacionais,
- b) A constatação da insuficiência do recurso a abordagens somente quantitativas de risco de crédito e de mercado para captar alguns tipos de risco e o reconhecimento de que a gestão de risco operacional deve ser uma disciplina por direito,
- c) A inclusão dos riscos operacionais nas metodologias de gestão global de risco
- d) O interesse crescente das entidades reguladoras pelo risco operacional ao nível dos requisitos de capital e da sua gestão.

O risco operacional pode ser definido como o risco resultante da materialização de uma vasta diversidade de eventos, incluindo fraude, roubo, perda de membros-chave da equipa, processos judiciais, perda de informação, terrorismo, vandalismo e desastres naturais.

O surgimento constante de escândalos financeiros (e.g. *Enron*, *Parmalat* e *Société Générale*), sem esquecer o facto de as perdas resultantes de eventos operacionais se encontrarem na base dos mais espetaculares falhanços empresariais (*Barings*, *Long Capital Management*), levam a que o risco operacional tenha vindo a receber progressivamente mais atenção por parte da comunicação social, de reguladores e gestores executivos.

“Para fazer face a esta realidade, as entidades reguladoras têm investido em apresentar novas normas e regras das quais são exemplos os Acordos Basileia II e Solvência II, visando, respetivamente, a área da banca e a área seguradora”. (Saidenberg et al. 2003).

Jobst (2007) aponta a desregulamentação dos mercados financeiros, a crescente complexidade da indústria financeira, as grandes fusões e aquisições e o recurso massivo a contratos de *outsourcing* como fatores preponderantes para o aumento da exposição das atividades das instituições financeiras ao risco operacional.

Também a tendência para uma maior dependência tecnológica, a maior intensidade na concorrência e a globalização dos mercados, todos estes fatores têm vindo a deixar as empresas mundiais mais expostas do que nunca ao risco operacional.

Numa referência particular à indústria financeira, Buchelt e Unteregger (2004) argumentam que o “risco de fraude e os eventos externos sempre estiveram presentes ao longo da história, mas foi o progresso da tecnologia que elevou o potencial do risco operacional” – os avanços tecnológicos fomentam a rápida inovação financeira e a proliferação de produtos financeiros fortemente dependentes de serviços e sistemas bastante expostos a risco operacional, como é o caso do *e-banking*.

As instituições financeiras têm vindo a tomar consciência de que o risco operacional está presente em toda a sua atividade e de que a gestão deste risco deve ser abordada com o mesmo nível de importância que é dado ao risco de crédito ou ao risco de mercado.

A elevada atenção depositada, por parte dos reguladores, no risco operacional pode ser atribuída à mudança no perfil desse risco no setor de serviços financeiros, resultante de fatores como o crescimento do comércio eletrónico, a crescente dependência tecnológica deste setor, o desenvolvimento de novos produtos e serviços de elevada complexidade e o emergente carácter global dos mercados.

Todavia, foram alguns dos eventos de risco operacional já mencionados que puseram em causa a firmeza do sistema financeiro, motivando os reguladores para reforçar fortemente a supervisão sobre o risco operacional – o Comité de Basileia de Supervisão Bancária expressou, em 1999, a sua visão de que o risco operacional é “suficientemente importante para os bancos lhe dedicarem os recursos suficientes à sua quantificação”.

Também as empresas de *Rating*, como a *Moody's Investor Service* (*Moody's Analytical Framework for Operational Risk Management of Banks, 2003*) e a *Fitch Ratings* (*Operational Risk Management & Basel II implementation: Survey Results, 2004*), publicaram entre 2003 e 2004 relatórios acerca do papel da gestão de risco operacional nas empresas de serviços financeiros e do risco operacional no cálculo de *Ratings* corporativos.

Estes relatórios indicavam linhas orientadoras do que seria necessário, ao nível da sua governação e dos sistemas de informação, para que uma instituição financeira pudesse ser bem avaliada na vertente de gestão de risco operacional, tais como, a capacidade de avaliação de riscos e controlos.

Apesar de Lewis e Lantsman (2005) descreverem o risco operacional como idiossincrático, uma vez que “o risco de perda tende a ser não correlacionado com as forças gerais do mercado” – ou seja, quando uma empresa é atingida por risco

operacional, este não se dissemina para outras empresas – esta visão de idiosincrasia do risco operacional é pouco sustentável porque implica que, sempre que um banco incorre numa perda por um incumprimento num crédito, ou por flutuações de mercado, a sua capacidade para fazer face às suas obrigações com outros bancos é afetada; não será o caso quando um banco incorre em perdas resultantes de atividades não autorizadas ou fraude. Contudo, em certos tipos de riscos operacionais, como a fraude, existe uma clara tendência para uma situação de contágio em que a partilha ou não partilha de informação entre instituições pode reduzir, ou, pelo contrário, elevar o risco operacional a que cada instituição está exposta.

“É justo preconizar que tanto a prática como a ciência continuam à procura de um método eficiente para medir, controlar e gerir o risco operacional em instituições financeiras” (Saidenberg & Schuermann 2003).

Quer a indústria financeira, quer os investigadores serão agora e no futuro, confrontados com a necessidade de desenhar modelos e sistemas de informação que respondam à dinâmica e à complexidade, cada vez maiores, das diferentes atividades em que as instituições vão estar envolvidas (Brink 2002). Esta evolução dos sistemas de informação irá passar não só pela melhoria e automatização de muitas das tarefas dos atuais sistemas, mas também por aspetos como a integração com outras aplicações e a expansão das funcionalidades a novas áreas, tornando a gestão de risco operacional num vetor fundamental na gestão diária das instituições, bem como nos seus processos de tomada de decisão.



Figura 9 - Estado de maturação da investigação na área de risco
Fonte: Raft survey: Emerging Trends in Operational Risk 2002)

Não sendo consensual o conceito sobre risco operacional entre académicos e profissionais, bem como as suas causas, consequências, características e gestão, o mesmo existe na opinião da sua diversidade e difícil quantificação. A mais usual das definições de risco operacional foi apresentada, pela primeira vez, por Morris et al. (1999), que o interpretaram como “a perda direta ou indireta resultante de processos internos inadequados, falhas, pessoas, sistemas, ou de eventos externos”. Inicialmente, o Comité de Basileia adotou esta definição, mas a referência a perdas indiretas foi subsequentemente eliminada devido ao pressuposto da quantificação de capital regulamentar, já que estas perdas apresentam obstáculos à sua medição.

Assim, o Acordo de Basileia II definiu risco operacional como “o risco resultante de processos internos inadequados, falhas, pessoas, sistemas, ou de eventos externos”. Esta definição, que se baseia nas causas subjacentes (fontes) de risco operacional, inclui o risco legal, mas exclui os riscos de negócio e reputação. Em 2005, Vinella e Jin avançaram com uma nova descrição de risco operacional, nomeadamente “o risco de a operação vir a falhar um, ou mais objetivos de performance operacional, quer esta seja pessoas, tecnologia, processos, informação, ou a infraestrutura que suporta as atividades de negócio”.

Analisando todas as definições e tipos de risco operacional, somos persuadidos a concordar que a sua característica principal é a multidiversidade. Esta diversidade torna difícil limitar o número de dimensões de análise e metodologias de gestão. Qualquer que seja a metodologia utilizada para a gestão de risco operacional, existem três dimensões fundamentais que caracterizam qualquer fenómeno de risco operacional:

- ✓ A causa ou fonte (os fatores de risco que provocam, ou podem potenciar, a ocorrência de determinado evento),
- ✓ O tipo de risco (as características do risco associado ao evento),
- ✓ A consequência (os impactos resultantes para a instituição da ocorrência do evento).

Segundo Wahler (2002), enquanto os eventos de risco de mercado ou de crédito são influenciados por transações e parceiros de negócio da instituição, o risco operacional deriva de três fontes genéricas internas e externas, a saber,

- ✓ Mudança: causas externas e internas que influenciam a estratégia da instituição;
- ✓ Complexidade: em produtos, processos e tecnologia;
- ✓ Complacência: gestão ineficiente do negócio e do seu risco.

Diferentes categorias de risco foram já apresentadas para classificar eventos de risco operacional, das quais se têm destacado a apresentada pelo Comité de Basileia II para a banca e a proposta pelo COBIT (*Control Objectives for Information and Related Technology*) para a área das tecnologias de informação. É, no entanto, de realçar que, na sua maioria, as instituições financeiras têm desenvolvido os seus próprios catálogos de riscos para classificação dos seus eventos, mesmo que tal exija mapear os seus tipos de riscos para os catálogos de riscos do supervisor.

A terceira dimensão é a consequência, ou seja, o impacto financeiro, ou não financeiro, que a instituição pode ter de enfrentar. Kingsley et al. (1998) identificaram três tipos de impacto que podem resultar de eventos de risco operacional:

- ✓ Perdas financeiras diretas como, por exemplo, perdas relativas a fraude ou a coimas;
- ✓ Perdas financeiras indiretas, tais como perdas relativas a má reputação ou à necessidade de alocação de mais recursos a certas atividades,
- ✓ Redução de proveitos devido à falta de operacionalidade de fazer negócio, do qual constituem exemplos as perdas de receita por causa da incapacidade da instituição em responder aos requisitos dos clientes.

Na análise da dimensão “consequência”, emerge um determinante fundamental que é necessário estudar – *A Mitigação*. A existência ou não de mecanismos de mitigação desempenha uma influência significativa sobre o real impacto para a instituição de um determinado risco. Kaiser e Kohne (2006) argumentam que a característica mais endógena do risco operacional em relação aos riscos de mercado ou crédito significa que as oportunidades de mitigação de risco são frequentemente maiores no caso do risco operacional.

A utilização das medidas de mitigação para redução de impactos, sem esquecer os custos associados à sua implementação ou manutenção, deverão ser consideradas no cálculo da taxa de retorno da instituição. Em muitas instituições, o papel da gestão de risco operacional nunca esteve bem definido. Na falta de objetivos tangíveis, esta área acolhia um conjunto de atividades estanques, desenhadas para responder a supervisores, empresas de *Rating* e requisitos de auditoria.

A nova regulamentação (e.g. Basileia II, Solvência II, SOX) veio ajudar a criar um espaço próprio para a gestão de risco operacional nas instituições financeiras através de criação de novas estruturas orgânicas, ou do desenvolvimento, em estruturas existentes, de novas funções dedicadas a este risco. Apesar dos fortes investimentos realizados, muitas instituições não estão impressionadas com os resultados obtidos pela gestão de risco operacional, não só porque muitos dos procedimentos que são realizados por estas novas estruturas se assemelham muito aos que eram normalmente efetuados pela Auditoria Interna ou pelo *Compliance*, mas também por requererem um conjunto de atividades que exigem numerosos recursos das unidades de negócio, sem que pareçam produzir, contudo, outros benefícios para a instituição, para lá de esta poder afirmar que está de acordo com as normas do supervisor. No entanto, a existência de um programa corporativo de gestão de risco operacional pode proporcionar, a uma instituição, atingir objetivos que lhe faculte incrementar aspetos estratégicos da sua atividade

5.8 Regulamentação para a gestão de risco operacional

Atualmente já existe um conjunto de regulamentação que “conduz” as instituições financeiras para uma melhor gestão do risco operacional. Muita desta regulamentação foi essencialmente produzida para proteger o sistema financeiro e os investidores de perturbações no sistema que pudessem, de alguma forma, colocar em risco, não só as próprias instituições em que o risco surgisse, mas também todo o sistema no qual se encontram integradas. No âmbito deste trabalho, são apresentadas três destas estruturas regulamentares, a saber, o Acordo Basileia II para instituições bancárias, o Acordo Solvência II para a indústria seguradora e o decreto *Sarbanes-Oxley*, desenvolvido nos Estados Unidos da América, a cujos requisitos algumas empresas em Portugal decidiram responder.

5.8.1 Decreto-lei nº298/92 de 31 de Dezembro

O Banco de Portugal exerce a função de supervisão – prudencial e comportamental – das instituições de crédito, das sociedades financeiras e das instituições de pagamento, tendo em vista assegurar a estabilidade, eficiência e solidez do sistema financeiro, o cumprimento de regras de conduta e de prestação de informação aos clientes bancários, bem como garantir a segurança dos depósitos e dos depositantes e a proteção dos interesses dos clientes. As instituições sujeitas a supervisão do Banco de Portugal devem observar regras prudenciais, que visam o controlo dos riscos inerentes às suas atividades. Pretende-se por um lado, garantir a solvabilidade e solidez financeira dessas instituições e por essa via, a manutenção da estabilidade (e da confiança na estabilidade) do sistema financeiro; por outro lado, visa-se a proteção dos utilizadores (depositantes, investidores) contra perdas resultantes de má gestão, fraudes ou falência dos fornecedores/prestadores de serviços financeiros.

5.8.2 Acordos Basileia

Os acordos de Basileia (I, II e III) consistem num conjunto de recomendações de supervisão prudencial aplicadas ao setor financeiro em geral e ao bancário em especial. O acordo de Basileia I tinha um padrão único de apurar o capital regulamentar mínimo, apresentava um único pilar, relativo ao requisito mínimo de capital o que permitiu a simplificação da implementação e da comparação dos resultados entre as instituições financeiras.

Carneiro et al. (2004:5) e Silva (2008:1) referem que no Acordo de Basileia I são recomendados, aos países que estavam “representados pelos supervisores dos bancos centrais ou pelas autoridades com responsabilidades pela supervisão, padrões mínimos de requisitos de capital devido ao nível de descapitalização dos bancos nos anos 80. Em 1988, o Comité introduz regras de cálculo de capital regulamentar, exigindo que o capital mínimo passe a ser de 8% até ao final de 1992. Este Acordo, adotado pelos membros e por outros 100 países, conduziu à ponderação dos ativos de acordo com o risco de incumprimento das obrigações da contraparte, ou seja, o risco de crédito. Exige também, as melhores práticas e *standards* de supervisão, cabendo às autoridades dos países membros a sua implementação”.

Entre as lacunas de Basileia I, são de destacar a pouca sensibilidade ao risco e o estímulo da avaliação de capital regulamentar. A revisão da versão inicial do Acordo de Capital (de 1988) – e respetivas emendas entretanto incorporadas (a última das quais relativa aos riscos de mercado, em Janeiro de 1996) – teve início em 1999 e encontra-se expressa no documento do Comité de Supervisão Bancária de Basileia, publicado em Junho de 2004 e codificado em Julho de 2006, intitulado “*International Convergence of Capital Measurement and Capital Standards*”. Esse documento é mais conhecido por “Basileia II”

Na reformulação do Acordo de Capital, além dos objetivos basilares da suficiência de fundos próprios e neutralidade competitiva, foram fixados os seguintes propósitos:

- ✓ Assegurar maior sensibilidade dos requisitos de capital ao perfil de risco das instituições, através do reconhecimento para efeitos regulamentares, e desde que cumpridas determinadas condições, dos sistemas de gestão e as medidas de risco das instituições e da autonomização do risco operacional;
- ✓ Alargar o regime de fundos próprios, não o limitando à fixação de rácios regulamentares mínimos, de modo a reconhecer a relevância da atuação das autoridades de supervisão e da disciplina de mercado.
- ✓ Difundir as “melhores práticas” no sistema financeiro, desenvolvendo um conjunto de incentivos que premeia a capacidade das instituições em mensurar e gerir o risco. Com efeito, as novas regras serão, em princípio, indutoras de alterações na forma como as instituições mensuram e gerem os riscos, o que provocará, inevitavelmente, adaptações nas estruturas organizativas, processos internos e na própria cultura das instituições.

O regime de adequação de capital proposto em “Basileia II” foi acolhido na ordem jurídica comunitária com a publicação das Diretivas 2006/48/CE e 2006/49/CE, de 14 de Junho de 2006, que vieram alterar as Diretivas 2000/12/CE e 93/6/CE, respetivamente. O pacote regulamentar constituído pelas versões reformuladas das duas Diretivas é habitualmente designado por “*Capital Requirements Directive*” (CRD). O risco operacional perfaz uma parte fundamental dos processos de negócio dos bancos e não pode ser completamente eliminado – é interesse comum de bancos e supervisores que este risco seja identificado, medido e controlado. Com esse objetivo, o Acordo Basileia II introduz o tratamento do risco operacional – os bancos irão ter de reter capital regulamentar para este risco, assente em três pilares:

- ✓ (Pilar I); Determinação dos requisitos mínimos de fundos próprios - observar os requisitos de gestão definidos pelas entidades supervisoras
- ✓ (Pilar II) Processo de avaliação pela autoridade de supervisão - apresentar relatórios relativos aos seus níveis de exposição, capital alocado e políticas de gestão de risco
- ✓ (Pilar III) Disciplina de Mercado - Visa-se a suficiência e transparência na divulgação de informação pelas instituições em diferentes mercados, com o objetivo de assegurar uma efetiva disciplina de mercado

O Acordo de Basileia II aborda, pela primeira vez, a questão do risco operacional, sendo o único tipo de risco a receber uma definição regulamentar oficial por parte do Comité de Basileia (o risco de mercado e o risco de crédito não têm definições oficiais), o que parece indicar o reconhecimento da complexidade, e porventura algum desconhecimento, dos conceitos e das metodologias associadas a este tema.

Assim, Basileia II define o risco operacional como “o risco resultante de processos internos inadequados, de falhas, pessoas e sistemas, ou de eventos externos”. Esta definição inclui risco legal, mas exclui risco estratégico e de reputação.

Em Dezembro de 2010, o Comité de Basileia de Supervisão Bancária (BCBS) publicou o designado “Acordo de Basileia III”, que integra alterações regulamentares extremamente importantes nos seguintes domínios: capital, liquidez e rácio de alavancagem, as quais serão aplicadas, de modo faseado, a partir de 2013, alterando nomeadamente o Pilar I do anterior acordo (Basileia II). Estas alterações regulamentares irão ser incorporadas no direito comunitário através da revisão da “*Capital Requirements Directive*” (processo de revisão designado de CRD IV).

Em particular, as medidas do BCBS³⁶ visam aumentar a resiliência do setor bancário, através do reforço da qualidade e da consistência do capital regulamentar, com vista a assegurar que os riscos assumidos pelos bancos se encontram adequadamente suportados por uma base de capital de elevada qualidade, que seja facilmente comparável entre instituições.

³⁶ Comité de Basileia de Supervisão Bancária

O BCBS (2010:63) “implementou novas alterações regulamentares de capital para a melhoria da qualidade do capital, as novas determinações implicaram o alargamento da cobertura de riscos. O aumento da quantidade de capital é outro elemento de importância. Foi dado destaque à criação de “*Buffers de capital*” em períodos de tranquilidade de forma a criar um amortecedor a ser utilizado em períodos de *Stress*³⁷. Esta percepção substanciou a criação de um “*Buffers de capital*”, estabelecido em 2,5% do património comum.

A não observância deste requerimento implica a imposição de restrições na capacidade do banco em distribuir ganhos, se não manter este requerimento as consequências do *Buffers de Capital* são: as restrições na sua capacidade de distribuir ganhos e a soma dos requerimentos mínimos de 4,5 % a este de 2,5% leva os requerimentos a 7%. Sancionou-se também a criação de um *Buffer* contra cíclico, que significa a possibilidade de elevação da conservação *Buffer* em 2,5% em períodos de grande elevação do crédito, ou seja, quando a formação de uma bolha se inicia e pode implicar risco para o sistema. E tal *Buffer* pode ser minorado quando o sistema bancário se vê diante da necessidade de absorver perdas que podem afetar a estabilidade financeira”.

Mendonça et al.(2011:10), referem ainda outra mudança: “a restrição da alavancagem está na introdução de um rácio não ponderado pelo risco, que possa atuar como um *backstop* para os requerimentos de capital, estamos assim perante um novo elemento que passa a compor a nova estrutura regulamentar. A justificativa para tal foi a percepção de que, no processo de geração da crise, a manutenção de níveis de capital adequado, mesmo “*Tier 1*³⁸”, não impediu que instituições assumissem elevadas posições alavancadas, dentro e fora do balanço. Desta forma, outra lição entendida pelo Comité da crise foi que há situações em que os requerimentos de capital ponderado pelo risco não possibilitam uma boa avaliação da saúde do banco”.

Segundo Cecchetti (2010:24, citado por Mendonça 2011:10), “em algumas situações as regras de ponderação de risco não são representativas do risco efetivo. Neste sentido, a introdução do rácio de alavancagem vem atuar como *backstop* aos requerimentos de capitais sensíveis ao risco, assim como os modelos de risco. O objetivo explicitado é contribuir para a contenção de risco sistémico que pode resultar de processos de crescimento excessivos da alavancagem”.

³⁷ Períodos de instabilidade financeira por razões endógenas ou internas das instituições

³⁸ O rácio do capital próprio do banco versus os seus ativos ponderados pelo risco

Mendonça et al.(2011:10), referem a mudança relacionada com os Índices de liquidez. Consideram que a “eclosão da crise e seus desdobramentos sobre os sistemas bancários acabaram por apontar a importância da liquidez das carteiras das instituições bancárias. Neste sentido, a introdução de índices de liquidez surgiu como resposta à fragilidade observada quando da crise”.

O BCBS (2010:9) salienta que “o objetivo é tornar os bancos mais resistentes a dificuldades potenciais em captações de curto prazo, assim como de enfrentar os desencontros estruturais de prazos de suas posições ativas e passivas. E, propõe a criação de dois instrumentos complementares: Os requisitos de liquidez incluem a introdução de um rácio de cobertura de liquidez de curto prazo (*Liquidity Coverage Ratio LCR*) que se destina a garantir que os bancos detêm ativos líquidos de elevada qualidade suficientes para fazer face a um cenário de crise grave com a duração de um mês, e um rácio de financiamento estável líquido (*Net Stable Funding Ratio NSFR*) a mais longo prazo, que aumenta os incentivos para que os bancos se financiem através de fontes mais estáveis numa base estrutural”.

Mendonça et al.(2011:11), verificam que “além destes indicadores, Basileia III inclui um sistema de monitorização que possibilite ao Supervisor a identificação e análise das tendências de liquidez não só de bancos individualmente, mas do sistema. A introdução de índices de liquidez coloca duas questões de ordens distintas. A primeira questão é da assunção do Comité de que a manutenção de capital em níveis adequados pode ser entendida como fundamental, porém não é suficiente para garantia da estabilidade do sistema bancário e a segunda questão da procura de instrumentos amplamente presente em estruturas regulamentarem prévio ao “regime de Basileia”. Na verdade, as transformações nos mercados financeiros, com o amplo desenvolvimento de instrumentos negociáveis e organização de mercados secundários acabaram por disseminar a crença de que liquidez não era mais uma questão a ser enfrentada. No entanto a crise, marcada por uma forte elevação da preferência pela liquidez dos agentes, mostrou o contrário”.

Cecchetti (2010:3, citado por Mendonça 2011:9) considera que “Basileia III representa uma expansão substancial e significativa dos *Buffers* de capital de apoio ao sistema bancário mundial. Também na taxa efetiva, as exigências são mais fortes e para introduzir mais rápido do que possa parecer. Por fim é possível afirmar que o reforço do capital resulta da forma de conceituação, da composição e do tamanho do capital a ser mantido”.

Neste sentido, considerando que a forma predominante de capital deve corresponder a ações ordinárias, reservas e resultados retidos, o BCBS reformulou integralmente as componentes de fundos próprios, que passaram a corresponder ao conjunto de:

“*Tier 1 Capital*” (*Going-Concern Capital*, ou capital regulamentar com capacidade de absorção de prejuízos numa perspetiva de continuidade da atividade de uma instituição), constituído pelo “*Common Equity Tier 1*” e “*Additional Going-Concern Capital*”; e “*Tier 2 Capital*” (*Gone-Concern Capital*, ou capital regulamentar disponível para absorver prejuízos numa perspetiva de liquidação de uma instituição).

Na prática, o “*Common Equity Tier 1*” constitui o capital de melhor qualidade da instituição, em termos de permanência e capacidade de absorção de prejuízos. Salvo no caso de uma eventual capitalização com recurso a investimento público, concretizada através da aquisição de ações pelo Estado com direitos especiais em termos de remuneração, o conceito de “*Common Equity Tier 1*” corresponde, no início da aplicação das novas regras de Basileia III, ao numerador do rácio “*Core Tier 1*” definido pelo Banco de Portugal.

A legislação nacional não previa até à presente data, o conceito de “*Core Tier 1*”, com o Aviso agora aprovado, passa a ser fixado um limite mínimo de 8% para este indicador, sendo o cálculo dos fundos próprios “*Core*” efetuado, tendo desde já por base as regras de Basileia III aplicáveis em 2013 para a definição do “*Common Equity Tier 1*”, i.e., antes da aplicação do regime transitório para determinadas deduções. No que se refere ao rácio *Tier 1* (também designado de rácio de adequação de fundos próprios de base), o Banco de Portugal recomendou em 2008 (Carta-Circular n.º 83/2008/DSB) o cumprimento de uma percentagem mínima de 8%. Em 2013, os rácios mínimos de “*Common Equity Tier 1*”, “*Tier 1*” e “*Total Capital*” serão, respetivamente, de 3,5%, 4,5% e 8,0%, não se aplicando ainda as deduções ao “*Common Equity Tier 1*”, aumentando gradualmente até 1 de Janeiro de 2015, onde atingirão os seus valores definitivos (4,5%, 6,0% e 8,0%, respetivamente).

Em complemento a estes rácios mínimos, encontra-se prevista a constituição de uma almofada de capital, exigível de forma gradual a partir de 2016, que ascenderá a 2,5% em 1 de Janeiro de 2019.³⁹

³⁹ Informação banco de Portugal

Chabanel (2011:4) refere que Basileia III “constitui uma oportunidade, assim como um desafio para os bancos, pode fornecer uma base sólida para a evolução próxima do setor bancário e pode garantir que os excessos do passado sejam evitados. Basileia III está a mudar a forma como os bancos abordam a gestão de risco e as finanças. O novo regime visa uma integração muito maior do financiamento e funções de gestão de risco. Isto irá provavelmente conduzir à convergência das responsabilidades do diretor financeiro na concretização dos objetivos estratégicos do negócio. No entanto, a adoção de uma postura regulamentar mais rigorosa pode ser dificultada por uma dependência de bases de dados e por uma separação de poderes entre aqueles que são responsáveis pelas finanças e aqueles que gerem risco. A nova ênfase na gestão de risco que é inerente a Basileia III exige a introdução ou a evolução de uma estrutura de gestão de risco que é tão robusto como as infraestruturas de gestão já existentes no setor financeiro”.

Maia (2010:3) refere “impactos relevantes sobre a economia portuguesa no setor financeiro do país. Os Acordos de Basileia III, obrigatoriamente, terão reflexos sobre os restantes agentes económicos e suas inter-relações: o Estado (e suas relações com outros), as empresas, as famílias e, implicitamente, a postura e a quantificação dos níveis de risco. O Estado passa a obter financiamentos a custos mais elevados por força de maiores exigências de capital, de precaução com o risco e liquidez do sistema bancário. A dívida soberana, teoricamente, deverá conhecer um custo acrescido nas taxas de juro, em todos os segmentos temporais (especialmente os mais longos).

Nas empresas, ao financiarem-se junto do sistema financeiro a um custo mais elevado, refletindo a precaução acrescida na concessão de crédito, investirão menos, criarão menos postos de trabalho e a economia terá disponível menos dinheiro para o investimento de substituição e de raiz (conduzirá a um crescimento real do produto menor). As famílias, por seu lado, conhecerão (tal como as empresas) *Spreads* mais elevados do que os atuais, decorrentes de exigências superiores com os riscos de crédito e de liquidez, conhecendo o crédito a conceder limites mais apertados do que os atuais”.

5.8.3 Sarbanes-Oxley

Hoje, continua o debate sobre as vantagens e os custos do SOX. Os seus apoiantes preconizam a imprescindibilidade da legislação, visto que veio desempenhar um papel útil em matéria de restauração da confiança do público nos mercados, através, entre outras medidas, do reforço dos controlos contabilísticos das empresas. Os seus opositores afirmam, em contraste, que este decreto introduziu um ambiente regulamentar extremamente complexo, que retira competitividade às empresas que o têm de implementar. Uma das secções mais significativas na área do risco operacional é a secção número 404. Nesta, é requerida à gestão das empresas a produção de um “relatório de controlo interno”. Este relatório deve conter uma avaliação de eficiência e eficácia da estrutura de controlo interno e procedimentos – para o fazerem, muitas empresas estão a adotar a arquitetura de controlo interno descrita na “*Framework COSO – Committee of Sponsoring Organizations of the Treadway Commission*” – que integra cinco componentes, nomeadamente, Ambiente de Controlo, Assessoria de Risco, Atividades de Controlo, Comunicação e Informação e Monitorização. O SOX é uma abordagem orientada para processos, característica que tem vindo a tornar-se comum à quase totalidade das implementações de risco operacional nas instituições financeiras portuguesas. A particularidade da sua orientação para a gestão de risco operacional incentiva a que as linhas orientadoras definidas pelo SOX sirvam também como facilitadoras para novas *Frameworks* e metodologias de gestão, como é o caso do “*BPM*” (*Business Process Management*), e para a identificação e a implementação de situações de melhoria ou de redesenho de processos. Para que possamos falar sobre sistemas de informação para a área de gestão de risco, devemos primeiro compreender as razões que levam as instituições financeiras a implementar este tipo de sistemas. Para Gibson (1997), podem ser apontadas três necessidades, a saber, a instituição deve;

- ✓ Ser capaz de medir os riscos a que está ou poderá vir a estar exposta, para entender mais plenamente esses mesmos riscos
- ✓ Procurar a melhor forma de poder recompensar as unidades de negócio ou os seus colaboradores, ajustando os incentivos à performance na área de risco
- ✓ Fornecer aos acionistas um “*Trade-Off*” ótimo entre risco e retorno.

O desenvolvimento de sistemas de informação para risco operacional em instituições financeiras ainda é recente e o menos avançado das diferentes áreas de risco (as áreas de risco de mercado e de crédito estão já a ser cobertas por sistemas de informação bastante robustos). No entanto, os mais novos desenvolvimentos em áreas como a modelação de dados e a quantificação de risco operacional levaram à promoção de um conjunto de blocos (arquitetura de um sistema de informação para risco operacional – figura 10) que já poderão ser aplicados à implementação de sistemas de informação para a gestão de risco operacional em instituições financeiras.

Alguns deste conhecimento foi recolhido em implementações de sistemas noutras áreas, como é o caso da indústria química que demonstra uma vasta experiência na aplicação de sistemas de informação de risco operacional.

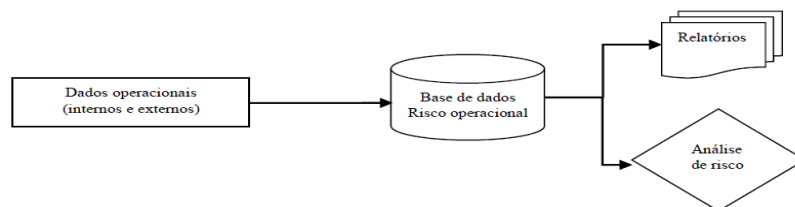


Figura 10 - Arquitetura de um sistema de informação para risco operacional

Uma das abordagens mais comuns para modelar risco operacional tem como finalidade construir uma distribuição das perdas potenciais de risco operacional para um determinado período temporal (Distribuição de perdas operacionais – figura 11). Tipicamente, esta distribuição é obtida através da combinação das distribuições da frequência e severidade das perdas, o que possibilita obter a medida “*VaR*” (*Value at Risk*), que representa o valor que a instituição pode esperar perder a um certo nível de probabilidade (e.g. 99.9%), sendo com base neste valor que esta deve alocar capital para se proteger contra este risco e evitar situações de insolvência.

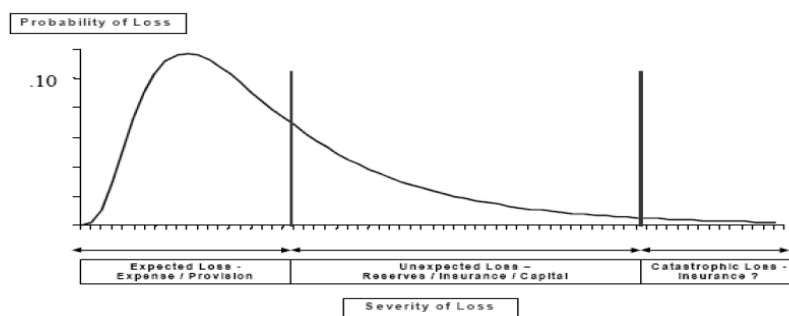


Figura 11 - Distribuição de perdas operacionais
 Fonte: Rosengren 2001

Uma das abordagens possíveis para classificação dos modelos de risco operacional divide-os em modelos “*Top-Down*” e “*Bottom-Up*”. Os modelos “*Bottom-Up*” baseiam-se na análise de eventos de perda em processos individuais, enquanto os “*Top-Down*” começam no nível de topo da organização e vão descendo para as linhas de negócio. Os modelos “*Bottom-Up*” são suportados por dados fornecidos por colaboradores que estão sob avaliação e que têm, por isso, pouco incentivo para serem pró-activos. Há que realçar que estes modelos podem ser utilizados, inclusive, com o propósito de diagnóstico de risco e no desenho de controlos internos, ao passo que os modelos “*Top-Down*” podem ser efetivos na estimação de requisitos de capital económico.

6. Conflito Interesses

Ainda que os conflitos de interesse surjam em diferentes profissões, o objeto que pretende acautelar é comum a todas elas. Neste sentido, devemos referir que o que se visa proteger com a regulação dos conflitos de interesse é a preservação de valores como a legalidade, lealdade, confiança e ética. A regulação no âmbito das relações profissionais revela-se essencial e imprescindível para que estes valores não sejam quebrados. Daí que, desde logo, seja primordial garantir a estreita relação entre as entidades e os clientes, através de mecanismos que previnam estes conflitos de interesse. Neste sentido, a regulação legislativa comunitária, nacional e a regulamentação interna de vários sectores têm um papel essencial.

A ausência destes normativos poderia criar na população em geral desconfiança em determinadas profissões. Cada profissão regula os seus conflitos de interesses da forma como entendem ser mais adequado, não se podendo esquecer que, em cada uma delas, se colocam problemáticas de formas diferentes, com agentes diferentes, podendo afetar interesses diferentes.

Com a globalização, a questão dos conflitos de interesse surge ainda com mais relevância no seio de grandes estruturas, como as grandes sociedades, exigindo da parte destas um grande esforço para conseguir cumprir todas as imposições legais, que se mostram cada vez mais rígidas. No entanto, é essencial que estas regras sejam cada vez mais apertadas uma vez que corrupção, a influência e pressão junto de potenciais grupos de risco tem crescido.

É possível afirmar que as implicações e as consequências que derivam dos conflitos de interesse são mais preocupantes em algumas áreas do que noutras. O setor económico-financeiro pelas suas particularidades torna-se bastante vulnerável ao tema. Nos últimos anos várias situações têm vindo a público, tal realidade pode ser justificada pela crise económica ou por uma crise de valores.

Genericamente o conflito de interesses caracteriza-se por uma situação em que alguém, potencialmente ou aparentemente, se vê confrontado com uma determinada situação que poderá originar uma quebra na sua confiança enquanto profissional, podendo comprometer de forma irreversível um negócio, uma relação jurídica ou uma simples decisão.

Uma outra situação que se pode caracterizar como sendo um conflito de interesse é aquela em que alguém tendo um interesse pessoal ou privado em determinada matéria influencie, ou tente influenciar o desempenho de outrem, de forma que este atue e seja parcial, atingindo assim o objetivo que pretende. Por interesse pessoal ou privado entenda-se qualquer potencial vantagem para o próprio, para os seus familiares, afins ou para o seu círculo de amigos.

6.1 Sociedades Financeiras

As sociedades financeiras estão hoje obrigadas a agir segundo princípios de integridade, equidade e imparcialidade, daí que procurem implementar medidas que garantam a identificação e a gestão de potenciais conflitos de interesses. A constante procura por uma atuação cada vez mais dentro das normas da ética, torna imprescindível a regulação de eventuais situações que possam originar conflitos de interesse.

Neste sentido, sempre que se verifique uma situação de potencial conflito de interesses entre uma instituição e determinadas pessoas ligadas à instituição, entre deveres que a instituição tem para com o cliente ou entre os diferentes interesses que diferentes clientes possam ter, há que ter em atenção tais situações para que ninguém seja lesado. Estas preocupações têm uma particular relevância quando estamos perante investimentos, gestão de carteiras, aplicações financeiras bem como processos de estudo, negociações e aconselhamento (efetuados pelas instituições financeiras). Assim algumas instituições implementaram medidas que visam a identificação de potenciais situações de conflitos de interesse, as quais em alguns casos, são a título exemplificativo descritas pelas normas de regulação interna das respetivas instituições (códigos deontológicos). A título de curiosidade deixamos aqui uma lista retirada das informações disponibilizadas *on-line* por algumas instituições e em que se considera haver conflito de interesses:

- ✓ Quando uma pessoa está em posição de obter um ganho financeiro ou evitar uma perda financeira por conta do cliente;
- ✓ Quando alguém tem interesse num determinado resultado num serviço prestado ou transação efetuada ao ou pelo cliente
- ✓ Quando alguém tem uma vantagem financeira ou benefício de outra natureza para favorecimento de um cliente ou vários clientes;
- ✓ Quando a instituição tem um interesse antagónico ao do cliente;
- ✓ Realização de operações por trabalhadores da instituição com acesso a informação privilegiada.

Algumas instituições dispõem de departamentos específicos que asseguram a prevenção de conflito de interesses e mesmo assim, quando essa prevenção não resulta, promovem o tratamento de eventuais reclamações a que tenha dado lugar. Desta forma, pretende-se assegurar a independência dos agentes económicos face aos interesses das pessoas cujas responsabilidades ou interesses representam. Com vista à prossecução deste objetivo mostra-se da maior importância a prevenção. As medidas de prevenção podem passar simplesmente, pelo esclarecimento e informação, pela separação das várias fases dos processos, sendo os intervenientes pessoas diferentes; por uma maior responsabilização destes e pela escolha de técnicos com rigor, de forma que seja um processo totalmente imparcial e ético.

Podem ocorrer conflitos de interesses entre:

- ✓ O Banco e um Cliente
- ✓ Uma Pessoa relevante e um Cliente
- ✓ Dois ou mais Clientes do Banco
- ✓ O banco como distribuidor e um Cliente

A “Diretiva dos Mercados de Instrumentos Financeiros” (*DMIF*) é uma “Diretiva Comunitária, (Diretiva 2004/39/CE, de 21 Abril de 2004)”, que entrou em vigor a 1 de Novembro de 2007, surgindo do esforço conjunto dos países membros (Comunidade Europeia) no sentido de tentar harmonizar a nível comunitário esta atividade (financeira), regulando a concorrência entre os mercados e as duas novas formas de negociação reconhecidas na “Diretiva”: sistemas de negociação multilateral e a internalização sistemática, visando garantir um maior grau de proteção aos investidores em sede de contratação de serviços de investimento e de atividades com eles relacionados, sendo os seus princípios orientadores:

- ✓ Reforço da proteção dos investidores;
- ✓ Integração comunitária dos Mercados de Capitais;
- ✓ Dinamização dos espaços de negociação;
- ✓ Regulação das condições do exercício de atividade.

A “*DMIF*” veio atualizar e alargar o conceito de atividades financeiras, abrangendo serviços de investimento e outros serviços auxiliares, bem como reforçar os deveres dos intermediários financeiros, o que representa uma maior garantia e maior proteção para o investidor.

Os intermediários financeiros passaram a ter como dever a deteção de efetivos e potenciais conflitos de interesse, pelo que surge a necessidade de adotarem medidas necessárias para evitar que os interesses dos seus clientes saiam lesados. Quando tal não seja possível, os clientes têm de ser informados. De acordo com a “Diretiva”, uma sociedade de investimento deve tomar todas as medidas razoáveis ao seu alcance de forma a evitar que conflitos de interesse relevantes prejudiquem os interesses dos clientes. Isto significa adotarem uma política de gestão de conflitos de interesse adequada à dimensão, organização, natureza e complexidade da sua atividade. Desta forma, devem tentar implementar procedimentos eficazes para impedir ou controlar a troca de informações entre colaboradores; fiscalizar os colaboradores envolvidos na prestação de serviços a clientes; adotar medidas que impeçam ou limitem qualquer pessoa de exercer influência e evitar que haja envolvimento simultâneo ou sequencial em diferentes atividades do mesmo funcionário. A “DMIF” veio ainda estabelecer que os intermediários financeiros devem criar e manter atualizados registo de serviços suscetíveis de integrarem conflitos de interesse potencialmente prejudiciais aos interesses de um ou vários clientes, devendo ainda procurar estabelecer medidas que visem defender os interesses dos clientes, de forma honesta, equitativa e profissional. Uma das conclusões evidenciadas é que os conflitos de interesse devem ser localizados e resolvidos (o mais breve possível) de forma a não resultar num prejuízo para uma das partes. Há algumas áreas em que se começam a desenvolver verdadeiros processos de resolução de conflitos de interesse. Estes processos passam por uma tutela de antecipação e previsão. Quer isto dizer que o facto de se ter um plano para executar uma política de conflito de interesses permite muitas vezes evitar esses mesmos conflitos. O plano deve passar pela previsão e registo de situações potencialmente originadoras de conflitos de interesse e as formas de lidar com essas situações, seja resolvendo o conflito de forma a não lesar uma das partes, seja comunicando à parte o conflito, quando não seja possível resolvê-lo.

Outra forma de prevenir eventuais conflitos passará pela separação de diferentes áreas de interesse, com diferentes intervenientes, por fiscalizações regulares por entidades externas, por estabelecer mecanismos de hierarquia sem que haja uma intromissão no trabalho dos profissionais, mas apenas uma função de controlo das funções (não das competências) e ainda pela atribuição de remunerações que não permitam que qualquer um dos intervenientes se sinta seduzido a deixar-se influenciar numa situação potenciadora de conflitos.

O desafio está em conseguir gerir os conflitos de interesses, criando soluções que reduzam ou eliminem estes conflitos, através de soluções que passem pelo envolvimento de vários agentes, desde o legislador aos auditores, aos acionistas, aos sócios e os próprios órgãos de gestão. Há necessidade de maior transparência na legislação para que se consiga prever, identificar e evitar os conflitos e os interesses. Nesta necessidade de maior transparência e maior previsão das situações, as sociedades reguladoras das várias atividades e profissões têm um papel muito importante, pois cada grupo deve definir os seus potenciais conflitos de interesse.

7. Fraude Bancária

O elevado número de clientes que se desloca aos balcões da vasta rede de agências bancárias aumenta o risco de exposição das instituições, no entanto o risco pode também surgir a nível interno, quando os próprios funcionários são os protagonistas no que diz respeito à ocorrência de fraude. O crime é encarado como um investimento económico, sendo que os próprios criminalistas defendem que o crime organizado é um investimento económico para aqueles que apreciam retornos consideráveis de forma rápida, com níveis de investimento e de risco mínimos. De facto, “desde que foram constituídos os bancos têm sido alvo de roubos e vigarices” (Narasimhan, 2005).

“A existência de falhas no controlo interno é apontada como uma das causas que levam ao aumento da probabilidade de ocorrência de fraude, nomeadamente, as práticas de gestão, a falta de segregação de funções, falta de controlos independentes, falta de atividades físicas salvaguardadas, falta de autorizações adequadas, falta de documentos e registos corretos e um sistema de contabilidade impróprio” (Albrecht, 1996).

“Para além disso, existem, ainda, outros fatores que aumentam a probabilidade de ocorrência de fraude no sistema bancário: recompensas insuficientes, ambiguidade nas funções desempenhadas, nos deveres, nas responsabilidades e nas áreas de responsabilidade, quando se verificam níveis de desempenho e comportamentos pessoais inferiores aos desejáveis e, por último, carência de inspeções periódicas e oportunas, que visem o cumprimento dos objetivos definidos pela instituição” (Bolonha, 1994).

As instituições bancárias são frequentemente alvo de tentativa ou de ocorrência de fraude, o cliente ou o potencial cliente e o próprio funcionário agem com intenção ilícita de obtenção de ganhos pessoais sobre terceiros e contra a própria instituição, sendo importante que as mesmas definam políticas mitigadoras e persuasoras de tais situações. A identificação e o reconhecimento de situações de risco de fraude às quais as instituições bancárias estão expostas permite agir em conformidade no que diz respeito à adoção de procedimentos e de normas de carácter interno e externo. O Banco de Portugal, no âmbito das suas atribuições e competências, tem vindo a acompanhar com especial cuidado o novo enquadramento legislativo dos mercados bancários de retalho, introduzindo a regulamentação necessária e em prol do seu completo entendimento pelos agentes. Embora a resposta à crise financeira se tenha sobretudo centrado nas questões prudenciais, é verdade que também as regras comportamentais se tornaram neste contexto, de importância crescente, impulsionadas não só pelas autoridades nacionais como pelas instâncias internacionais, como a União Europeia e a OCDE⁴⁰.

Por outro lado, os mercados bancários de retalho tornaram-se, em todo o mundo, cada vez mais exigentes e complexos, e em consequência, muitos clientes deixaram de ser capazes de perceber todas as características dos produtos que adquirem, e até, de avaliar os riscos que muitas vezes inadvertidamente são levados a assumir. Como resposta à nova situação verificaram-se alterações significativas nos normativos legais que regem os mercados bancários de retalho, nomeadamente no que se refere aos depósitos bancários, ao crédito à habitação e ao consumo, e ainda, à publicidade sobre os produtos bancários em geral.

“Em virtude da importância estratégica para a economia, o setor bancário tem despertado o interesse da generalidade dos economistas, sendo que tendencialmente, a banca tem vindo a ser alvo de alterações significativas resultantes de vários fatores, nomeadamente a evolução tecnológica, que tem sido destacada como sendo um dos principais fatores que impulsionam e facilitam as referidas mudanças” (Instituto de Formação Bancária, 2004).

⁴⁰ Organização para a Cooperação e Desenvolvimento Económico

As tecnologias têm provocado alterações nas diferentes práticas sociais, económicas e culturais, o que permite atingir grandes níveis de desenvolvimento associados, essencialmente à informatização e à automatização dos processos, no que diz respeito especialmente, à prestação de serviços bancários. O aumento significativo das atividades bancárias realizadas através de meios eletrónicos permitiu a conversão de elevados níveis de dinheiro em fluxos informacionais, que são movimentados, transacionados e armazenados em suportes e meios eletrónicos.

“Por consequência, a quantidade de movimentações financeiras realizadas de forma eletrónica, ou medidas com recurso às tecnologias de informação, têm vindo a crescer de forma considerável, tornando a banca uma área bastante aliciante no que diz respeito à captação dos recursos dos investidores pelas vias enumeradas. Em contrapartida, verificou-se o despertar do interesse fraudulento de outros indivíduos pela mesma área, dando lugar a comportamentos ilícitos e prejudiciais por parte dos mesmos” (Neto, 2010).

“É unânime a opinião de que o combate a este tipo de comportamentos fraudulentos e de outros associados à atividade bancária passa, em grande parte, pela prevenção: melhorar a prevenção e manter uma atitude atenta e vigilante são algumas das recomendações por parte dos responsáveis” (Bento, 2011).

“O modelo de negócio encontra-se em constante mutação, pelo que, a cada dia que passa, surgem novas vulnerabilidades e, conseqüentemente, a obrigação por parte dos funcionários e responsáveis a refletir sobre o nível de segurança necessário a cada momento” (Bento, 2011).

Wells (2009) refere que “No mundo do comércio, as organizações incorrem em despesas para produzir e vender os seus produtos ou serviços. Estes custos percorrem toda a linha: mão-de-obra, impostos, publicidade, rendas, matérias-primas, investigação, desenvolvimento e, também, fraude e abuso. Este último custo, contudo, é radicalmente diferente dos primeiros: a verdadeira despesa da fraude e do abuso encontra-se oculta, mesmo que refletida nos números de perdas e lucros”.

Nesse sentido, sendo a fraude uma realidade presente nas instituições, que se manifesta através da prática intencional de atos ilícitos para a obtenção de ganhos sobre terceiros, é necessária a existência de mecanismos e de procedimentos que tenham como objetivo diminuir a frequência da sua ocorrência ou, pelo menos, minimizar os seus efeitos através de práticas de prevenção e controlo por parte dos diferentes colaboradores.

Wells (2009) refere que “É importante compreender as razões que levam as pessoas a cometerem atos fraudulentos, para que seja possível melhorar a avaliação de risco e ajudar os diferentes empregadores e clientes na implementação de medidas que tenham como objetivo a prevenção e a detenção da fraude”.

7.1 Fraude e Abuso Ocupacional

Quando falamos em fraude estamos a englobar um vastíssimo conjunto de situações, tendencialmente intencionais, em que uns cidadãos ou instituições enganam outros, causando direta ou indiretamente danos económico-sociais. Estamos, sobretudo, a considerar os processos que se inserem no tecido económico em crescente globalização. Os comportamentos fraudulentos são pouco visíveis por diversas razões. Como referia, Alves dos Reis, “se todas as caixas de fósforos trouxerem menos cinco fósforos que o que consta da caixa, ninguém dará por isso”.

“A fraude é todo e qualquer ato ilegítimo caracterizado por engano, encobrimento ou violação da confiança, que não depende do recurso à ameaça, à violência ou à força física. As fraudes são praticadas por indivíduos e por organizações que visam a apropriação de dinheiro e de bens ou serviços, o alcance de vantagens pessoais ou comerciais e evitar o pagamento ou a perda de serviços” (Instituto Português de Auditoria Interna, 2009).

Black (1979) define fraude como “a deturpação da verdade e de fatos para induzir terceiros a agir com intuito de detrimento alheio”. Para efeitos e segundo a “*Association of Certified Fraud Examiners*” (1996), “fraude e abusos ocupacionais dizem respeito à utilização de um emprego para enriquecimento pessoal através do uso deliberado ou da indevida aplicação dos recursos ou dos ativos da entidade empregadora”. Em termos genéricos, o conceito de fraude ocupacional assume uma natureza económica, independente das suas consequências legais, estando presente a intencionalidade de quem executa.

A “*Association of Certified Fraud Examiners*” (2006) classifica e estrutura o conceito de fraude através da Árvore da Fraude, distinguindo e definindo três grandes categorias de fraude:

- ✓ Corrupção
- ✓ Apropriação indevida de atos
- ✓ Relatórios de contas fraudulentos.

Podemos definir corrupção como todo e qualquer esquema através do qual uma pessoa usa a influência que detém numa determinada transação ou num determinado negócio, nos quais intervém, para obter um benefício associado e, logicamente, não autorizado. Por apropriação indevida de ativos entende-se todo e qualquer esquema que envolve furto de ativos da organização. Por relatórios de contas fraudulentos entende-se a falsificação intencional da informação financeira de uma organização, com o objetivo de tornar a situação económico-financeira rentável.

Almeida (2003) considera a existência de dois tipos de fraude relativamente à abordagem feita pela “*Association of Certified Fraud Examiners*” (2006): “fraude organizacional e fraude contra a própria empresa”. A primeira é cometida em benefício da própria entidade e implica o envolvimento de práticas que atuam, normalmente, contra entidades exógenas à empresa, como a administração fiscal, os credores, os sócios ou os acionistas e resulta, geralmente, na falsificação de Demonstrações Financeiras.

A fraude contra a própria empresa é cometida a favor do sujeito que pratica o ato fraudulento e consiste, essencialmente, no roubo de ativos e no desfalque. Ferreira (2007) propõe uma articulação entre as duas classificações, isto é, entre a proposta apresentada pela “*Association of Certified Fraud Examiners*” (2006) e por Almeida (2003), concluindo que corrupção e a apropriação indevida de ativos são classificadas como atos fraudulentos contra a empresa, classificação ordeira relativamente à classificação defendida pela “*Association of Certified Fraud Examiners*”.

Relativamente à fraude organizacional, também designada por fraude nas Demonstrações Financeiras, Ferreira (2007) refere que “a mesma pressupõe a manipulação de registos contabilísticos em benefício da própria empresa e incentiva o uso de práticas que atuam contra os agentes económicos externos à empresa”.

Ou seja, a própria empresa está envolvida e a favor das opções que são deliberadas no Relatório Financeiro, revelando-se parte ativa do ato fraudulento, aspeto não salientado na classificação defendida pela “*Association of Certified Fraud Examiners*” (2006) e por Almeida (2003).

A fraude pode incluir qualquer crime para obtenção de lucro, utilizando como principal ferramenta o logro⁴¹, quer isto dizer: a imposição de uma ideia ou crença falsa, que provoque a ignorância, a perplexidade ou a impotência. No entanto, para que todos os logros sejam considerados atos fraudulentos é necessário a existência de danos, geralmente associados a dinheiro, para a vítima.

“É possível identificar três formas de retirar dinheiro a uma vítima de forma ilegal: força, logro ou furto, sendo que, nos termos do direito comum, existem quatro elementos gerais, que devem estar presentes, para que ocorra uma fraude: uma declaração material falsa, o conhecimento de que a declaração era falsa no momento em que foi proferida, a confiança na declaração falsa por parte da vítima e os danos daí resultantes” (Wells, 2009).

“As práticas abusivas são uma realidade nas diferentes organizações, o que representa custos para os empregadores, pelo que se podem fazer sentir de diversas formas por parte dos empregados: utilização de descontos de empregado para aquisição de bens para amigos e parentes, apropriação de produtos pertencentes à organização, pagamento superior ao número de horas às que trabalham, recebimento de mais dinheiro do que o devido relativamente ao reembolso de despesas, realização de almoços de longa duração ou de pausas sem autorização, atrasos nas horas de entradas e saídas do trabalho mais cedo, utilização da baixa por doença quando não estão doentes, desenvolvimento de funções lenta ou desleixadamente e sobre a influência de álcool ou drogas” (Wells, 2009).

7.2 O Triângulo da Fraude de Donald R. Cressey

Cressey (1919-1987) criminalista, interessava-se essencialmente, nas condições que levavam os diferentes fraudadores, “*violadores da confiança*”, segundo as suas palavras, a ser dominados pela tentação inerente ao ato de praticar a fraude.

⁴¹ “Ação e/ou comportamento que, sendo desonesto e ardiloso, tem a intenção de enganar ou ludibriar alguém” (Dicionário Língua Portuguesa)

“As pessoas, em quem se confia, tornam-se violadoras dessa confiança quando imaginam que têm um problema financeiro impossível de partilhar e que acreditam poder ser secretamente resolvido, através da violação da confiança financeira. Para além disso, são capazes de aplicar à sua conduta, naquela situação, justificações que lhes permitem ajustar o conceito, que têm de si próprios, de pessoas de confiança, de utilizadores dos fundos ou propriedade que foram confiando” (Cressey, 1973).

A referida hipótese passou a ser conhecida como o “*Triângulo da Fraude*”, apresentado na Figura 12, em que o primeiro vértice representa uma necessidade financeira sentida, impossível de partilhar, o segundo vértice representa a oportunidade apercebida e o terceiro vértice representa a justificação.



Figura 12 - Triangulo da Fraude
Fonte: Adaptado de Cressey, 1973

Nos casos de violação de confiança identificados, o infrator pensava que o problema financeiro com que se encontrava, não podia ser partilhado com pessoas que, provavelmente poderiam ter contribuído para a solução do problema (Cressey, 1973).

Cressey (1973) declarou que aquilo que é considerado como “*não partilhável*” é, apenas, segundo o ponto de vista do potencial fraudulento ocupacional e dividiu os problemas não partilháveis em seis categorias básicas:

1. Violação das obrigações imputadas

“A incapacidade de pagar dívidas tem-se revelado historicamente, um forte motivador” (Wells, 2009). Os problemas financeiros resultantes de posição de confiança não financeira são, frequentemente, considerados impossíveis de partilhar, uma vez que são encarados como uma ameaça ao estatuto inerente a determinada posição.

“Por vezes, as pessoas incorrem em dívidas ou, de algum outro modo, tornam-se devedoras, sendo que, muitas consideram que as mesmas dívidas devem permanecer secretas e que encará-las se torna um problema financeiro impossível de partilhar” (Cressey, 1973). Wells (2009) recorre ao exemplo dado por Cressey, onde este descreve uma situação que todos podemos compreender: ser capaz de pagar as dívidas e depois ter de admiti-lo ao empregador, à família e aos amigos.

2. Problemas resultantes do fracasso pessoal

Cressey considera que os problemas resultantes do fracasso pessoal podem ser de vários tipos: “Enquanto alguns problemas financeiros podem ser considerados como resultado de condições económicas (...) outros foram criados por atividades insensatas ou mal planeadas”. “Para um potencial delinquente, a possibilidade de escolher entre encobrir as suas más opções de investimento pela violação da confiança ou admitir que não é um bom investidor, pode colocar em causa o discernimento de pessoas orgulhosas. A eventual perda de estatuto faz com que as pessoas tenham receio em admitir que têm, de facto, um problema, consequência dos seus próprios comportamentos” (Wells, 2009).

3. Reveses de negócios

“Diferentes dos problemas resultantes do fracasso pessoal, uma vez que algumas pessoas de negócios consideram que os seus deveres financeiros resultam de condições fora do seu controlo: inflação, taxas de juros (elevadas), financiamentos e empréstimos” (Cressey, 1973). “Há muito poucas pessoas capazes de abandonar um negócio falhado. Quando a ponte está a cair, quase toda a gente corre para obter um pedaço de madeira. No mundo dos negócios, existe um eterno optimismo de que as coisas melhorarão no dia seguinte. Pomos o negócio em marcha, mantemo-lo em funcionamento, e quase ficamos hipnotizados por ele (...) a maior parte de nós não sabe quando desistir, quando dizer, fui derrotado. Eis uma vitória para o adversário” (Cressey, 1973).

4. Isolamento físico

Cressey (1973) refere também, “o isolamento físico, no qual a pessoa que se encontra em dificuldades financeiras está isolada das pessoas que eventualmente as poderiam ajudar”.

5. Obtenção de estatuto

“Verifica-se que por vezes, a pessoa é confrontada com o facto de não possuir os meios financeiros necessários para se associar a pessoas com o nível de estatuto ambicionado, avaliando a situação como um problema, que se torna impossível de partilhar quando sente que não pode desprezar as suas aspirações de admissão do grupo desejado, nem obter as características de prestígio necessárias para a sua admissão. Nesse sentido, o tormento provocado pela necessidade de conseguir estar ao mesmo nível das outras pessoas revela-se uma realidade enfrentada por muitos delinquentes ocupacionais” (Cressey, 1973).

6. Relações empregado-empregador

“O ressentimento, por parte do empregado para com a organização, é o problema mais comum resultante da relação entre as partes, que pode resultar de desigualdades económicas sentidas, tais como o ordenado, ou do sentimento de estar sobrecarregado ou ser subvalorizado. O empregado considera o referido problema impossível de partilhar quando conclui que ao fazer sugestões, que tenham como objetivo minimizar determinado (mau) tratamento, possa colocar em causa a sua posição na organização” (Cressey, 1973).

Em todos os casos de estudo, existia uma sensação de que, devido a atividades anteriores ao desfalque, a aprovação por parte de grupos financeiros valorizados, para a pessoa de confiança, se havia perdido ou a sensação de que a aprovação por parte dos mesmos grupos ficaria perdida, se fossem reveladas determinadas atividades, isto é, o problema financeiro difícil de partilhar, que estabelece nas pessoas, em quem se confia, o desejo de um tipo de solução específica para os problemas que enfrenta.

“Os resultados revelaram-se uniformes, isto é, a solução ou a solução parcial do problema passa pela utilização de fundos obtidos por um método independente, secreto e seguro, de acordo com os seus critérios e justificações, disponíveis para as pessoas naquele momento” (Cressey, 1973). Ou seja, para um violador de confiança é necessário que este acredite que a sua situação possa ser, secretamente, resolvida.

“O violador de confiança tem de ter dois pré-requisitos, nomeadamente, informações gerais e competência técnica e deve revelar-se capaz de desculpar os seus atos perante si próprio, avaliando os seus delitos segundo três pontos de vista: como não criminoso, como justificado ou como parte de uma situação que os infratores não controlam” (Cressey, 1973).

“É necessária a existência de três elementos para que a violação de confiança ocorra, nomeadamente, o motivo, a oportunidade apercebida e a capacidade de justificação, sendo que a violação de confiança ocorre quando a posição de confiança é encarada como forma de revolver um problema não partilhável, pela pessoa de confiança, com base nos conhecimentos adquiridos sobre os fundos que lhe são confiados e com base nas justificações consideradas para a utilização dos mesmos. Nesse sentido, os três elementos constituem as condições sob as quais a violação da confiança ocorre, sendo que sempre que a conjuntura dos elementos ocorra, verifica-se a violação de confiança, se a conjuntura dos elementos não ocorre, não há violação de confiança” (Cressey, 1973).

7.3 A Balança da Fraude de W. Steve Albrecht

Albrecht⁴², contribuiu para a investigação da fraude, sendo que numa das suas análises, apurou as diferentes motivações dos autores da fraude e do abuso ocupacional:

- ✓ Viver acima das suas poses;
- ✓ Um desejo irresistível de lucro pessoal;
- ✓ Elevada dívida pessoal;
- ✓ Uma associação íntima aos clientes;
- ✓ Sentir que o ordenado não é proporcional à responsabilidade;
- ✓ Uma atitude intriguista;
- ✓ Um forte desafio de vencer o sistema;
- ✓ Hábitos de jogo excessivos;
- ✓ Pressão indevida de família ou de pares.

⁴² W. Steve Albrecht, professor e presidente da “Association of Certified Fraud Examiners” (1989-1992) e da “American Accounting Association” (1997-1998).

“Os autores de grandes fraudes utilizavam os ganhos para comprar casas, automóveis, propriedades de lazer, fazer férias dispendiosas, sustentar relações extraconjugais e realizar investimentos especulativos e os autores de pequenas fraudes tinham um procedimento diferente” (Albrecht, Howe e Rommey 1984).

Tal como Cressey (1973), também Albrecht, Howe e Rommey (1984) sugerem fatores envolvidos nas fraudes ocupacionais: “a pressão situacional, a perceção da oportunidade para cometer e, posteriormente, ocultar o ato desonesto e o facto de se considerar o referido ato como sendo inconsistente com o nível de integridade pessoal ou como justificável”. A chamada “*Balança da Fraude*”, apresentada na Figura 13, que inclui “fatores como a pressão situacional, as oportunidades de concretização e a integridade pessoal, permite concluir que quando a pressão situacional e as oportunidades de concretização são elevadas e a integridade pessoal é baixa, é mais provável que ocorra a fraude ocupacional do que quando se verifica o contrário” (Albrech, Howe e Rommey, 1984).



Figura 13 – A balança da Fraude
Fonte: Adaptado de Albrech, 1983

As pressões situacionais são descritas como os problemas imediatos que as pessoas sentem nos seus ambientes, sendo que, possivelmente, as dívidas elevadas ou os prejuízos financeiros assumem um carácter mais premente. “As oportunidades de concretização, isto é, as oportunidades para cometer a fraude podem ser criadas por controlos internos deficientes ou inexistentes, quer por parte do empregado, quer por parte da empresa. A integridade pessoal diz respeito aos comportamentos éticos que cada pessoa adota” (Albrecht, Howe e Rommey, 1984).

7.4 Gestão de Risco de Fraude no Sistema Bancário

Na execução das suas atividades, os bancos comerciais enfrentam riscos ao nível de vários domínios, nomeadamente, risco de crédito, risco de mercado, risco de liquidez, risco da taxa de juro, risco cambial e risco operacional, para além disso, enfrentam também o chamado risco de fraude, sendo que a fraude representa, por si só, um crime, pelo que, nesse sentido, reúne características diferentes dos restantes domínios associados ao risco.

Relativamente ao risco operacional, trata-se de um tipo de risco que resulta de falhas dos bancos ao nível de controlo interno, de erros humanos, de problemas e/ou falhas no sistema informático e da falta de compreensão da administração ou da falta de conhecimento de outros sistemas operacionais.

“Apesar de os avanços tecnológicos e informáticos terem permitido aumentar a eficiência no negócio bancário, acabaram por originar, também, novas fontes de risco e de fraude” (Lastra, 2000).

A gestão do risco de fraude deve ser definida a partir do topo, nomeadamente, a partir dos diretores executivos, da comissão de auditoria e dos conselheiros independentes, isto é, essencialmente, a partir de cargos associados a funções de chefia e de controlo. A estratégia deve ser assente na compreensão, redução e deteção de riscos, na análise e deteção de sinais de alerta, na gestão de incidentes e na prevenção de risco de fraude, o que implica a existência de meios e técnicas que permitam aumentar a segurança e a resistência de uma instituição.

Ou seja, a estratégia de gestão do risco de fraude deve ser composta por seis elementos conforme ilustra a Figura 14. “Os mesmos responsáveis devem assegurar a definição de um código de conduta, isto é, a definição de princípios e valores associados à ética, à cultura e ao comportamento empresarial e a política de gestão de risco de fraude deve apostar na gestão de risco, na denúncia e na investigação, que permitam combater a fraude” (Iyer e Samociuk, 2006).



Figura 14 – Estratègia de Gesto de risco
Fonte: Adaptado de Iyer e Samociuk, 2006

“A gesto do risco de fraude deve definir objetivos claros e compreensivos, os quais podem ser definidos segundo duas categorias: principais, nomeadamente, criar um ambiente favorvel  preveno, construir uma organizao resistente, reduzir os custos, aumentar o valor e garantir a continuidade do negcio e secundrios, nomeadamente, recuperar perdas, proteger os trabalhadores honestos, corresponder s obrigaoes legais e proteger a reputao da organizao” (Iyer e Samociuk, 2006).

“A no compreenso dos riscos e a falta de formao na preveno e na deteo da fraude pode dar lugar  resistncia no que diz respeito  implementao e  aceitao de polticas de gesto de risco na instituio, nomeadamente, nas pessoas que nela exercem funoes, o que se torna um obstculo no combate  fraude” (Iyer e Samociuk, 2006). O conselho de administrao da instituio deve ser responsvel pela estratègia de gesto de risco, o que inclui a avaliao, a reduo e a deteo de risco de fraude, sendo, tambm, importante determinar um conjunto de pessoas, principalmente associadas a funoes corporativas, que levem a cabo os referidos programas.

No entanto, as tarefas de avaliao, reduo, deteo e preveno da fraude devem passar pelos diferentes colaboradores de uma instituio, isto , as diferentes responsabilidades devem ser distribudas pela instituio, esperando uma atitude pr ativa por parte de todos os que a constituem e que na mesma exercem funoes.

“Os papéis e as responsabilidades devem ser claramente definidos nas políticas da organização e a estratégia de gestão de risco deve incluir também os colaboradores, os quais se revelam importantes na estratégia de gestão de risco de fraude, uma vez que não é solução incluir apenas determinados órgãos na estratégia de gestão de risco, sendo que, idealmente, todas as pessoas de uma instituição devem assumir um papel ativo no combate à fraude” (Iyer e Samociuk, 2006).

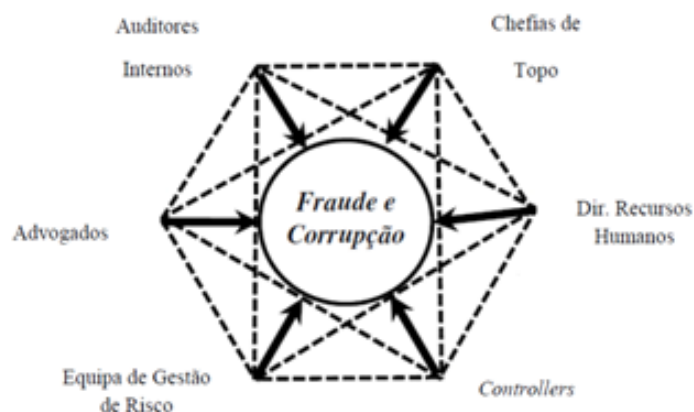


Figura 15 – Protagonistas na Gestão de Risco
Fonte: Adaptado de Iyer e samociuk, 2006

“Os funcionários bancários não dão a devida importância ao problema relacionado com a existência de fraude, sendo que o nível de consciência existente a respeito da fraude é pouco satisfatório e a maioria deles não revela uma atitude favorável” (Khanna e Arora, 2009).

“O impedimento da fraude e do abuso dos profissionais começa no pensamento do empregado, uma vez que os empregados que sentem que serão apanhados na fraude e no abuso ocupacional têm menos probabilidades de os cometer” (Wells, 2009).

“O mundo dos negócios revela-se muito competitivo e, conseqüentemente, os funcionários manifestam sintomas relacionados com o Stress, o que resulta em sentimentos associados à sensação de não reconhecimento do trabalho que desenvolvem na instituição onde exercem funções. Com a existência de problemas pessoais e de falhas existentes no controlo interno, a motivação para a prática de atos fraudulentos, por parte dos funcionários, pode surgir ou tornar-se mais evidente, cenário indesejável para qualquer instituição” (Haugen e Selin, 1999).

“As fraudes são praticadas, frequentemente, por pessoas que possuem autoridade, sobretudo, quando acumulam funções. Geralmente ocorrem de forma premeditada, e portanto, a sua deteção torna-se mais difícil e a sua existência tende a perdurar caso não existam controlos adequados. Existem várias razões para a ocorrência de fraude por parte dos funcionários, nomeadamente, razões financeiras, isto é, a prática de atos fraudulentos por parte dos empregados pela simples necessidade financeira, razões relacionadas com a insatisfação profissional e com a vingança, (uma vez que muitas fraudes decorrem do sentimento de desvalorização profissional), razões relacionadas com irregularidades generalizadas, (ocorrem quando os funcionários realizam atividades de forma ilegal na empresa, sem qualquer penalização, o que leva os restantes funcionários a agir da mesma forma, dado que não existirá penalização), e razões relacionadas com a tentação pelo perigo, dado que existem profissionais que exercem atos fraudulentos, simplesmente, pelo prazer em infringir a lei, desenvolvendo esquemas de fraudes” (Sá, 1997).

Cada pessoa avalia o seu próprio valor, sendo que se considerar que está a ser compensada de forma injusta relativamente ao seu salário, isto é, se o empregado se revelar insatisfeito, frequentemente, surge a motivação para agir de forma fraudulenta, sendo esta a razão mais apontada para a ocorrência de comportamentos fraudulentos por parte dos funcionários.

Para além disso, “as pressões financeiras, isto é, a necessidade de cumprir com as suas obrigações financeiras, nomeadamente, de carácter pessoal, revelam-se, também, como um fator impulsionador da fraude por parte dos funcionários” (Wells, 2001).

7.5 Avaliação e Prevenção da Fraude

A prevenção da fraude requer uma forte ênfase na criação de um ambiente de trabalho que promove a ética comportamental, impede a ilegalidade e incentiva os funcionários a denunciar situações de fraude ou situações de suspeita de fraude.

“Os diferentes funcionários devem, portanto, ser instruídos com base nos valores da empresa, o que lhes fornece uma orientação clara sobre o comportamento e as ações que lhes são ou não permitidas” (*Association of Certified Fraud Examiners*, 2006).

“A prevenção da fraude deve começar no início da relação com os empregados, isto é, a partir da sua contratação, com o objetivo de se proceder a um levantamento do histórico dos potenciais empregados, nomeadamente, dos locais onde já exerceram funções e dos seus comportamentos” (Santi, 1988).

Posteriormente, as organizações devem fornecer formação de carácter antifraude na altura em que os trabalhadores são contratados, de natureza fatural e não acusatória. Deste modo, os empregados tornam-se os olhos e os ouvidos da organização, tornando-se mais provável que denunciem eventuais comportamentos e atividades fraudulentas. “A fraude, independentemente da sua natureza, acaba por ter consequências negativas para a organização e para as pessoas que nela exercem funções, uma vez que tem impacto sobre os salários, os empregados, os benefícios, a moral, os lucros e a integridade pessoal. A mão-de-obra informada sobre a fraude é, de fato, a melhor forma de prevenir a sua ocorrência nas organizações” (Wells, 2009).

“A formação na qualidade possui um duplo efeito positivo sobre os funcionários, uma vez que, se por um lado, ajuda no desenvolvimento do trabalho, por outro lado, maximiza o potencial desempenho dos funcionários, fornecendo-lhes conhecimento e competências necessárias para a compreensão das práticas e dos princípios bancários” (Barnes, 2005).

A existência de programas de denúncia adequados é essencial para detetar e impedir a fraude e o abuso ocupacional, uma vez que, frequentemente, os empregados suspeitam de atividades ilegais, mas não têm forma de comunicar essa informação, sem receio de serem, eles próprios, arrastados para a investigação. Nesse sentido, os programas de denúncia devem salientar, pelo menos, seis pontos:

- 1) A fraude, o desperdício e o abuso ocorrem, de uma maneira ou de outra, em quase todas as organizações;
- 2) A fraude tem um efeito negativo sobre os postos de trabalho, carreiras, remunerações e os lucros da entidade;
- 3) A organização deve encorajar de forma ativa os empregados a darem informações com intuito de persuadir a fraude;
- 4) Não existem sanções pelo fornecimento de informações (se as mesmas não tenham fundamento, mas fornecidas de forma desinteressada)

- 5) Existe um método exato para denunciar, por exemplo, um número de telefone, um endereço eletrónico, um “Link”, sem identificação do utilizador;
- 6) As denúncias de atividades suspeitas não têm que ser comunicadas pelos empregados aos seus supervisores imediatos (podendo ser encaminhadas diretamente para área correspondente).

A linha direta (Link ou endereço eletrónico) é considerada, pela maioria dos profissionais, como decisiva nos programas de denúncia de fraude, sendo que muitos dos casos de fraude descobertos, o são efetivamente através do referido método, os mesmos não teriam sido descobertos através de qualquer outro método. Também as linhas diretas, independentemente do seu tipo, contribuem para aumentar a perceção da deteção da fraude. “Os empregados que têm consciência de que as atividades desonestas podem ser denunciadas por um colega de trabalho terão menos probabilidades de se comportarem de tal forma” (Wells, 2009).

Por vezes, existem ocasiões em que determinados fatores ou acontecimentos, designados por sinais de alarme, podem suscitar interrogações na pessoa que constata ou assiste, nomeadamente, o comportamento de um indivíduo, um documento ou uma transação e até mesmo uma atividade no sistema ou na instituição fora do comum. De acordo com a sensibilidade da pessoa em causa, o incidente pode ser acompanhado ou pode ser ignorado e, conseqüentemente cair em esquecimento. O “sinal de alarme” é um indicador de um potencial problema, podendo incluir a fraude, e é classificado segundo quatro categorias: comportamental, transacional, sistema e organização, sendo que cada categoria pode ser classificada segundo a sua forma de deteção, isto é, reativa, caso seja detetada sem recurso a um sistema de deteção, ou pró-ativa, caso seja detetada com recurso a um sistema de deteção.

“O reconhecimento de sinais de alarme por parte dos colaboradores e dos responsáveis de uma instituição é facilitado com a existência de formação nesse sentido, a qual permite aumentar a sensibilidade e, conseqüentemente, a possibilidade dos trabalhadores reconhecerem os sinais de alarme e saberem como agir em cada situação” (Iyer e Samociuk, 2006).

7.6 Risco e Probabilidade de Ocorrência

É importante garantir que os riscos aos quais determinada instituição está exposta são analisados de forma consistente, o que é feito, geralmente, através da avaliação da frequência, isto é, da probabilidade de ocorrência de um acontecimento, e do impacto consequente, inerentes a cada situação de risco. No entanto, o processo de análise de risco não especifica a forma como a probabilidade de ocorrência e o impacto de cada situação de risco devem ser calculados, pelo que a avaliação pode ser feita a nível quantitativo, isto é, recorrendo ao uso de uma escala numérica, ou a nível qualitativo, isto é, recorrendo ao uso de uma escala descritiva.

	Impacto			
Frequência*	Baixo	Médio	Elevado	Severo
Baixa	Baixo	Baixo	Baixo	Médio
Média	Baixo	Médio	Médio	Elevado
Elevada	Baixo	Médio	Elevado	Severo

➔ Nível de Risco

* Probabilidade de ocorrência

Quadro 3 – Matriz de Risco Standard
 Fonte: Adaptado de Iyer e Samociuk, 2006

O Quadro 3 ilustra “as classificações possíveis para a probabilidade e o impacto, que permitem aferir o nível de risco, independentemente da escala que é dita em conta na avaliação do mesmo” (Iyer e Samociuk, 2006).

7.7 Construção de Perfil de Risco

“O processo de redução de risco numa instituição passa, também, pela construção de perfis de risco, que permitem definir os responsáveis pela gestão de risco tendo em conta o nível de risco determinado para cada situação. Consoante o nível de risco assim se define os responsáveis pela sua gestão e consequentemente, os métodos e as técnicas inerentes ao processo de avaliação e prevenção da fraude.

A construção de perfis de risco permite tornar mais visível e quantificável o risco inerente às situações de fraude, facilitando os métodos e as técnicas que ajudam na sua gestão e, conseqüentemente, a reduzir custos” (Iyer e Samociuk, 2006).

O processo de construção de um perfil de risco implica três etapas, nomeadamente, o levantamento de situações de risco, a avaliação do nível de risco para cada uma das situações de risco identificadas, através da probabilidade e do impacto inerentes a cada uma delas, e, por último, a hierarquização das referidas situações, conforme ilustra o esquema apresentado pela Figura 16. “A hierarquização é feita segundo o nível de risco, sendo que, quanto maior o nível de risco associado a determinada situação, os responsáveis pela sua gestão são os gestores de topo e auditoria. Em contrapartida, quanto menor o nível de risco associado a determinada situação, a responsabilidade da sua gestão deve ser assegurada pela gestão de rotina ao nível da área operacional” (Iyer e Samociuk, 2006).



Figura 16 – Construção de Perfil de Risco
Fonte: Adaptado de Iyer e Samociuk, 2006

7.8. Procedimentos e Prevenção da Fraude no Sistema Bancário

Em todas as partes do mundo têm sido desenvolvidos modelos que pretendem detetar e prevenir a existência de fraude no mercado de trabalho. “Governos, órgãos reguladores e entidades comerciais consideram, cada vez mais, as melhores medidas práticas para prevenir a fraude” (Cafferty, 2003).

Existem medidas organizacionais que podem e devem ser levadas em consideração para minimizar o risco de fraude, que em muitos casos, passa mesmo despercebido, sendo que a avaliação do risco de fraude pode revelar-se uma eficaz ferramenta pró ativa na luta contra a fraude em qualquer negócio.

“As entidades reguladoras e as autoridades policiais têm enfatizado o papel crucial que a avaliação do risco de fraude desempenha no desenvolvimento e manutenção de programas eficazes de gestão de risco de fraudes e controles. A identificação prévia de situações de risco de fraude permite evitar problemas em detrimento da ocorrência de fraude” (*Association of Certified Fraud Examiners, 2009*).

As eventuais situações de fraude representam um risco que não deve ser ignorado, uma vez que qualquer organização que não adote medidas para se proteger ou que não atue de acordo com os procedimentos disponibilizados, por exemplo, por entidades reguladoras, enfrenta uma maior vulnerabilidade face a situações de carácter fraudulento.

“Desta forma, dado que a luta contra a fraude tem-se revelado uma prioridade das entidades reguladoras, que desenvolvem técnicas antifraude, é da responsabilidade e da consciência de cada organização adotar e cumprir os diferentes procedimentos e as diferentes normas” (*Cafferty, 2003*).

A gestão de risco de uma instituição revela-se particularmente importante no que diz respeito, ao combate e à prevenção da fraude. É importante que exista uma estratégia definida, objetiva e clara, que assente na compreensão, na redução e na deteção de risco, criando um ambiente favorável à avaliação e à prevenção da fraude, complementado por normas e procedimentos externos publicados, nomeadamente, pelo Banco de Portugal, bem como por normas e procedimentos internos comumente conhecidos e aceites por todos os colaboradores. Ainda que a gestão de risco de fraude seja definida a partir do topo, e também, segundo normas e procedimentos externos à instituição, é importante garantir que os diferentes colaboradores que exercem na instituição estejam inseridos na estratégia de combate à fraude.

8. Auditoria e Compliance

A palavra “*Compliance*” vem do verbo inglês “*to comply*”, que significa “cumprir, executar”. Na prática implica concordância, tem como propósito acatar o espírito das leis, regulamentos, normas internas ou externas. Visa impedir o não cumprimento, é sinónimo de qualidade. “*Compliance*” não tem funções de fiscalização mas tem de criar controlos que lhe permita monitorizar as operações que a organização efetua. Deve certificar-se de que os colaboradores fazem o que devem. O objetivo é evitar falhas. Claro que é difícil existir uma organização à prova de falhas mas a preocupação de as evitar deve ser constante. Só assim se garantirá um desempenho de qualidade, consiste na confiança nos processos, na transparência dos procedimentos e na ética profissional, sendo um conceito muito importante para a estrutura organizacional de uma instituição financeira.

A missão do “*compliance*” é assegurar a adequação, fortalecimento e funcionamento do sistema de controlo interno das instituições financeiras, em articulação com os demais órgãos da instituição. Procura assim, mitigar os riscos de acordo com a complexidade dos negócios e disseminar a cultura de controlos para assegurar o cumprimento das leis e regulamentos existentes. Através de monitorização permanente, procura amenizar, o risco decorrente de:

- ✓ Conformidade com leis e regulamentos
- ✓ Conformidade com códigos de conduta, práticas instituídas ou princípios éticos
- ✓ Responsabilidade perante terceiros
- ✓ Grau de transparência
- ✓ Envolvimento em operações de branqueamento capitais

“O *Compliance Office*, tem por missão assegurar que os órgãos de gestão, as estruturas funcionais e todos os Colaboradores do Grupo cumpram a legislação, regras e normativos (internos e externos) que pautam a atividade do Banco e as suas associadas, de forma a evitar o risco de a Instituição incorrer em sanções de carácter legal ou regulamentar e em prejuízos financeiros ou de ordem reputacional, decorrente do incumprimento das leis, códigos de conduta e regras de “boas práticas” negociais e deveres a que se encontram sujeita”. (*Informação institucional BCP*)

“O *Compliance Office* integra como seus objetivos o respeito pelas disposições legais e regulamentares aplicáveis, incluindo as relativas à prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como das normas e usos profissionais e deontológicos, das regras internas e estatutárias, das regras de conduta e de relacionamento com Clientes, das orientações dos órgãos sociais e das recomendações do Comité de Supervisão Bancária de Basileia e do Comité das Autoridades Europeias de Supervisão Bancária (CEBS), de modo a proteger a reputação da Instituição e a evitar que esta seja alvo de sanções, conforme estabelecido no Art. n.º 2, alínea c) do Aviso 5/2008 do Banco de Portugal (BdP)”.(Informação institucional BCP)

A Auditoria Interna efetua seus trabalhos de forma aleatória e temporal, por meio de amostragens para se certificar do cumprimento dos processos e das normas instituídos pelos dirigentes máximos da organização, já o “*Compliance*” executa tais atividades de forma rotineira e permanente, monitorizando-as para assegurar, de maneira corporativa e tempestiva, que as diversas unidades da instituição estão a respeitar as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para prevenção e controlo dos riscos envolvidos em cada atividade e em cada momento.

“*Compliance*” é um grande apoio dos órgãos reguladores junto à administração no que se refere à preservação da boa imagem e reputação e às normas e controlos na busca da conformidade. Deve ser também tão independente quanto a auditoria interna, dirigindo-se aos dirigentes superiores da organização para informá-los de eventos que representem riscos para a instituição, principalmente risco de “*compliance*”, neste sentido, faz parte da estrutura de controlos, enquanto a auditoria avalia essa estrutura. Assim, a área de “*compliance*”, deve ser objeto de avaliação da auditoria interna. Auditar “*compliance*”, constitui excelente oportunidade para a compreensão do seu processo na instituição, isto é, para a avaliação da cultura de conformidade e do grau de comprometimento dos profissionais.

O risco de “*compliance*” é supervisionado pela atividade de Auditoria Interna, em grande parte dos casos, no entanto, tem-se autonomizado devido à exigência dos organismos reguladores e da necessidade da própria entidade no controlo de risco, levando os departamentos de “*compliance*” e de Auditoria Interna a perfilarem-se ao mesmo nível, assumindo uma relação de complementaridade.

O departamento de “*compliance*” poderá ser supervisionado pela Comissão de Auditoria ou por uma “*Comissão específica de Compliance*”, conforme nos é mostrado na figura seguinte:

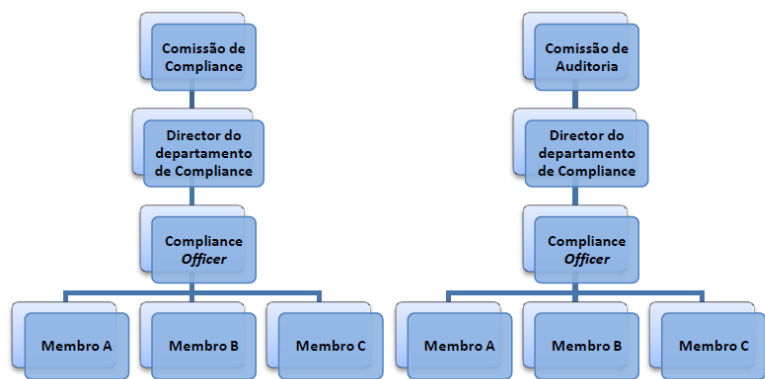


Figura 17: Exemplos de Modelos alternativos de supervisão de compliance
Fonte: *Auditoria Interna, Função e Processo*, 3ª Edição, Georgina Morais e Isabel Martins, Página 114

Os auditores internos devem desenvolver a existência de uma função de “*compliance*” organizada. Somente se o Auditor estiver inteirado das atividades desenvolvidas pelo “*compliance*”, é que poderá executar o seu trabalho, com o estabelecimento de um trabalho coordenado e em parceria, onde e aquando das visitas, a Auditoria possa munir-se das informações relevantes, especialmente sobre o resultado da identificação e avaliação dos controlos e riscos.

A Auditoria Interna ao executar um trabalho complementar, com o objetivo de avaliar a adequação da entidade e de seus colaboradores às normas legais e procedimentos de “*compliance*”, pretende evitar futuros pontos de atrito com a auditoria externa ou quaisquer Órgãos Reguladores, zelando assim, pela imagem da entidade. Os Auditores Internos devem avaliar se os programas de “*compliance*” ajudam as entidades a⁴³:

- ✓ Prevenir violações inadvertidas pelos empregados;
- ✓ Detetar atividades ilegais;
- ✓ Desincentivar violações não intencionais dos empregados;
- ✓ Comprovar reclamações;
- ✓ Determinar a responsabilidade de diretores e executivos;

⁴³ Auditoria Interna, Função e Processo, 3ª Edição, Georgina Morais e Isabel Martins, Pág. 115

- ✓ Criar ou melhorar a identidade corporativa;
- ✓ Decidir se uma indemnização por danos e prejuízos é apropriada.
- ✓ A entidade estabeleceu normas e procedimentos de “*compliance*” capazes de minimizar a possibilidade de conduta ilícita.
- ✓ Foi atribuída a responsabilidade específica à pessoa ou pessoas, posicionada ao nível hierárquico, de supervisionar o “*compliance*” com as normas e procedimentos regulamentares.
- ✓ Não foi delegada a responsabilidade discricionária e relevante a pessoas com tendência para atividades ilegais.
- ✓ Se existe uma comunicação eficaz das normas e procedimentos a toda a entidade e outros agentes.
- ✓ Se a entidade tomou diligências necessárias para cumprir com as normas, utilizando sistemas de vigilância e auditoria razoavelmente concebidos para detetar condutas ilícitas por parte dos empregados ou agentes, pondo em prática e publicitando um sistema de informação na qual os empregados e outros agentes podem denunciar a conduta ilícita, através de linhas abertas de *hotline*, de outros dentro da entidade, sem temer represálias.
- ✓ Se as normas são aplicadas de forma consistente, mediante mecanismos disciplinares apropriados, incluindo, quando apropriado, as sanções para as pessoas responsáveis por não terem detetado o delito, e se é adequada ao delito praticado.
- ✓ Se a entidade responde adequadamente ao delito detetado a fim de evitar repetições de violações idênticas, incluindo modificações ao programa de “*compliance*”, se necessário.

Em forma de conclusão poderemos resumir que a Auditoria realiza trabalhos periódicos com metodologia específica, por seu lado o “Compliance” atua no dia-a-dia e insere-se num contexto de cultura organizacional.

Outra questão bastante pertinente decorre do fato de uma organização ou instituição, ao longo da sua vida se deparar com diversas situações que podem influenciar a tomada de decisões e até a forma operacional de laborar. Estas situações podem advir de circunstâncias intrínsecas da empresa (fatores endógenos) ou então de circunstâncias externas à empresa, sobre as quais a mesma não tem qualquer controlo (fatores exógenos). Ora o mesmo acontece na tomada de posição por parte de um auditor, relativamente à continuidade de uma empresa.

Tais situações estão identificadas e enumeradas ISA 570: “a dependência excessiva de empréstimos a curto prazo para financiar ativos de longo prazo; indicações de retirada de apoio financeiro por credores; perdas operacionais substanciais ou deterioração significativa no valor dos ativos usados; incapacidade de cumprimento das condições dos acordos; perda dos principais gestores sem substituição; perda de um grande mercado, do(s) principal(ais) cliente(s), de uma concessão, de uma licença ou do(s) principal(ais) fornecedor(es); aparecimento de um concorrente com grande sucesso; alterações na legislação, regulamentação ou na política governamental e, catástrofes não cobertas ou insuficientemente cobertas por seguros” (ISA 570, §A2).

O despoletar da crise económico-financeira, designada por “*Subprime*”, iniciada nos EUA e propagada pela Europa, voltou a colocar em causa o sistema financeiro e levou a colocar mais uma vez em causa a credibilidade das opiniões emitidas pelos auditores (e suas administrações), relativamente à continuidade das empresas em análise. O caso mais alarmante foi sem dúvida, a falência do Banco Lehman Brothers. “Todas as opiniões emitidas pelos auditores responsáveis, pela execução dos trabalhos, não revelaram quaisquer incertezas sobre a continuidade da entidade bancária. Este fato foi tido em conta por parte do Ministério Público dos EUA, responsabilizando a empresa de auditoria por induzir em erro os clientes e investidores do Lehman Brothers” (Diário Económico e Agência Lusa, 2010).

Atendendo a esta e a outras situações idênticas, a sociedade em geral começou a questionar qual a credibilidade e qual a utilidade dos relatórios e certificações emitidas pelos auditores e revisores de contas, em especial no que respeita à continuidade.

“Neste sentido, um dos organismos responsáveis pela atividade de auditoria, o IAASB, emitiu um alerta de boas práticas intitulado Considerações de Auditoria respeitantes à continuidade no atual ambiente económico, providenciando alguns tópicos guia para a avaliação da gestão das asserções de continuidade, atendendo ao que consta na ISA 570 – Going-Concern” (Chi, 2009).

Por outro lado, o potencial conflito de interesses que possa existir na conceção da informação, entre os gestores e os vários intervenientes na sociedade, acionistas e/ou investidores, dá-se o nome de Teoria da Agência, esta teoria explica a “relação existente de agência estabelecida entre um principal (proprietário) que delega num agente (gestor) a decisão e execução de uma determinada função/ação” (Borralho, 2007, p. 15).

“A diferença entre o proprietário (acionistas/sócios) e o gestor (administradores/gerência) devem-se a objetivos diferentes que cada um tem, enquanto os acionistas pretendem a maximização da rentabilidade do capital investido, maximizando o valor da empresa, os gestores pretendem reduzir o esforço despendido com o desempenho das suas funções e a maximização da sua remuneração” (Borrvalho, 2007).

Levanta-se aqui um problema de idoneidade da gestão, atendendo à importância do papel que esta desenvolve. Esta questão toma uma relevância ainda maior, quando está em causa a possibilidade de emissão por parte do auditor de uma opinião sobre continuidade. Pois, perante tal, interessa saber quais as opiniões, decisões futuras e explicações da situação atual e do futuro da entidade ou parte dela, de acordo com, o que nos é dito por Ryu e Roh (2007).

É perceptível que a emissão de uma opinião sobre continuidade por parte do auditor seja algo de extrema importância e de enorme dificuldade, basta pensar que estamos a alertar todos os utilizadores para a possibilidade de num prazo relativamente curto a entidade incorrer em situações que podem colocar em causa subsistência e continuidade da mesma o que, teoricamente pode afastar investidores, financiadores e clientes. Atende-se a que, em todo este processo, o auditor deve ser uma entidade independente e isenta na prossecução das suas tarefas, de acordo com a sua ética, deontologia e normativos legais a que está sujeito e, por isso, não se espera que tome o posicionamento de defensor da empresa. No entanto, sendo uma decisão que pode influenciar bastante o comportamento dos *stakeholders* a mesma terá que ser ponderada por parte do auditor.

Por outro lado, existe outro aspeto importante, que é o fato de o auditor ser colaborador (auditor interno) da própria entidade, sendo a mesma a efetuar o pagamento dos honorários, e daqui poder existir alguma influência por parte da gestão/administração da empresa na opinião do mesmo, com especial relevo, no que toca à continuidade. Isto porque, existe aqui uma relação de cliente versus prestador de serviços, em que o interesse do auditor em manter o seu cliente pode-se sobrepor à da responsabilidade e ao cumprimento dos deveres e obrigações a que está sujeito. Para além do incumprimento de normas e regras de índole profissional, indo contra a ética e deontologia da profissão, estas situações de interferência da vontade dos clientes no trabalho dos auditores e da informação a constar da sua opinião, coloca em causa o trabalho do auditor.

Concluindo-se que, perante fatos que coloquem em causa a continuidade da empresa, o auditor deve assegurar a divulgação de⁴⁴:

- ✓ Condições e eventos pertinentes que colocam em causa a continuidade da empresa;
- ✓ Potenciais efeitos dessas condições e eventos;
- ✓ Avaliação por parte da gestão destas condições e eventos;
- ✓ Possibilidade de descontinuidade da atividade;
- ✓ Planos da gestão

⁴⁴ Boynton et al, 2006

9. *Investigação*

Metodologia

A escolha da metodologia aplicada neste trabalho teve como objetivo, compreender o ambiente de controlo existente nas instituições financeiras, bem como o papel desempenhado pela auditoria no incremento de valor e gestão dos riscos inerentes aos processos de negócio. Neste sentido foi elaborado um questionário (capítulo 12 - anexos), o qual foi divulgado junto dos colaboradores de várias instituições de crédito nacionais, com dimensão, territorialidade e complexidades distintas, junto da “família” de auditoria interna – IPAI, e classe académica da área de estudo. Com base nos objetivos pretendidos e de acordo com a disponibilidade dos seus colaboradores (de forma anónima), enumeramos as instituições que deram o seu contributo para este trabalho:

- BANIF - BES
- BCP - BIC
- BPI - CCAM
- CGD - MONTEPIO

O inquérito foi desenvolvido de forma a recolher informações sobre temas como risco operacional, ética, conflitos interesse e fraude, junto dos colaboradores das instituições financeiras a operar em Portugal, tentando obter por um lado, uma perspetiva dos intervenientes sobre os temas enumerados e quais as repercussões que tem na entidade onde colaboram, contrapondo á posição da auditoria cada vez mais limitada pela imperatividade das sociedades em obter a máxima eficiência dos recursos, numa crescente crise económica e de valores que se verifica na sociedade.

A recolha de respostas foi efetuada de forma aleatória simples, uma vez que o formulário foi enviado diretamente para as instituições devido a contatos institucionais existentes, com a colaboração do “IPAI”, divulgando junto dos associados através do seu portal, pela instituição de ensino (ISCAC) de acordo com os meios institucionais existentes para a divulgação de informação junto dos alunos e interessados nas matérias abordadas.

Segundo Bacelar (1999), “as amostras aleatórias simples apresentam algumas vantagens, como sejam os menores custos envolvidos e o fato de tenderem a assegurar amostras representativas e estatisticamente significativas”. “Para além destas vantagens, por vezes apresenta-se ao investigador como único método possível, em amostras grandes e representando populações homogêneas, este método é eficaz” (Drew e Hardman, 1995)

“As suas desvantagens, por um lado, decorrem do não conhecimento minucioso dos estratos da população à partida e logicamente, da não distribuição equitativa destes na amostra formada” (bacelar, 1999). Verifica-se, ainda que nas Ciências Sociais e humanas se torna frequentemente difícil especificar os indivíduos na sua globalidade, nem mesmo fazê-lo de acordo com as suas categorias de pertença, ou seja, estratos.

Neste sentido, a primeira parte visa enquadrar o entrevistado em termos de exercício da atividade profissional, englobando idade, experiência profissional, grau académico e dimensão da empresa que representa.

A segunda parte aborda os entrevistados sobre a representatividade da auditoria na entidade, se fazem parte da área, se existe Comité de auditoria, bem como a possibilidade de a sociedade recorrer a serviços de auditoria externa.

Numa fase posterior o inquérito aborda a sensibilidade dos colaboradores perante os Auditores, nomeadamente ao nível dos seus conhecimentos, prioridades, características pessoais e profissionais, bem como a forma e metodologia de desenvolver o seu trabalho junto das sucursais.

De seguida, questões destinadas a perceber o que leva os colaboradores das entidades financeiras a cometer fraude e quais os procedimentos adequados para a sua prevenção e detenção, se os mesmos têm uma maior probabilidade de sucesso se forem efetuados de forma mais frequente ou com recurso auditorias externas.

Por ultimo a questão dos colaboradores, a sua motivação e postura perante a difícil conjuntura atual de exigência a nível comercial, pessoal e social. Que papel tem a auditoria nos trabalhos desenvolvidos junto das sucursais, que objetivos e mais valia incrementam.

Resultados e Considerações

Dos resultados obtidos na primeira parte do inquérito podemos evidenciar uma heterogeneidade de idades, níveis académicos e anos de experiência, bem como a dimensão e complexidade da entidade onde colaboram, o que evidencia a pluralidade existente nas instituições financeiras. De referir que a grande maioria das respostas obtidas foram efetuadas por colaboradores com experiência profissional superior a 5 anos (75% das respostas), e que a grande maioria nunca exerceu funções de auditoria (68%), baseando-se o trabalho fundamentalmente na área comercial e operacional das Instituições.

Como conclusões da 2ª parte do inquérito, verificamos que os colaboradores têm a perceção que os reguladores têm encorajado as instituições financeiras a validarem de modo independente os respetivos modelos de gestão de risco, para melhor avaliarem a probabilidade e magnitude dos riscos potenciais. Verifica-se assim que a função da Auditoria (Interna) está hoje intimamente ligada à gestão de risco, dado que é esta função que permite à gestão de topo ter acesso a um conjunto de informações que a auxiliarão numa eficaz tomada de decisões sobre a forma como deverá ser encarada a abordagem do negócio bem como fazer face ao risco inerente da atividade. As respostas evidenciam que as instituições onde colaboram têm uma preocupação bastante grande a nível de Ambiente de controlo e políticas de gestão de risco, detendo departamentos de auditoria interna (gráfico 1), bem como a necessidade (ou obrigatoriedade) de recorrer a serviços externos.

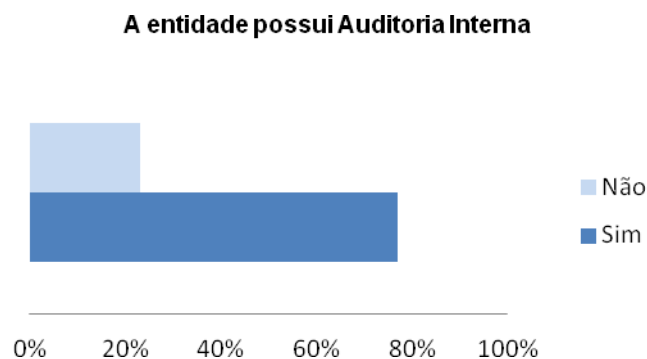


Gráfico 1: A entidade possui Auditoria interna

O Gráfico 2 evidencia (74% das respostas afirmativas), que as instituições de crédito para além de possuir departamentos de auditoria interna, recorrem a trabalhos de auditoria externa, tal fato prende-se pela imposição dos normativos e leis definidas pelas instâncias de controlo, bem como a necessidade de as instituições apresentarem dados e resultados credíveis juntos dos *Stakeholders* e demais interessados.

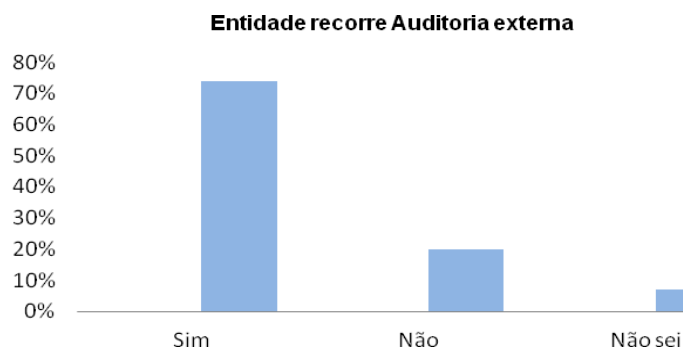


Gráfico 2: Utilização Auditoria externa pelas Entidades

O atual ambiente em que se desenvolvem os negócios, em constante mudança, imprevisível e volátil, com fortes pressões económicas, está exposto a uma enorme variedade de riscos – flutuações de taxas de juro, dificuldade de acesso ao crédito, *Ratings* de crédito, imparidades, riscos operacionais, “*Compliance*”, fraude, desastres naturais, entre muitos outros. Cada um destes riscos pode trazer benefícios ou prejuízos para as organizações, mas a sua gestão é cada vez mais complexa e exige que os decisores tenham disponível informação relevante e atempada para que possam tomar as decisões mais acertadas.

O sistema de gestão de riscos deve ser proporcional à dimensão, natureza e complexidade da atividade da instituição, tomando nomeadamente em consideração a natureza e magnitude dos riscos que a mesma assume e ou pretende assumir. No normal desenvolvimento das suas atividades de negócio, todas as organizações gerem riscos, e oportunidades.

A informação recolhida deve ser adequadamente corporizada e integrada na cadeia de valor da organização e respetivos processos de negócio, considerando uma ótica “*End-to-End*”, acrescentando valor ao nível de:

- ✓ Planeamento estratégico;
- ✓ Gestão da performance;
- ✓ Gestão de Capital (*Opex* e *Capex*);
- ✓ Decisão de investimento;
- ✓ Planeamento, controlo e tomada de decisão.

Deve ser criado ou reforçado o sistema de comunicação interna, quer ao nível horizontal quer ao vertical, baseada na divulgação a toda a organização, da missão, dos valores, do conteúdo, bem como dos níveis de responsabilidade, atribuições e explicação das motivações que originaram a criação do departamento de auditoria interna. No entanto devido ao *stress* diário das Instituições, oriundo da exigente agenda comercial bem como o volume de Informação recebida diariamente (sob forma de comunicações internas, procedimentos, normas e regulamentos), a complexidade e número de transações efetuadas, os valores envolvidos e meios cada vez mais informatizados, conjugados com motivação acrescida pela conjuntura/necessidade atual da sociedade e colaboradores, leva a que a auditoria tenha que ter uma posição presente e proactiva perante o risco. Neste sentido os trabalhos de acompanhamento e revisão adotam uma periodicidade mais regular esperando-se atingir uma revisão contínua e constante (melhoria contínua será o grande objetivo das instituições para superar períodos em que a sua subsistência é colocada em causa). O auditor interno deve ser um componente ativo da organização da gestão interna, fazendo com que as diversas observações e informações recolhidas no trabalho de campo sejam úteis e essenciais na procura de uma adequada gestão de recursos. A sua opinião e visão crítica dos procedimentos e processos devem estar fundamentadas em evidências que proporcionem aos gestores a exata mensuração das técnicas utilizadas na gestão do negócio, em que a forma de expressão do auditor, quer oral quer escrita, pode alterar a aceitação de mudanças no rumo estipulado por parte da gestão. Neste sentido, o auditor interno deve desempenhar a sua atividade com visão holística e proactiva, antecipando-se aos factos, de modo que a sua opinião seja de fundamental importância nas escolhas da organização. Deverá também, ao mesmo tempo estar atento a novas tendências no mercado em que a sua organização opera.

A sua participação na gestão operacional deve ir muito além de uma “fiscalização” sobre os processos, atuando em sintonia com as solicitações do mercado, bem como com metas e estratégias bem delineadas, que é essencial para a sobrevivência organizacional. As respostas obtidas demonstram que as instituições referenciadas apresentam trabalhos de auditoria nas sucursais, com periodicidades reduzidas, 70% das respostas indicam que os mesmos são efetuados anualmente, no entanto as restantes respostas não ultrapassam os três anos (gráfico 3). No entanto não se conhece resultados sobre os que são efetuados a distância, ou seja pela entidade sem que a área comercial tenha conhecimento, sem necessidade de deslocar efetivos junto das sucursais. Esta situação prende-se pelo fato de cada vez mais se ponderar uma relação custo/benefício dos trabalhos desenvolvidos pela auditoria, bem como a implementação de procedimentos (auditoria/controlo interno/*compliance*) junto das áreas comerciais, para diminuir o risco operacional, como exemplo, temos a digitalização de documentos e contratos, o que simplifica a verificação e controlo de processos. Tal situação tem benefícios nomeadamente ao nível de “*compliance*” e procedimentos, com reconhecidos proveitos de tempo e custos para a Instituição, no entanto sobrecarrega a área comercial com trabalho administrativo, numa cada vez mais exigente conjuntura a nível objetivos comerciais.

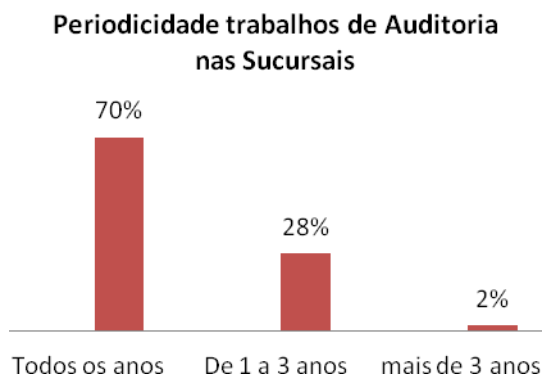


Gráfico 3: Periodicidade Trabalhos Auditoria Sucursais

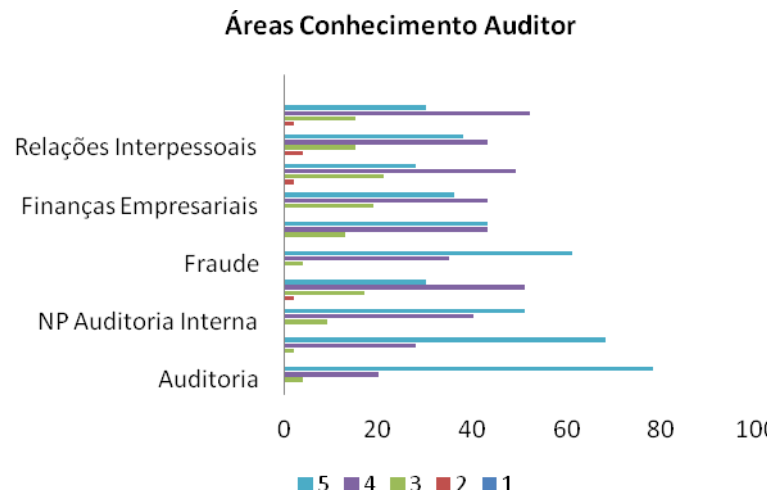


Gráfico 4: Áreas de Conhecimento Auditor das Organizações aquando dos trabalhos a executar

No exercício das suas funções o auditor terá que para além dos conhecimentos técnicos e profissionais que adquiriu anteriormente (normas e procedimentos de Auditoria), valer-se de todo o tipo de informação que pode influenciar a entidade que vai analisar, neste sentido informações como as relações interpessoais e empresariais, o meio onde se encontra inserido (indicadores sociais e pessoais) bem como procedimentos e métodos de prevenção e deteção de fraude são muito importantes (de acordo com respostas obtidas) como forma de mitigar os riscos associados à entidade (gráfico 4). O objetivo de uma arquitetura de risco é identificar, avaliar, controlar e mitigar este risco, bem como desenvolver reporte efetivo e enfrentar desafios emergentes. Neste sentido a metodologia de auto-avaliação (*self-assessments*) constitui um elemento integral desta arquitetura, pois fornece uma excelente oportunidade para as instituições integrarem os processos de identificação de riscos e o programa de gestão de risco de uma forma mais geral, com vista a melhorar a compreensão e o controlo dos seus riscos (operacionais). Os “*self-assessments*” podem ser utilizados igualmente como um método para identificar falhas em controlos passíveis de ameaçar a concretização de objetivos de processos ou de negócio e controlar as medidas que a gestão está a desenvolver a fim de reduzir estas falhas. Com base nos seus resultados, podem ser construídos planos de acção para mitigar riscos e melhorar controlos. A implementação do CSA – “*Control Self Assessment*” - surge como uma ferramenta inovadora e capaz de otimizar os recursos da auditoria interna e da organização como um todo.

O CSA pode ser visto como um processo de avaliação dos controlos internos, sendo uma abordagem simples para as partes envolvidas. Enquanto alguns profissionais olham para a avaliação do risco e dos controlos internos do COSO como um processo demasiado complexo e difícil de entender, o CSA é uma abordagem onde departamentos específicos numa organização podem comunicar, num ambiente de grupo facilitado (*workshop*), avaliando os riscos e controlos internos dentro do seu departamento ou função. É um processo desenhado para ajudar os departamentos dentro de uma organização a avaliar os seus controlos internos. Em muitos aspetos, a abordagem do CSA usa os mesmos conceitos encontrados no *framework* de controlo interno do COSO. O modelo defende que uma organização deve implementar fortes objetivos de controlo e atividades de controlo, para que exista um forte ambiente de controlo. Estes dois elementos são rodeados por um bom sistema de informação e comunicação bem como de processos para avaliação de risco para monitorizar a performance.

Deverá servir como *guideline* para o comportamento organizativo no que ao controlo interno diz respeito. Deverá adotar uma postura proactiva e por vezes agressiva em relação a comportamentos e processos obsoletos, a capacidade de quebrar rotinas poderá fazer a diferença e levar a organização para uma nova fase evolutiva, inculcando uma cultura de controlo em toda a organização. No entanto um dos elementos mais importantes a ter em conta na criação e condução de um projeto de CSA é a criação de processos de comunicação efetivos e eficientes na medida em que o *timing* em que é feita a comunicação de conclusão de determinada fase do projeto pode contribuir de forma decisiva para o sucesso da fase seguinte.

Com a utilização do CSA os recursos das áreas operacionais são dinamizados, de uma forma simplista, pode-se dizer que a auditoria interna orienta a área operacional para esta avaliar os seus processos, identificar os riscos e propor ações de melhoria que mitiguem os riscos identificados. De uma forma natural as equipas operacionais passam a utilizar terminologias até então desconhecidas e a palavra risco passa a ser vista não só com a natural conotação negativa mas também como uma oportunidade de melhoria. A identificação prematura de riscos processuais passa de um fator negativo com culpabilização nominal para uma procura constante de oportunidades de melhoria nos processos.

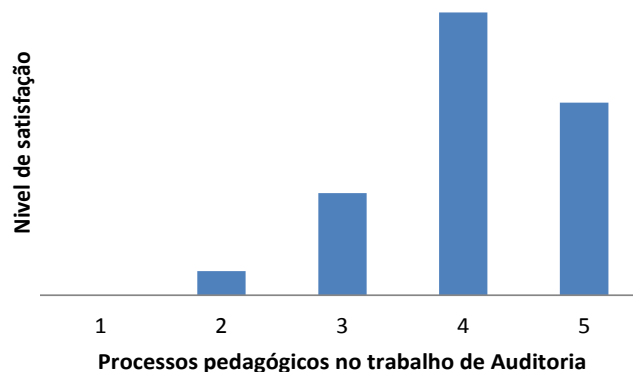


Gráfico 5: Processos Pedagógicos versus Satisfação colaboradores

“A atividade bancária continua a desenvolver-se num contexto particularmente adverso e exigente do ponto de vista macroeconómico, financeiro e regulamentar, que coloca desafios assinaláveis sobre todos os níveis. Um dos maiores desafios da gestão de recursos humanos num período como o que atravessamos é manter uma equipa

coesa, motivada e mobilizada para a concretização dos objetivos. Por outro lado a questão da retenção dos talentos e a garantia de manter nas equipas os melhores colaboradores e fundamental para a sobrevivência das instituições” (inforbanca)⁴⁵.

O foco incide cada vez mais na capacidade de a organização como um todo enfrentar os riscos e apresentar ações de melhoria constante, criando uma responsabilidade de controlo em cada colaborador para benefício não só da organização, mas também dos seus objetivos individuais, elevando assim a motivação e satisfação, com repercussões ao nível de desempenho individual e por inerência da organização (gráfico 5). O trabalho do auditor devera ser visto pelos colaboradores de uma forma construtiva, sendo incluído nos mesmos a vertente pedagógica, ao contrário da visão tradicionalista de “fiscal” do auditor.

O gráfico 5 demonstra pelas respostas apresentadas que para além das funções de prevenção e deteção o trabalho do auditor deve incluir a componente pedagógica, aumentando a satisfação dos colaboradores com incrementos reconhecidos nos processos e resultados da entidade. Podemos aferir que um dos aspectos mais importantes para o auditor se relacionar bem com o auditado é a empatia, assim terá de conjugar atributos profissionais e pessoais como forma de identificar oportunidades de melhoria nos processos e a busca da satisfação do cliente (interno e externo). Os atributos profissionais são os conhecimentos relativos ao desempenho da atividade de auditoria, aliado à experiência profissional no processo a ser auditado, os atributos pessoais são as habilidades e aptidões que dão suporte ao auditor para um bom desempenho da sua função. Os atributos pessoais necessários a um auditor são baseados no bom relacionamento interpessoal que ele deve utilizar com a finalidade de passar e obter a confiança dos auditados.

Houve uma transição da auditoria baseada em sistemas para a auditoria baseada em processos, e atualmente sobretudo por razões de custo e eficácia, a ênfase está na Auditoria Baseada em Riscos (ABR). O auditor deve obter conhecimento suficiente dos sistemas de controlo interno implementados na organização de forma que lhe permita planear o seu trabalho e determinar a natureza, o momento e o alcance dos testes a realizar. Tal avaliação permite diminuir os testes de substanciação a efetuar e por conseguinte diminuir o tempo de realização do trabalho. Enquanto o controlo interno oferece uma perspetiva dinâmica e valorizadora que permite manter o domínio, a Auditoria avalia o grau de domínio alcançado.

⁴⁵ Jorge Tomé, Presidente Comissão executiva Banif - Inforbanca Out/Dez 2013,

A organização forma um todo (sistemas, organizações, funções, operações, ativos e passivos) que deverá estar sob controlo interno e potencialmente sujeita a Auditoria. Embora o governo das sociedades seja definido e regulamentado de diferentes formas em todo o mundo, organizações de todas as dimensões, atividades e países estão de acordo quanto aos seus objetivos principais: auxiliar os líderes a manter organizações sustentáveis, merecedoras da confiança do mercado e capazes de retornar o valor do investimento aos seus accionistas. A Auditoria Interna tem um papel importante na avaliação da eficácia da gestão de risco na organização. Deve avaliar com regularidade a eficácia dos controlos internos relativos à quantificação, informação e limitação dos riscos. A avaliação dos diferentes riscos ajudam a Auditoria Interna a definir o seu plano de trabalho, uma vez que lhe permite determinar quais são as áreas de maior risco, isto é, as áreas prioritárias e sobre as quais devem recair todas as atenções, portanto, as que devem ser analisadas primeiro.

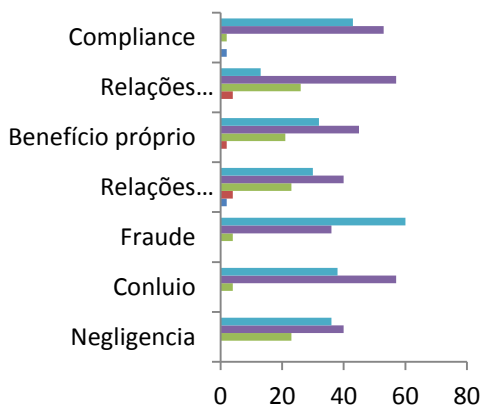


Gráfico 6: Temas de trabalho e sua prioridade

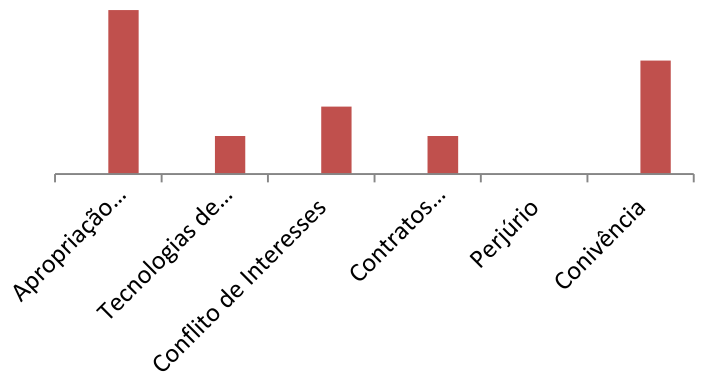


Gráfico 7: Tipos de Fraude mais frequentes

Todo o trabalho de AI deverá ter como ponto de partida um detalhado e exaustivo planeamento de todas as tarefas a efetuar, pois é a partir daqui que se consegue delinear a estratégia a seguir para a consecução dos objetivos estabelecidos. Nesta fase deverá ser delineado um plano de ações de forma a cobrir com transversalidade todas as áreas da entidade onde exista risco associado, não fazendo sentido do ponto de vista operacional e monetário, alocar recursos a um setor onde o risco seja materialmente irrelevante (eficiência de recursos).

O conhecimento do auditor nas mais variadas áreas que englobam a complexidade do negócio, bem como a sua priorização ficam bem patentes no gráfico 6, sendo o “*Compliance*”, relações interpessoais e a fraude, fatores prioritários no trabalho a desenvolver.

“O mundo dos negócios revela-se muito competitivo e, conseqüentemente, os funcionários manifestam sintomas relacionados com o *stress*, o que resulta em sentimentos associados à sensação de não reconhecimento do trabalho que desenvolvem na instituição onde exercem funções. Com a existência de problemas pessoais e de falhas existentes no controlo interno, a motivação para a prática de atos fraudulentos, por parte dos funcionários, pode surgir ou tornar-se mais evidente, cenário indesejável para qualquer instituição” (Haugen e Selin, 1999).

Na terceira parte do questionário ficou evidente que a gestão do risco de fraude deve ser definida a partir do topo. A estratégia deve ser assente na compreensão, redução e deteção de riscos, na análise e deteção de sinais de alerta, na gestão de incidentes e na prevenção de risco de fraude, o que implica a existência de meios e técnicas que permitam aumentar a segurança e a resistência das instituições.

“A prevenção da fraude requer uma forte ênfase na criação de um ambiente de trabalho que promove a ética comportamental, impede a ilegalidade e incentiva os funcionários a denunciar situações de fraude ou situações de suspeita de fraude. Os diferentes funcionários devem, portanto, ser instruídos com base nos valores centrais da empresa, o que lhes fornece uma orientação clara sobre o comportamento e as ações que lhes são ou não permitidas”. (*Association of Certified Fraud Examiners*, 2006).

A fraude materializa-se frequentemente (de acordo com respostas obtidas gráfico 7), pela apropriação indevida de ativos e conivência, o que para além dos custos monetários, afeta severamente a confiança dos clientes, colocando em causa o *Core Business* do negócio e a continuidade da instituição. Só com o aumento da eficiência na identificação, avaliação, controlo e mitigação das exposições ao risco e com o alargamento da abrangência dos controlos a efetuar, se pode minimizar as eventuais perdas para a instituição, detendo o controlo interno um papel determinante.

“O ambiente de controlo reflete a atitude e os atos da instituição perante o controlo interno, resultando das convicções, preferências e juízos de valor manifestados pelo órgão de administração e pelos restantes colaboradores da instituição em relação ao sistema de controlo interno, bem como da ênfase colocada no controlo interno nas medidas tomadas, nas políticas e procedimentos aprovados e na definição e implementação da estrutura organizacional” (Aviso do Banco de Portugal nº 5/2008).

“O ambiente de controlo é influenciado, designadamente, pelo padrão de valores éticos seguido pela instituição, pela existência de meios humanos e materiais suficientes e adequados, pelo grau de transparência da estrutura organizacional e da sua adequação face à complexidade e dimensão da atividade da instituição, pela clareza da cadeia hierárquica e das responsabilidades e competências atribuídas a cada função, pela qualidade do processo de planeamento estratégico e pelo grau de envolvimento do órgão de administração na atividade desenvolvida” (Aviso do Banco de Portugal nº 5/2008).

As instituições devem ter uma estrutura organizacional bem definida, transparente e perceptível, que sirva de suporte ao desenvolvimento da atividade e à implementação de um sistema de controlo adequado e eficaz, no sentido de assegurar que a gestão e o controlo das operações são efetuados de uma forma prudente, neste sentido o sistema de controlo interno não é um fim em si mesmo, deve servir os objetivos estratégicos da gestão. Cabe ao órgão de administração o dever de zelar pela sua eficácia e de dar a sua opinião sobre essa eficácia (artigo 11.º-B do Regulamento da CMVM n.º 2/2007). A eficácia deste sistema é essencial para a confiança nas instituições e para a proteção dos investidores. Podemos assim elencar objetivos de:

- Controlo interno
 - ✓ Identificar e gerir os riscos das atividades, procedimentos e sistemas,
 - ✓ Definir o nível de risco tolerado
 - ✓ Adotar políticas e mecanismos eficazes para gerir os riscos
 - ✓ Avaliar a adequação e a eficácia da gestão do risco
 - ✓ Avaliar o cumprimento pelo intermediário financeiro e pelos colaboradores dos procedimentos de gestão do risco
 - ✓ Corrigir as políticas de gestão do risco
 - ✓ Adotar um plano de auditoria interna

- Funções de *compliance*
 - ✓ Identificação dos riscos de incumprimento
 - ✓ Aplicação de medidas para a sua correção ou mitigação
 - ✓ Colaboração com a CMVM
 - ✓ Prevenção e combate ao abuso de mercado,
 - ✓ Branqueamento de capitais e fraude
 - ✓ Análise de ordens e operações

“A estrutura organizacional, incluindo as competências e responsabilidades de cada unidade de estrutura e ou função, as linhas de reporte e de autoridade e o grau e âmbito de cooperação entre as diversas unidades de estruturas ou funções, deve ser documentada, analisada e revista periodicamente, com vista a garantir a sua permanente adequação” (Aviso do Banco de Portugal nº 5/2008).

Com a Implementação e massificação do uso de sistemas informáticos, levou à necessidade de serem criadas várias ferramentas para uso no trabalho de auditoria, como forma de obter informação, temos assim as do tipo CAAT⁴⁶ que se generalizaram a nível mundial, entre as quais podemos nomear duas atualmente em uso no meio profissional: IDEA (*Interactive Data Extraction and Analysis*) e ACL (*Audit Control Language*) e ferramentas desenvolvidas em “*co-sourcing*” ou “*in-house*” como ferramentas de “*data mining*”. O modo de exercer Auditoria, e o objeto da análise, foram evoluindo ao longo do tempo, desde a conceção da Auditoria Inspeciva, passando pelo Controlo, pelo Risco e pela Auditoria Contínua. Nesta ultima vertente o apelo à utilização das ferramentas CAATs é determinante para o atingir dos objetivos preconizados, tal fato foi identificado pelas respostas obtidas.

De fato 61% das respostas (gráfico 8), apontou o uso de *softwares* específicos como a forma mais adequada para a deteção e prevenção de Fraude, superando a denúncia e o uso de entrevistas. O uso de *softwares* específicos de deteção e o conhecimento pelos colaboradores da sua existência pode também ser um fator dissuasor e inibidor de atos fraudulentos.

⁴⁶ Técnicas de auditoria assistidas por computador (CAATs) ou ferramentas de auditoria assistidas por computador e técnicas (CAATTs) é um campo em crescimento dentro da profissão de auditoria. CAATs é a prática de utilização de computadores para automatizar o processo de auditoria

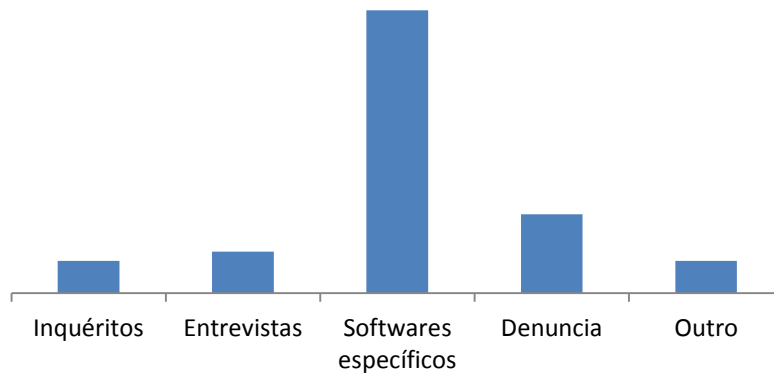


Gráfico 8: Detenção e prevenção fraude nas instituições financeiras

Embora existam diversos meios para um funcionário cometer uma fraude, há sempre três denominadores comuns: incentivo, oportunidade e racionalidade. A incapacidade de pagar dívidas tem-se revelado historicamente, um forte motivador, sendo referenciado no estudo como um dos fatores principais para tal situação devido a atual crise financeira (28%), no entanto o meio envolvente (15%), as relações interpessoais (17%) e o conflito de interesses (15%) acompanham os motivos que levam a situações duvidosas. Em casos extremos e em menor número (9% mas não menos importante), esta o vício pelo jogo, que apesar de em número reduzido pode envolver valores bastante superiores.

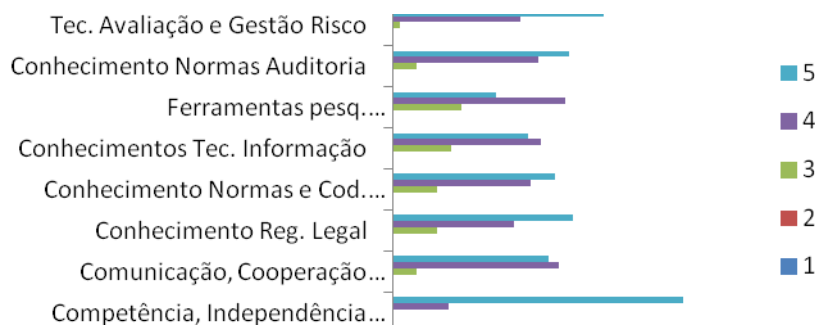


Gráfico 9: Características Auditor

O Auditor na execução do seu trabalho deve reger-se por elementos fundamentais como a competência, independência e ética – (gráfico 9), no entanto o conhecimento das normas e códigos internos da instituição bem como dos órgãos reguladores são fundamentais para o seu bom desempenho, englobando conhecimentos das normas de auditoria e técnicas de avaliação e gestão risco

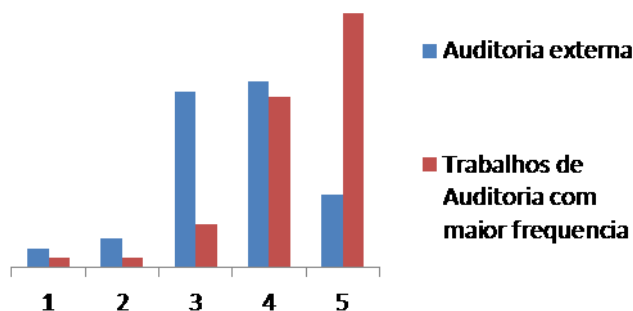


Gráfico 10: Detecção fraude
Relação Auditoria Interna/externa

O gráfico 10 representa as respostas obtidas sobre a relação entre a frequência de trabalhos e a detenção da fraude, aumentando a possibilidade de detenção com o incremento de revisões efetuadas, no entanto não existe correspondência entre os trabalhos efetuados pela auditoria interna com os realizados pela auditoria externa, tal situação prende-se pelo fato de o objetivo ser distinto nas duas situações, embora devam executar os seus trabalhos de forma concertada. O exercício da atividade das auditorias internas e externas é, de alguma forma, condicionado por conceitos de materialidade e de risco. Qualquer delas deve avaliar a eficácia do controlo interno, identificar as áreas de maior risco e fazer incidir as suas observações e análises nas suas áreas julgadas mais críticas e materialmente mais relevantes. Mas a par destas semelhanças existem, porém, significativas diferenças de conceitos e da sua utilização entre estes dois ramos de auditoria. A auditoria externa privilegia o risco associado a erros e omissões que possam influenciar significativamente as demonstrações financeiras. A auditoria interna, por seu lado, baseia-se num conceito de risco mais alargado. Preocupando-se também com os erros que possam afetar as demonstrações financeiras, preocupa-se mais com o risco associado à ineficiente utilização de recursos e a ineficácias de vária ordem, desde as relacionadas com a estrutura organizativa e a prossecução dos objetivos, gerais e departamentais, até às relacionadas com a imagem externa da instituição.

A materialidade é o conceito de primordial importância para a auditoria externa, que analisa e avalia em função da maior ou menor relevância das consequências que os erros possam ter nas demonstrações financeiras. Para a auditoria interna, pelo contrário, a materialidade não tem de se avaliar necessariamente em termos

financeiros. Por exemplo, uma situação de fraude interna, mesmo que nela se tenham envolvido valores relativamente pouco importantes, pode ou deve ser considerada de interesse relevante para os auditores internos pelas consequências adversas que daí possam advir, seja em termos concorrenciais e financeiros ou de imagem da instituição junto de consumidores e público em geral.

Mesmo a auditoria interna sendo diferenciada da auditoria externa, e respeitando as suas peculiaridades, será produtivo para a organização que elas atuem de forma integrada. Pois a auditoria interna, por possuir conhecimentos mais aprofundados do *know-how* da organização e ter possibilidade de executar uma auditoria continuada, certamente, proporcionará maior segurança ao auditor externo aquando da emissão da sua opinião a respeito das demonstrações financeiras. Daí que os profissionais que as executam devem manter contatos frequentes com os auditores externos. Mas a par dessas semelhanças, estes dois ramos de auditoria apresentam diferenças quanto aos seus objetivos e destinatários dos trabalhos que realizam, ao âmbito das ações e à metodologia seguida, à ênfase posta nas suas apreciações, ao *timing* e à frequência com que ambas realizam trabalhos de auditoria numa mesma organização e até mesmo quanto a alguns conceitos em que assentam. Identificada a relação entre a auditoria externa e interna, importa distinguir claramente as funções de um auditor externo e as funções de um auditor interno.

Ambos são essenciais à garantia do bom funcionamento do governo das sociedades uma vez que, pela sua necessária independência, conferem uma garantia acrescida de transparência e confiança, quer à informação financeira prestada pelas organizações ao mercado (auditoria externa), quer aos procedimentos de funcionamento interno que garantam uma atuação transparente no desenvolvimento dos negócios, em prol dos interesses dos investidores e distintos *Stakeholders* (auditoria interna).

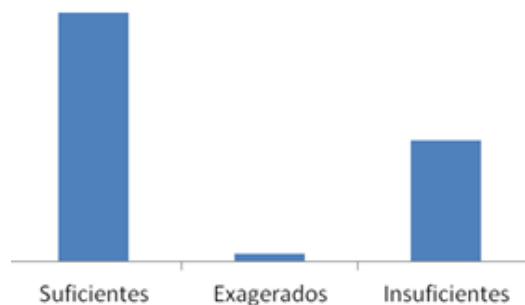


Gráfico 11: Trabalho de Auditoria junto das Sucursais

Outro aspeto importante abordado no questionário foi aferir a sensibilidade dos inquiridos sobre a necessidade de aumentar os trabalhos de auditoria realizados junto das sucursais, as respostas obtidas demonstram que os trabalhos realizados são suficientes para garantir o bom desenvolvimento do *core business* das entidades, nomeadamente ao nível de objetivos, manutenção de ativos e continuidade da atividade, prevalecendo a prioridade da prevenção e incremento de valor na sociedade (gráficos 11 e 12), no entanto com a politica de redução de custos devido às contingências atuais da economia, as organizações estão a reduzir os recursos humanos alocados a funções de auditoria, podendo colocar em risco a sua função de prevenção e deteção com incremento de valor nas organização. Os recursos humanos devem ser em número suficiente face à estrutura organizacional implementada e possuir os níveis de competência, conhecimento e experiência necessários para a execução das responsabilidades que lhes sejam atribuídas.

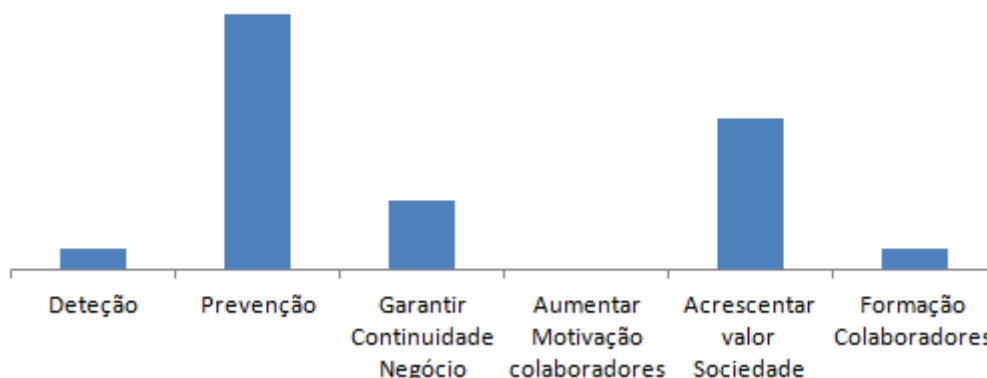


Gráfico 12: Objetivo dos trabalhos desenvolvidos Sucursais

“O sistema de controlo interno dever garantir a existência de informação substantiva, atual, compreensível, consistente, tempestiva e fiável, que permita uma visão global e abrangente sobre a situação financeira, o desenvolvimento da atividade, o cumprimento da estratégia e dos objetivos definidos, o perfil de risco da instituição e o comportamento e evolução do mercado ou mercados relevantes” (Aviso do Banco de Portugal nº 5/2008).

“A instituição deve desenvolver, implementar e manter processos formais de captação e tratamento da informação, apropriados à dimensão, natureza e complexidade da atividade desenvolvida que suportem a tomada de decisões pelos órgãos de administração e de gestão e permitam o cumprimento das obrigações perante terceiros, nomeadamente as de reporte às autoridades de supervisão” (Aviso do Banco de Portugal nº 5/2008).

O trabalho da auditoria interna fica espelhado na emissão de um relatório, este é o produto dos estudos, investigações e análises realizadas durante o trabalho de campo e traduz por escrito a opinião e as recomendações de todo o trabalho desenvolvido. É necessário que todos estejam conscientes que os relatórios assinalam falhas e deficiências dos controlos, sistemas e procedimentos de que são responsáveis em último caso, os cargos superiores da organização. Incluem ainda recomendações e propostas de como evitar e eliminar falhas ou deficiências. A Norma 2400 “Comunicação dos Resultados” contida nas Normas Internacionais para a Prática Profissional de Auditoria do IIA, define que os auditores internos devem comunicar os resultados do trabalho, essa comunicação deve incluir os objetivos do trabalho e o seu âmbito bem como as conclusões aplicáveis recomendações e planos de ação. Qualquer relatório de auditoria, quer emanado pela auditoria externa quer pela interna, deve conter a avaliação do sistema de controlo de interno da organização, independentemente da perspetiva. Neste sentido o órgão de administração deve enviar anualmente à CMVM um relatório sobre controlo interno de acordo com o aviso nº 5/2008, com uma descrição clara e concisa dos desvios encontrados no sistema de controlo interno por comparação com os requisitos da norma:

- Conteúdo obrigatório do relatório
 - ✓ Opinião global do órgão de administração sobre a adequação e a eficácia do sistema de controlo interno.
 - ✓ Descrição sintética do negócio e perspetivas de evolução futura
 - ✓ Organograma, descrição de competências funcionais e identificação dos responsáveis
 - ✓ Atividades e/ou funções subcontratadas e identificação das empresas contratadas
 - ✓ Identificação dos responsáveis do “*compliance*”, gestão do risco e auditoria e descrição das deficiências detetadas por estes serviços

- ✓ Descrição, por áreas funcionais, das deficiências não corrigidas, justificação e prazo previsto para a respetiva correção
 - ✓ Demonstração das condições para beneficiar das exceções aplicáveis
 - ✓ Descrição do plano de auditoria interna
- Conteúdo obrigatório do anexo ao relatório
- ✓ Informação sobre as operações analisadas no âmbito do combate ao branqueamento de capitais
 - ✓ Informação sobre a análise de ordens e operações sobre instrumentos financeiro e respetivas conclusões
 - ✓ Descrição dos riscos de cada atividade de intermediação financeira exercida e dos procedimentos e sistemas existentes, indicando, se for o caso, parâmetros de alerta e níveis de risco tolerados
 - ✓ Descrição sintética das atividades desenvolvidas através de agentes vinculados, incluindo eventuais incidentes e o número de clientes angariados
 - ✓ Indicação do número total de reclamações por área de atividade e assunto, prazo médio de resposta aos reclamantes e o peso relativo das respostas favoráveis a estes.
- Importância do relatório de controlo interno das Instituições financeiras na atividade CMVM
- ✓ Recolha de informação para definição do modelo de supervisão baseado no risco (seleção dos intermediários financeiros a sujeitar a supervisão presencial)
 - ✓ Verificação do cumprimento pelo intermediário financeiro do dever de análise de operações
 - ✓ Possíveis indícios de responsabilidade criminal dos administradores por não porem termo a comportamentos manipulatórios de que tenham conhecimento puníveis criminalmente.

Ao lidar com os requisitos de Basileia III os bancos devem conceber uma organização estruturada e transparente com responsabilidades claras a todos os níveis e com um sistema de normas e regras adequados aos modelos, processos e dados envolvidos. Como não podia deixar de ser, é fundamental uma política concertada de recursos humanos que garanta que as instituições possuam capital humano suficiente para lidarem com novas necessidades de especialização e até novas funções.

Resumidamente, Basileia III cobre um largo número de áreas, pelos que é fortemente aconselhável uma revisão detalhada e rigorosa dos dados de suporte à informação de gestão e respetiva arquitetura informática, das metodologias de gestão de risco, da estrutura de governo das instituições, dos sistemas de reporte e de todos os processos envolvidos

Em conclusão, podemos aferir que as respostas obtidas identificam uma preocupação constante das instituições em implementar e manter um sistema gestão de riscos eficaz, sólido e consistente com a dimensão, estrutura e estratégias definidas. Embora as instituições se encontrem sujeitas aos requisitos estabelecidos e recomendados pelos órgãos de controlo e normativos vigentes, o ambiente de controlo é influenciado pelo “ADN” da instituição, assente em padrões de valores éticos, integridade e profissionalismo.

10. Conclusões

Face ao elevado grau de complexidade das atividades e dos negócios das organizações, bem como a diversificação de mercados onde atuam, detendo na conjuntura atual níveis superiores de incerteza e elevada dispersão geográfica nacional e internacional, implica que as organizações, bem como a função da auditoria interna se estruturem e capacitem com recursos e competências por forma a cumprir os objetivos previamente definidos.

O que move as organizações é hoje em dia, mais do que nunca, e inequivocamente, os objetivos que ela pré-determina e que regulam todo o seu *modus operandi*. A consecução dos objetivos vai depender em grande medida da capacidade da organização delinear uma estratégia que se enquadre nas exigências internas e externas. A nível interno, uma correta avaliação de capacidades e recursos disponíveis, com indicações claras de eficácia e eficiência dos mesmos, bem como a nível externo com a análise da envolvente, identificando oportunidades e ameaças. Para Tal, uma análise *SWOT* (*Strengths; Weaknesses; Opportunities; Threats*) permitirá formular um conjunto de estratégias económicas possíveis a aplicar que associadas ao sistema de valores interno e externo (por exemplo o conjunto de valores da sociedade onde a organização está inserida) conduzirá a um processo de tomada de decisão acerca da estratégia a seguir para atingir os objetivos previamente estabelecidos.

A banca deve desenvolver a sua atividade com responsabilidade na relação com Colaboradores, Clientes, Acionistas e demais *Stakeholders* e pautar a sua atuação pelo cumprimento de princípios internos de rigor e das disposições emitidas pelas competentes entidades reguladoras. Por outro lado as instituições financeiras são o reflexo da excelência dos seus Colaboradores, sendo eles imprescindíveis para o sucesso da organização e do seu desenvolvimento sustentável. A sua gestão constitui um vetor estratégico na relação de elevada qualidade e de permanente apoio aos Clientes que é um dos fatores distintivos das mesmas. Para a gestão e controlo do Risco Operacional a banca tem vindo a adotar de forma crescente e muito relevante, um conjunto de princípios, práticas e mecanismos de controlo, claramente definidos, documentados e implementados, de que são exemplo; a segregação de funções, a definição de linhas de responsabilidade e respetivos níveis de autorização, a definição de limites de tolerância e de exposição aos riscos, os códigos deontológicos e de

conduta, os indicadores chave de risco (*KRI – key Risk Indicators*), os controlos de acesso (físicos e lógicos), as atividades de reconciliação, os relatórios de exceção, os planos de contingência, a contratação de seguros e a formação interna sobre processos, produtos e sistemas. Assim pretende-se alcançar uma cada vez maior eficiência na identificação, avaliação, controlo e mitigação das exposições ao risco operacional. A gestão do risco operacional deve assentar numa estrutura de processos “*end-to-end*”, definidas e implementadas para todas as áreas da organização, beneficiando com uma perceção mais abrangente dos riscos, decorrente de uma visão integrada das atividades desenvolvidas ao longo da cadeia de atividades de cada processo, sendo dinâmico, ajustado e diferenciado em função das práticas operacionais e de negócio de cada uma.

A responsabilidade pela gestão dos processos será atribuída a *Process Owners*⁴⁷ que têm por missão:

- ✓ Caraterizar as perdas operacionais capturadas no contexto dos seus processos;
- ✓ Realizar a autoavaliação dos riscos (*RSA – Risks Self-Assessment*),
- ✓ Identificar e implementar as ações adequadas para mitigar exposições ao risco, contribuindo para o reforço do ambiente de controlo interno;
- ✓ Monitorizar os indicadores de risco (*KRI*⁴⁸).

O objetivo da autoavaliação dos riscos é o de promover a identificação e a mitigação (ou mesmo eliminação) de riscos, atuais 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 operacional sem considerar a influência dos controlos existentes (Risco Inerente);
- ✓ Avaliar a influência do ambiente de controlo existente na redução do nível das exposições (Risco Residual);
- ✓ Identificar o impacto das oportunidades de melhoria na redução das exposições mais significativas (Risco Objetivo).

⁴⁷ Abordagem sistemática para ajudar a organização a identificar, analisar e melhorar os processos de negócio

⁴⁸ *key Risk Indicators*

Por outro lado o “*compliance*” tem por missão assegurar que os órgãos de gestão, as estruturas funcionais e todos os Colaboradores cumpram a legislação, regras e normativos (internos e externos) que pautam a atividade, de forma a evitar o risco de as Instituições incorrerem em sanções de carácter legal ou regulamentar e em prejuízos financeiros ou de ordem reputacional, decorrente do incumprimento das leis, códigos de conduta e regras de “boas práticas” negociais e deveres a que se encontram sujeitas.

Integra como seus objetivos o respeito pelas disposições legais e regulamentares aplicáveis, incluindo as relativas à prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como das normas e usos profissionais e deontológicos, das regras internas e estatutárias de cada instituição, das regras de conduta e de relacionamento com Clientes, das orientações dos órgãos sociais e das recomendações do Comité de Supervisão Bancária de Basileia e do Comité das Autoridades Europeias de Supervisão Bancária (CEBS), de modo a proteger a reputação das Instituições e a evitar que estas sejam alvo de sanções, conforme estabelecido no Art. n.º 2, alínea c) do Aviso 5/2008 do Banco de Portugal (BdP).

A Auditoria deve ser uma componente do Sistema de Controlo cuja missão principal é assegurar a adequação e a eficácia do sistema de controlo interno como um todo e ainda assegurar a adequação dos processos de identificação e gestão de riscos e de governação das instituições.

O exercício da função de auditoria interna deverá ter carácter permanente e ser independente, devendo a Direção de Auditoria desempenhar a sua missão mediante a adoção dos princípios de auditoria interna reconhecidos, devendo emitir recomendações baseadas nos resultados das avaliações efetuadas que deverão acrescentar valor à organização e melhorar o controlo e a qualidade das suas operações, contribuindo para a realização dos seus interesses estratégicos e assegurando que:

- ✓ Os riscos são devidamente identificados e geridos e os controlos implementados são corretos e proporcionais aos riscos;
- ✓ O sistema de avaliação do capital da Instituição é adequado relativamente ao seu grau de exposição ao risco;
- ✓ Os vários órgãos de governação interagem de modo adequado, eficaz e eficiente;
- ✓ As operações são registadas corretamente e a informação operacional, financeira e de gestão é rigorosa, fiável e atempada;

- ✓ A salvaguarda e a segurança dos interesses e bens patrimoniais que lhes foram confiados estão devidamente acauteladas;
- ✓ Os Colaboradores desempenham as suas funções em conformidade com as políticas, códigos de conduta, normas e procedimentos internos e com a legislação e demais regulamentação aplicável;
- ✓ Os recursos são adquiridos economicamente, usados eficientemente e protegidos adequadamente;
- ✓ Os programas, planos e objetivos definidos pela gestão são cumpridos;
- ✓ As matérias legais e regulatórias com impacto significativo na organização são reconhecidas, claramente entendidas e devidamente abordadas.

Os códigos internos (deontológicos e ética) devem informar sobre deveres de ética e conduta profissional e neles enunciados deveres e obrigações, que tanto respeitam ao funcionamento da organização, como ao comportamento individual de cada um dos Colaboradores e dos Membros dos órgãos de administração e fiscalização, no exercício das respetivas funções, podendo enumerar alguns exemplos:

- ✓ Política de Sustentabilidade;
- ✓ Política Ambiental;
- ✓ Política Social;
- ✓ Estatutos e principais normas e regulamentos da organização.

Apesar de não ter sido abordado no trabalho, é importante referir que as instituições financeiras devem gerir também o tema da continuidade do negócio ao nível de instalações e dados, garantindo assim que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre até ao retorno da situação normal de funcionamento da instituição dentro do contexto de negócio da qual faz parte, não apenas as ameaças de terrorismo (inexistentes em Portugal no momento), mas também catástrofes naturais e desastres possíveis (incêndios, roubos, fuga de informação), com vertentes de contingência face a eventos de extrema gravidade que possam afetar de forma muito significativa ou mesmo pôr em causa a própria sobrevivência da instituição, podemos assim enumerar o DRP (*Disaster Recovery Plan*) e o PCN (Plano de Continuidade de Negócios), como exemplos, sendo a segurança e continuidade do negócio preocupações que estão na primeira linha de atuação das administrações.

Estes planos têm como objetivo principal a formalização de ações a serem tomadas, para que, em momentos de crise, a recuperação, a continuidade e a retoma possam ser efetivos, evitando assim que os processos críticos do negócio sejam afetados, incorrendo em perdas financeiras para as instituições.

Em conclusão podemos aferir que a existência de uma cultura organizacional focalizada na gestão integrada de risco e performance é o *driver* para a identificação e mitigação em tempo útil de riscos e ameaças, permitindo mitigá-los de modo eficaz e eficiente, bem como identificar e explorar oportunidades, que se poderão traduzir em criação de vantagens competitivas e deste modo contribuir para o sucesso de médio/longo prazo das organizações. Por muito que queiramos realçar as responsabilidades sociais das organizações não há como escapar ao objetivo principal e prioritário que é a criação de valor para os acionistas e *stakeholders* em geral, demonstrando consistência nos resultados obtidos em cada período económico e ainda garantindo e transparecendo uma segurança e confiança inabalável no reporte da informação financeira, fiscal e de gestão.

Esta segurança e confiança deve transparecer para os mercados e para a opinião pública em geral por forma a recolher o interesse de novos *stakeholders* e salvaguardar os que já depositam quer a confiança quer o capital nos ativos da organização em questão, pelo que a estratégia a seguir, será a que melhor servir os objetivos a atingir, dependendo daí o *modus operandi* da organização, com definição clara do seu *core business*.

11. Referências Bibliográficas

Bibliografia

Albrecht, W.S., Howe, K.R. e Romney, M.B. (1984), *Deterring Fraud: The Internal Auditor's Perspective*, Altamonte Springs, FL: The Institute of Internal Auditor's Research Foundation.

Almeida, B. e Taborda, D. (2003), A Fraude em Auditoria: Responsabilidade dos Auditores na sua deteção, *Revisores e Empresa*, 21: 28-38.

Almeida, D. (2005), Gestão de Risco e Governo das Sociedades, *Revista de Auditoria*

Associação Portuguesa de Bancos, *Boletins Informativos*, disponíveis em www.apb.pt; Auditoria; Universidade Aberta.

Aviso do Banco de Portugal nº 11/2005 de 13 de Julho de 2005, Diário da República nº 139, Série I-B, Banco de Portugal.

Aviso do Banco de Portugal nº 2/2007 de 8 de Fevereiro de 2007, Diário da República nº28/07, Série I, Banco de Portugal.

Azevedo, Belmiro; 2005; *Gerir o Risco através da Criação de Valor*; Revista IPAI, nº 23; Janeiro/Março 2006.

Banco de Portugal (2008), *Aviso nº5/2008 Sistema de Controlo Interno das Instituições Financeiras*, Banco de Portugal, Lisboa (Jun. 2008)

Banham, R. (2004), "Enterprising views of risk management", *Journal of Accountancy*, Jun:65/71.

Baptista da Costa, C. (2007). *Auditoria Financeira*; Editora Rei dos Livros – 8ª Edição.

Barnes, R.W. (1995), The Value of Quality Education to Banks and Bankers, *The Journal of Indian Institute of Bankers*, 66(3), 55-59

BEJA, Rui. - *Risk Management; Gestão, Relato e Auditoria dos Riscos do Negócio*, Áreas editora, 2004. ISBN 972-8472-69-2.

Bento, N. (2011), Segurança Bancária, *inforBANCA*, 87-12.

Bessis, J. (2002). *Risk Management in Banking* (2nd. edition). West Sussex: John Wiley & Sons.

Black, H.C. (1979), *Black's Law Dictionary*, 5ª Edição, St. Paul, MN: West Publishing.

Borge, Dan (2002), *The Book of risk*, John Wiley & Sons, ISBN-0471196703

Borrvalho, (2007), Manipulação de Auditores, Tese de Mestrado, ISCTE

Brasiliano, António Celso Ribeiro – *Entendendo Riscos Corporativos* – [Consult. 12 Out. 2009]. Disponível em <http://www.brasiliano.com.br/blog/?p=274>

Brink, Gerrit J. Van Der. (2002). *Operational Risk: The new challenge for banks*. Palgrave Publishers.

Buchelt, R. & Unteregger, S. (2004). “Cultural Risk and Risk Culture: Operational Risk after Basel II, Financial Stability Report 6.” http://www.oenb.at/en/img/fsr_06_cultural_risk_tcm16-9495.pdf.

Butler, Eamonn; - O Melhor Livro nenhuma Mercado (Sobre o Mercado),1ª [SL]. ISBN – 1864321377

Cafferty, D. (2003), Global Composite Model: A Plan to Detect and Prevent Fraud Worldwide, *The White Paper*, 17(6), 22-25

Câmara, P.(2008), A auditoria interna e o governo das sociedades -2ª parte; *Revista de Auditoria Interna*, nº31, Outubro/Dezembro.

Carneiro, L. F. F., Vivan A.G. F. & Krause K., (2004). O novo acordo da Basileia – um estudo de caso para o contexto brasileiro. Disponível em 24 de Novembro de 2011, em <http://www4.bcb.gov.br/pre/inscricaoContaB/trabalhos/O%20Novo%20Acordo%20de%20Basileia%20um%20estudo%20de%20caso%20para%20o%20contexto%20brasileiro.pdf>

Castanheira, N. (2007), Auditoria Interna Baseada no Risco - Estudo do caso Português, Tese de Mestrado em Contabilidade e Auditoria Universidade do Minho.

Castanheira, Nuno; Rodrigues, Lúcia; 2006a); *Gestão de Risco – Da Abordagem Tradicional à Gestão de Risco Empresarial (ERM)*; Revista Revisores & Empresas; Julho/Setembro; pág. 58.

Chabanel, P.E. (2011). Implementação de Basileia III: desafios, opções e oportunidade; Moody's Analyhes Enterprise Risk Solutions em Setembro 2011. Disponível em 3 de Janeiro de 2012, em <http://www.moodyanalytics.com/~media/Insight/Regulatory/Basel-III/Thought-Leadership/2011/11-01-09-Implementing-Basel-III-Whitepaper.aspx>

Cicco, Francesco; 2010; *Dos riscos “Negativos” aos Riscos “Positivos”* consultado em 20 Janeiro 2010 em <http://www.iso31000qsp.org/>

CMVM (2001), Regulamento da CMVM n.º 7/2001 Governo das Sociedades Cotadas.

CMVM (2005), Recomendações da CMVM sobre o Governo das Sociedades Cotadas.

CMVM (2007 a), Regulamento da CMVM nº 1/ 2007.

CMVM (2007 b), Recomendações da CMVM sobre o Governo das Sociedades

CMVM (2009), Consulta Pública da CMVM N.º 02/2009 - Projecto de Regulamento da CMVM Governo das Sociedades Cotadas (Revoga o Regulamento da CMVM N.º1/2007) e Projeto de Alteração ao Código do Governo das Sociedades (Recomendações).

COSO (2004), Interprise Risk Management - Integrated Framework – Executive Summary.

COSO (2009), Internal Control — Integrated Framework, Guidance on Monitoring Internal Control Systems.

COSTA, Carlos B. – *Auditoria Financeira: Teoria e Prática*. 8ª ed.: Rei dos Livros, 2007. ISBN 978-972-51-1127-7

Cressey, D.R. (1973), *Other People's Money*, Montclair, NJ: Patterson Smith

Cruz, M. (2003). “Operational Risk: Past, Present and Future.” Pp. 271–286 in *Modern Risk Management: A History*, ed. P. Field. London: Risk Books.

Cruz, Manuel Mendes – *Gestão do Risco Empresarial*, 2008: ISCAL, Sebenta de Apontamentos.

Cunha, V & Martins, A. (2007), Uma Visão Económica da Questão do Governo das Empresas, *Jornal de Contabilidade*, nº 367.

Deloitte (2005), Optimizing The Role of Internal Audit in The Sarbanes-Oxley, Era do Mercado de Capitais Brasileiro.

Ferma; 2003; Federation of European Risk Management Associations; *Norma de Gestão de Riscos*.

Ferreira, E. (2007), *O Papel do Auditor na Prevenção, Detecção e Denúncia da Fraude: Uma análise empírica em Portugal*, Dissertação de Mestrado em Contabilidade e Auditoria, Universidade do Minho.

Geiger, Hans (2000) Regulating and Supervising Operational Risk for Banks

Gibson, Michael S. (1997). *Information Systems for Risk Management*, www.bog.frb.fed.us.

Gómez Pérez (1990), Ética empresarial: teoría y casos, ISBN - 8432132292

Gonçalves, A. (2008), A evolução das Metodologias de Auditoria, *Revisores e Auditores*. Marques, M. (2003), O que é o “Corporate Governance”; *Revista de Auditoria Interna*, nº17, Outubro/Dezembro.

Haugen, S. e Selin, J.R. (1999), Identifying and controlling computer crime and employee fraud, *Industrial Management & Data Systems*, 99(8).

Hussein, Haji; 2008; E- Commerce e Ressource Centre; Article; *Risk Assesement; Using COBIT® as a Guide Risk Assesement Assurande Services*, consultado em 06/06/2009: <http://fata86.webs.com/riskassesment.html>.

IPAI (2007), *O Enquadramento de Práticas Profissionais de Auditoria Interna*, Lisboa: Instituto Português de Auditoria Interna.

Iyer, N. e Samociuk, M. (2006), *Fraud and Corruption – Prevention and Detection*, Burlington: Gower.

Jobst, Andreas A. (2007). “Consistent Quantitative Operational Risk Measurement and Regulation: Challenges of Model Specification, Data Collection and Loss Reporting”, IMF Working Paper.

Khanna, A. e Arora, B. (2009), A study to investigate the reasons of bank frauds and the implementation of preventive security controls in Indian Banking industry, *Int. Journal of Business Science and Applied Management*, 4(3).

Lastra, R.M. (2000), *Banco Central e Regulamentação Bancária*, BH: Livraria Del Rey Editora.

Lewis, C. M. & Lantsman, Y. (2005). What is a Fair Price to Transfer the Risk of Unauthorized Trading? A Case Study on Operational Risk.” Pp. 315–356 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Mendonça, A. R. R. de, Augusto A. F. & Vlatkovic G. C. (2011). Basileia III: Alterações Propostas, Institucionalidade Europeia e Adoção no Reino Unido. IV Encontro Internacional da Associação Keynesiana Brasileira (AKB), Rio de Janeiro/Brasil. Disponível em 24 de Novembro de 2011, em <http://www.ppge.ufrgs.br/akb/encontros/2011/47.pdf>.

Moreira, J. et al (2004), *Corporate Governance em Portugal*.

Narasimhan, R. (2005), *Frauds in Banks, 1ª Edição, Índia: The ICFAI University Press*.

Neto, J.A.M. e Parente, R.V. (2010), *Fraudes Tecnológicas Bancárias, XIX Encontro Nacional do CONPEDI, Fortaleza, Brasil*.

Pereira, G.& Branco, C.(2005), *As Novas Regras sobre Governo das Sociedades (“Corporate Governance”)*.

Pinheiro, J. (2008 a), *Auditoria Interna - Manual Prático para Auditores Internos –*

Pires, A. (2008), *Impacto da lei Sarbanes - Oxley no Sistema de Controlo Interno*

Ryu, Tae G., Roh, Chul-Young, (2007), The auditor’s going-concern opinion decision,

Sá, A.L. (1997), *Perícia Contábil, 3ª Edição, SP: Atlas*.

Saidenberg, M. & Schuermann, T. (2003). *The New Basel Capital Accord and Questions for Research*, <http://fic.wharton.upenn.edu/fic/papers/03/0314.pdf>.

Santi, Paulo Adolpho, *Introdução Auditoria*, ISBN - 8522403724

Série Risk Management; 2004; *Gestão de riscos: A norma AS/NZS 4360:2004*; Revisão Técnica Francesco De Cicco; Risk Tecnologia Editora Ltda; 2ª Edição; Dezembro

Série Risk Management; 2005; *Directrizes para a Implementação da AS/NZS 4360:2004*; Revisão Técnica Francesco De Cicco, Agosto; Risk Tecnologia Editora Ltda.

Série Risk Management; 2007; *Auditoria Baseada em Riscos – Como Implementar a ABR nas organizações: uma abordagem inovadora*; Revisão Técnica de Francesco De Cicco. Risk Tecnologia Editora Ltda.

Simões, Reinaldo; 2009; *Gestão de Riscos segundo as Normas AS/NZS 4360:2004 e ISO 31000:2009*; QSP- Centro da Qualidade, Segurança e Produtividade - consultado em 22 Nov.2009:http://www.abrapp.org.br/ppub/portal/adm/editor/UploadArquivos/30congresso/tecnicas/tec9/reinaldo_simoes.pdf.

Tavares, C. (2006), *Evolução e alterações no Governo das Sociedades*.

TUAC (2004), *Review of the OECD Principles of Corporate Governance: An Evaluation Uma abordagem proactiva e a evolução necessária*, Editora Rei dos Livros.

Veja, Luis; 2003; *La Gestión de Riesgos en Empresas no Financieras*; Revista Partida Doble, nº 150, Diciembre.

Vinella, P. & Jin, J. (2005). "A Foundation for KPI and KRI." Pp. 157–168 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Wahler, B. (2002). "Process-Managing Operational Risk – Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II-Framework", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=674221

Wells, J.T. (2001), *Why Employees Commit Fraud*, *Journal of Accountancy*, American Institute of Public Accountants, <http://www.acfe.com/resources/view.asp?ArticleID=41>.

Wells, J.T. (2009), *Fraude na Empresa - Detecção e Prevenção*, 2ª Edição, Coimbra: Almedina. **Willsher, Richard; 2007**, *Um negócio arriscado*; Revista Exame World Business; Agosto/Setembro/Outubro: 42 a 47.

WEBGRAFIA

WWW.ACFE.COM

WWW.AGENCIALUSA.PT

WWW.AICPA.ORG – THE AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

WWW.AICPA.ORG/SARBANES/INDEX.ASP - SARBANES-OXLEY

WWW.AIRMIC.COM - ASSOCIATION OF INSURANCE AND RISK MANAGERS (AIRMIC)

WWW.AUDIT-COMMISSION.GOV.UK – *AUDIT COMMISSION*

WWW.BANCOBPI.PT

WWW.BANIF.PT

WWW.BPORTUGAL.PT/

WWW.CCAM.PT

WWW.CGD.PT

WWW.CMVM.PT – *COMISSÃO DO MERCADO DE VALORES MOBILIÁRIOS*

WWW.CORPGOV.NET - *CORPORATE GOVERNANCE SITE*

WWW.COSO.ORG - COMMITTEE FOR SPONSORING ORGANIZATIONS (COSO)

WWW.DIARIOECONOMICO.PT

WWW.ECGI.ORG. EUROPEAN CORPORATE GOVERNANCE INSTITUTE

WWW.FERMA.EU – FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS

WWW.IPAI.PT – *INSTITUTO PORTUGUÊS DE AUDITORIA INTERNA*

WWW.MILLENNIUMBPC.PT

WWW.THEIIA.ORG - THE INSTITUTE OF INTERNAL AUDITORS

WWW.THEIRM.ORG - INSTITUTE OF RISK MANAGEMENT (IRM)

12. Anexos

➤ *Questionário*

➤ *Resultados Questionário*