

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE
CONTABILIDADE E ADMINISTRAÇÃO DE
LISBOA



ISCAL

O SISTEMA DE CONTROLO INTERNO NAS
INSTITUIÇÕES FINANCEIRAS

Maria João Esteves Fernandes Loureiro

Lisboa, Abril de 2015

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E
ADMINISTRAÇÃO DE LISBOA

O SISTEMA DE CONTROLO INTERNO NAS
INSTITUIÇÕES FINANCEIRAS

Maria João Esteves Fernandes Loureiro (aluna n.º 20120195)

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica de Ana Marinho Pires, professora da área científica de Riscos Empresariais e de Controlo Interno.

Constituição do Júri:

Presidente _____ Especialista Gabriel Alves

Vogal _____ Especialista Maria da Luz Miranda

Vogal _____ Especialista Ana Marinho Pires

Lisboa, Abril de 2015

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas. Mais acrescento que tenho consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

Dedicatória

Aos meus pituxos, Francisco e Guilherme, e ao pai deles, meu marido, Nuno Pereira, que muito me apoiaram... e reclamaram, pelas horas não partilhadas...

À minha irmã, Lili, porque é, e sempre será, parte de mim, e porque este é, sem dúvida, um projeto de ambas.

Ao Guga, porque não houve um só dia em que ele não estivesse presente.

Ao Kalú, porque já faz parte da família.

Agradecimentos

À minha orientadora Ana Marinho Pires, pela sua colaboração e paciência;

Às minhas colegas de mestrado, em especial à Mafalda e à Sandra, pelo espírito de entreaajuda e amizade que criamos, pelas críticas e motivação;

A todos os meus amigos, sem exceção, pois sem eles não seria quem sou;

Ao Nuno, ao Francisco e ao Guilherme, por todo o amor e cumplicidade;

A toda a minha família, pela amizade, companheirismo e alegrias;

Aos meus pais, Armando e Milú, e irmãos, Cláudia, Pedro e Lili, porque sempre fizeram dos meus sonhos os seus.

Resumo

Nos últimos anos, o conceito de controlo interno tem vindo a sofrer transformações, em resultado da necessidade de dar respostas à gestão de riscos nas organizações. Os modelos de avaliação de riscos, para além de constituírem uma ferramenta de apoio aos gestores na tomada de decisão, são também utilizados pelos auditores na avaliação do sistema de controlo interno a que estes têm que proceder.

Após a revisão da literatura, foi desenvolvido um estudo empírico, que tem origem num raciocínio dedutivo, com vista a concluir sobre se o uso dos modelos de gestão de riscos, enquanto ferramenta de gestão para obter um sistema de controlo interno efetivo, tem impacto no resultado das auditorias. Para o efeito, foi analisado o caso particular das instituições financeiras, na medida em que estas, ao abrigo do Aviso n.º 5/2008, se encontram obrigadas à adoção de um sistema de controlo interno suportado no *Internal Control Integrated Framework*, publicado pelo *Committee of Sponsoring Organizations of the Treadway Commission*.

Do exercício realizado, concluímos que, de facto, os resultados dos relatórios de auditoria para os anos considerados, foram bastantes positivos, contudo, os acontecimentos recentes no sistema bancário português fazem-nos questionar a qualidade dos trabalhos realizados pelo auditor.

Palavras-Chave: Controlo interno, gestão de riscos, *Governance*, instituições.

Abstract

The internal control concept is changing due to the need of answering to risk management requests in the organisations. The use of risk management models, are recognized all over the World as a tool that support Management in decision-making, as well as the auditors, in the evaluation of the internal control system.

After the literature revision, an empirical study has been developed, based on a deductive reasoning, in order to conclude if the risk management models, as a tool to achieve an effective internal control, improve the audit results. For this purpose, the exercise was performed for bank and financial institutions, due to the fact that, under the terms of the Bank of Portugal Notice 5/2008, those institutions are required to adopt the Internal Control Integrated Framework, published by the Committee of Sponsoring Organizations of the Treadway Commission.

From this, we can conclude that, despite the positive audit reports results in the years considered, the last events occurred in Portuguese banking system, leave us in doubt about the quality of audits.

Key-words: *Internal control, risk management, Governance, institutions*

Índice

1. Introdução	1
2. O controlo interno nas organizações em geral	4
2.1 – Enquadramento teórico	4
2.2 – Os principais requisitos da Lei <i>Sarbanes-Oxley</i>	6
2.2.1 – A criação do PCAOB e a independência do auditor	9
2.2.2 – Outros aspetos relevantes de <i>Corporate Governance</i>	13
2.3 – A internacionalização das normas de auditoria	14
2.4 – O <i>Committee of Sponsoring Organizations of the Treadway Commission</i> : O <i>Internal Control Integrated Framework</i> e o <i>Enterprise Risk Management</i>	17
2.4.1 – O <i>Internal Control - Integrated Framework</i>	17
2.4.2 – O <i>Enterprise Risk Management</i>	23
2.5 – O <i>Control Objectives for Information and Related Technology</i>	26
3. O controlo interno nas instituições financeiras	29
3.1 - Enquadramento teórico	29
3.2 – Os pilares do controlo interno nas instituições financeiras	32
3.2.1 - O <i>Framework for Internal Control Systems in Banking Organizations</i>	32
3.2.2 – As orientações de <i>Internal Governance</i> divulgadas pelo <i>Committee of European Banking Supervisors</i>	36
3.3 - O Controlo Interno na Banca em Portugal	41
3.3.1 O Modelo de Avaliação de Riscos	41
3.3.1.1 – Avaliação das categorias de risco e de controlos	43
3.3.1.2 – Solvabilidade e liquidez	45
3.3.2 - O Aviso n.º 5 do Banco de Portugal	46
3.3.2.1 - Riscos a considerar pelo sistema de gestão de riscos	50
3.3.2.2 – Funções de controlo	53
3.3.2.3 – Responsabilidades do órgão de administração	56
3.3.2.4 – O relatório de controlo interno	58

3.3.3 – A supervisão prudencial do Banco de Portugal	59
4. Estudo empírico	66
4.1 – Apresentação do Problema da Investigação	66
4.2 – Apresentação do desenvolvimento e desenho da investigação	67
4.3 – Seleção da amostra	67
4.4 – Recolha, análise e tratamento de dados	69
4.5 – Resultados e conclusões	75
4.5.1 – Limitações	81
5. Conclusão.....	82
Referências Bibliográficas	84
Apêndices.....	90
Anexos	91

Índice de quadros e tabelas

Table 2.1 O Normativo técnico de auditoria	16
Table 3.1 Supervisão	43
Table 3.2 Grelha de notações para avaliação de riscos	45
Table 3.3 Grelha de notações para avaliação de controlos	45
Table 4.1 Entidades supervisionadas obrigadas a apresentar relatório de controlo interno	68
Table 4.2 Nome e tipo de instituição a analisar	69
Table 4.3 Resultados das auditorias	70
Table 4.4 Resultados das auditorias de 2008	71
Table 4.5 Resultados das auditorias de 2013	71
Table 4.6 Ênfases e Reservas das CLC relativas a 2008	72
Table 4.7 Ênfases das CLC relativas a 2013	72

Índice de figuras

Figure 2.1 COSO Cube	22
Figure 2.2 COSO ERM Cube	25
Figure 3.1 Categorias de risco	53
Figure 3.2 As quatro linhas de defesa das instituições financeiras	64

Lista de Abreviaturas

AAA - *American Accounting Association*
AICPA - *American Institute of Certified Public Accountants*
AS2 – *Auditing Standard n. ° 2*
AS5 – *Auditing Standard n. ° 5*
BANIF – Banco Internacional do Funchal, S.A.
BBVA – Banco Bilbao Vizcaya Argentaria, S.A
BCP – Banco Comercial Português, S.A.
BES – Banco Espírito Santo, S.A.
BIC – Banco Internacional de Crédito (Português), S.A.
BPN – Banco Português de Negócios, S.A.
CCAM – Caixa de Crédito Agrícola Mútuo, CRL
CCCAM – Caixa Central de Crédito Agrícola Mútuo, CRL
CCO – *Chief Compliance Officer*
CEBS - *Committee of European Banking Supervisors*
CEO – *Chief Executive Officer*
CFO – *Chief Financial Officer*
CLC – Certificação Legal de Contas
CSC – Código das Sociedades Comerciais
CMVM – Comissão de Mercados e Valores Mobiliários
CNSA – Conselho Nacional de Supervisão de Auditoria
CNSF - Conselho Nacional de Supervisores Financeiros
COBIT - *Control Objectives for Information and Related Technology*
COSO - *Committee of Sponsoring Organizations of the Treadway Commission.*
DRA – Diretriz Revisão/Auditoria
EAD – *Exposure at Default*
EBA – *European Banking Authority*
ERM - *Enterprise Risk Management*
ESFG – Espírito Santo Financial Group
ESI - Espírito Santo Internacional, S.A.
EUA - Estados Unidos da América
GAAS – *Generally Accepted Auditing Standards;*
IAASB – *International Auditing and Assurance Standards Board;*

ICAAP – *Internal Capital Adequacy Assessment Process*
IFAC – *International Federation of Accountants;*
IG – *Internal Governance Guideline*
IIA - *Institute of Internal Auditors*
IRB – *Internal Ratings Based-approach*
ISA – *International Standard Audit*
ISACA - *Information Systems Audit and Control Association*
IT – *Information Technology*
ITGI – *Information Technology Governance Institute*
KRI - *Key Risk Indicators*
LGD – *Lost Given Default*
MAR – *Modelo de Avaliação de Riscos*
NAA - *National Association of Accountants*
OIP – *On-site Inspections Programme*
PCAOB - *Public Company Accounting Oversight Board*
PG – *Probably of Default*
PWC – *PricewaterhouseCoopers*
RJIPSP – *Regime Jurídico das Instituições de Pagamento e dos Serviços de Pagamento*
RGICSF – *Regime Geral das Instituições de Crédito e das Sociedades Financeiras*
ROC – *ROC*
RWA – *Risk-weighted Asset*
SEC - *Security and Exchange Comission*
SICAM - *Sistema Integrado do Crédito Agrícola Mútuo*
SIP – *Special Inspections Programme*
SOX - *Lei de Sarbanes-Oxley*
SROC – *Sociedade de Revisores Oficiais de Contas*
TI – *Tecnologias da Informação*
U.E. – *União Europeia*
VS.- *versus*

1. Introdução

No âmbito do Mestrado em Auditoria e com vista à sua conclusão, foi realizada a presente dissertação, que mais do que a obtenção do grau de mestre, me permite o desenvolvimento e consolidação de conhecimentos sobre controlo interno, bem como das devidas adaptações que foram ocorrendo ao longo dos tempos, tanto para as organizações de um modo geral, como no que concerne às especificidades exigidas pelas entidades reguladoras para as instituições financeiras.

O desenvolvimento pessoal é desde já a expectativa principal que este trabalho se propõe cumprir, permitindo-me uma boa arguência, bem estruturada e fundamentada e capaz de suscitar o interesse dos demais.

O estudo que se pretende analisar, no entanto, surge apenas do levantamento de uma curiosidade meramente académica, tendo por objetivo estabelecer uma relação entre o uso de modelos de gestão de risco, enquanto ferramenta para obter um bom sistema de controlo interno, e os resultados das auditorias. Para o efeito, iremos analisar o caso das instituições financeiras, uma vez que sabemos que o Banco de Portugal, através do Aviso n.º 5/2008, obriga à adoção de um sistema de controlo interno suportado no *Internal Control Integrated Framework*, publicado pelo *Committee of Sponsoring Organizations of the Treadway Commission*, pelo que desta forma, poderemos canalizar o nosso estudo e, consequentemente, as nossas conclusões para a área financeira.

Assim, pretende-se perceber se estes modelos de gestão de risco se adequam à realidade das instituições bancárias portuguesas e se o seu uso acresce valor, na medida em que deverão constituir uma ferramenta de apoio à gestão, minimizando os riscos na tomada de decisão e conferindo uma maior transparência à informação, reforçando, assim, a imagem da organização e captando o interesse dos investidores.

O controlo interno tem assumido um papel preponderante nas organizações e surge da necessidade de gerir o risco do negócio com vista ao alcance dos objetivos definidos, de forma mais eficiente e económica.

Este conceito, ao longo dos anos, tem vindo a dar uma maior relevância aos instrumentos de gestão de risco usados pela administração para identificar, avaliar e controlar os riscos relacionados com a atividade da organização, de modo a ir de encontro aos objetivos e metas definidos, salvaguardando o cumprimento de regras e estratégias estabelecidas no planeamento estratégico. A existência de um bom sistema de controlo interno tem, desde

então, assumido uma importância crescente nas organizações, não só pela necessidade da Gestão de controlar os processos e melhorar a eficácia e eficiência dos seus recursos, mas também para ir de encontro aos interesses dos restantes *stakeholders*, já que estes, para se relacionarem com uma empresa, necessitam de confiar na informação divulgada e no modo em como a Gestão conduz os seus negócios. Assim, este é um tema que, cada vez mais, merece a atenção de todos os agentes de mercado. O uso dos modelos de gestão de risco vem atender às exigências do mercado, tornando-se uma ferramenta de aceitação generalizada, quer por parte das entidades, já que apoiam os gestores na identificação e gestão dos riscos e credibilizam a informação, permitindo a tomada de decisões conscientes e alinhadas com os objetivos da organização, quer pelos auditores, conferindo uma maior qualidade ao seu trabalho, já que estes conseguem uma melhor e mais rápida avaliação do sistema de controlo interno, podendo dispensar mais tempo a aprofundar outras questões. Por outro lado, estes modelos deverão servir de referencial aos auditores na execução do seu trabalho de revisão aos processos, na hierarquização dos riscos e avaliação dos controlos.

Para as entidades bancárias, em particular, o *Basel Committee*, desde 1998 tem vindo a reforçar a importância do controlo interno para reduzir ou minimizar o risco operacional. O Basileia III vem reforçar ainda mais a necessidade de existência de um sistema de controlo interno e de gestão de risco dentro das instituições, o que tem vindo a refletir-se numa regulação bastante “apertada”. Simultaneamente, o Banco de Portugal, tem vindo também a definir diretrizes sobre este tema, através da publicação de Avisos.

No próximo capítulo será apresentado o conceito e importância do controlo interno, bem como o contributo da *Lei Sarbanes Oxley* e de outros organismos, como o já referido *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e o *Information Systems Audit and Control Association* (ISACA), com a publicação de *Frameworks* para gestão de riscos.

No terceiro capítulo, iremos fazer um enquadramento atual do controlo interno para o caso específico da Banca, em que serão abordados o impacto das medidas tomadas pelo *Basel Committee*, nomeadamente, através dos Acordos Basileia e da publicação do *Framework for Internal Control Systems in Banking Organisations*, e das orientações de *Internal Governance* divulgadas pelo *Committee of European Banking Supervisors* (CEBS). Será ainda efetuado um estudo sobre o controlo interno em Portugal e das publicações do Banco

de Portugal, nomeadamente o Modelo de Avaliação de Riscos (MAR), uma ferramenta de suporte à avaliação dos riscos a ser usada pelo supervisor, e do Aviso n.º 5/2008, o qual estabelece um conjunto de princípios orientadores à implementação e manutenção de um sistema de controlo interno, procedendo, complementarmente, à uniformização dos relatórios de controlo interno a enviar, quer ao Banco de Portugal, quer à Comissão do Mercado de Valores Mobiliários (CMVM), quanto à estrutura, conteúdo e prazos de reporte dos mesmos.

No quarto capítulo iremos desenvolver um caso empírico, onde será apresentado o problema de investigação, a metodologia a utilizar e razões que suportaram a sua escolha. Serão também analisados os resultados obtidos face às limitações encontradas.

Por último, tiraremos as nossas conclusões sobre a generalidade dos conceitos retidos em resultado do trabalho desenvolvido ao longo desta dissertação, que este, sim, é o objetivo principal de um académico.

2. O controlo interno nas organizações em geral

2.1 – Enquadramento teórico

Todas as organizações enfrentam riscos significativos, desde falhas no seu funcionamento, passando pelo uso indevido de ativos até à incorreta e incompleta preparação da informação financeira (Rittenberg, Johnstone e Gramling, 2010). Estes riscos precisam ser mitigados e, para tal, necessitam de controlos internos.

A primeira definição de controlo interno surgiu em 1934, através do *American Institute of Certified Public Accountants* (AICPA) e foi também a reconhecida pela *Security and Exchange Commission* (SEC):

O controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas adotadas num negócio a fim de garantir a salvaguarda de ativos, verificar a adequação e confiabilidade dos dados contabilísticos, promover a eficiência operacional e encorajar a adesão às políticas estabelecidas pela gestão¹ (*apud* Morais e Martins, 2013: 28).

De acordo com Moeller (2005), as décadas de 1970 e 1980, constituíram um período de falência de grandes empresas nos Estados Unidos da América (E.U.A), devido a fatores como inflação elevada, a consequente subida nas taxas de juro e aos custos de energia elevados resultantes de medidas governamentais, tendo-se verificado, em alguns casos, a existência de relatórios financeiros fraudulentos que haviam sido atestados por auditores externos. Em resposta às preocupações que se faziam sentir, em 1985 é formado o *National Commission on Fraudulent Financial Reporting*, que mais tarde viria a chamar-se *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Esta organização, também conhecida por *Treadway Commission*, era representada por organismos internacionais, como o AICPA, a *American Accounting Association* (AAA), a *National Association of Accountants* (NAA), o *Financial Executives International* (FEI), o *The Associations for Accountants and Financial Professionals in Business* e o *Institute of Internal Auditors* (IIA), e tinha como objetivo inicial a identificação dos fatores que permitiram o reporte financeiro fraudulento. O relatório resultante desta análise, emitido em 1987, incluía recomendações aos gestores e quadros de direção, aos profissionais de auditoria, entre outros, e apelava a que os relatórios de gestão se referissem aos sistemas de

¹ SAS n.º 1, updated at 2002

controlo interno, enfatizando os elementos essenciais para a existência de um controlo interno efetivo: ambiente de controlo, código de conduta, um Comité de Auditoria competente e envolvido, e um forte departamento de auditoria interna (ibid.:1). Esta comissão constatou assim que não existia uma definição de controlo interno consistente e, juntamente com outros especialistas externos, lançou-se num novo projeto que visava a obtenção de um novo conceito de controlo interno. Esta combinação de esforços, durante, aproximadamente 20 anos, resultou, em 1992, na publicação de um primeiro estudo sobre o controlo interno, o *Internal Control - Integrated Framework*, hoje em dia conhecido por metodologia COSO.

Em 1996, face à crescente dependência das tecnologias, o ISACA, adapta a estrutura do anteriormente citado COSO para ambientes mais tecnológicos, criando o *Control Objectives for Information and Related Technology* (CobiT), que surge como referencial focado nas Tecnologias de Informação (TI).

No início do Século XXI, uma nova onda de escândalos financeiros vem destabilizar os mercados financeiros. A falência de grandes empresas, tais a *Enron* - cujo facto de não terem sido detetadas quaisquer anomalias ou irregularidades nas auditorias efetuadas, dada a gravidade dos seus esquemas fraudulentos a nível contabilístico, levou à suspeita de conivência por parte da *Arthur Andersen* e, conseqüentemente, à sua saída do mercado - e a *Worldcom*, terminaram na condenação e detenção de vários gestores executivos. Para restaurar a confiança dos investidores, o governo dos EUA publicou, em 2002, a lei *Sarbanes-Oxley* ou *Sarbanes Oxley Act* (SOX)², proposta por Paul Sarbanes, democrata e senador de Maryland, e Michael Oxley, republicano e senador de Ohio. Esta lei destinava-se às empresas cotadas em bolsa de valores dos EUA, a SEC, e visava assegurar práticas éticas de negócio, fomentadas por uma gestão consciente, responsável e sustentável (Oliveira: 2011).

Moeller (2008) considera que uma das componentes principais da SOX foi a criação do *Public Company Accounting Oversight Board* (PCAOB), um organismo independente, com o objetivo de criar e estabelecer normas de auditoria e de prestação de contas. A SOX vem ainda rever os procedimentos de *Corporate Governance* para empresas cotadas, nacionais e estrangeiras, especialmente os relacionados com o relato financeiro. Esta lei

² Oficialmente denominada de *Public Company Accounting Reform and Investor Protection Act*

foi, sem dúvida, a grande alavanca ao conceito de controlo interno, desde o COSO, já que foi este o tema que esteve no foco das suas preocupações.

Em 2004, à metodologia COSO de 1992, foi introduzido o conceito *Enterprise Risk Management* (ERM), orientando os processos não só numa perspetiva de *compliance* mas também para a criação de valor.

2.2 – Os principais requisitos da Lei Sarbanes-Oxley

Ao longo dos seus 11 títulos, que totalizam 69 secções (artigos), a SOX impõe que as empresas aumentem os seus controlos, de modo a que estes possam conferir uma maior segurança e transparência sobre o modo como os órgãos de gestão estão a conduzir o negócio, bem como à informação por eles divulgada.

Ao longo deste subcapítulo, iremos analisar as secções da SOX que consideramos mais importantes, com base na avaliação de Moeller (2005 e 2008) e na leitura da própria lei. No entanto, por agora centrar-nos-emos apenas no estudo das secções 301, 302, 401, 404, 407, 409, 802, 806, 906 e 1105, já que a criação do PCAOB, enquanto organismo emissor de normas de auditoria e revisor do trabalho dos auditores, merece especial relevo, sendo tratado separadamente, dada a necessidade de fazer um enquadramento sobre as responsabilidades e requisitos do auditor, atendendo ao objetivo deste trabalho.

Título III – Responsabilidades da empresa

Secção 301: Independência do Comité de Auditoria

Estabelece que as sociedades têm de dispor de um Comité de Auditoria³ que apenas pode ser composto por membros do Conselho de Administração independentes e é diretamente responsável pela nomeação, remuneração, supervisão e avaliação do trabalho dos auditores externos, bem como pelo tratamento das deficiências reportadas de controlo interno, fraude, contabilidade e auditoria, podendo decidir recorrer a consultores externos, se assim o entenderem. Deve supervisionar todos os processos de controlo interno e a elaboração e divulgação das demonstrações financeiras, sendo também responsáveis pela existência de procedimentos relativos à receção, retenção e tratamento de reclamações relacionadas com controlo interno, contabilidade e auditoria recebidas pelas entidades reguladoras, bem como estabelecer programas de *whistleblowing* que assegurem a confidencialidade e

³ Comité ou Comissão de Auditoria

anonimato dos empregados que reportem fraudes financeiras ou preocupações relativas à contabilidade e auditoria – *raising concerns*.

Secção 302: Responsabilidade corporativa pelos reportes financeiros (numa perspetiva de correção e veracidade)

Determina que o CFO e o CEO devem incluir nos reportes financeiros periódicos certificação de como reviram a informação reportada e de que as demonstrações financeiras e informação relacionada apresentam de forma verdadeira a posição financeira e os resultados da empresa e que esta não contém distorções ou omissões materialmente relevantes. Estes devem assumir a responsabilidade pela implementação e avaliação do controlo interno e apresentar uma lista das deficiências encontradas. Devem ainda reportar quaisquer fraudes relacionadas com empregados que estejam envolvidos nas atividades internas da empresa. Por último, devem ainda informar quaisquer alterações nos controlos internos ou fatores que os possam afetar negativamente, ocorridos com data subsequente à da sua avaliação.

Título IV -Melhoria nas divulgações financeiras

Secção 401:As divulgações nos reporte periódicos

As demonstrações financeiras publicadas pelos seus emitentes devem ser precisas e apresentadas de uma maneira que não contenha incorreções ou omita factos materialmente relevantes. Os relatórios trimestrais ou anuais devem divulgar todos os ajustamentos materiais identificados pelos auditores não reconhecidos no balanço, tais como transações, acordos, obrigações realizadas com entidades não consolidadas, contingências e outras. O Comité de Auditoria deve levar a cabo uma análise da extensão das divulgações fora do balanço e reportar as suas conclusões, permitindo a transparência da informação. As informações financeiras não relacionadas com a manutenção de princípios contabilísticos geralmente aceites e outras leis devem ser também incluídas neste relatório.

Secção 404: Relatórios de controlo interno

Prevê a existência de um relatório de controlo interno em cada relato anual afirmando a responsabilidade da gestão por criar e manter um adequado sistema de controlo interno para o relato financeiro, bem como pela avaliação da eficácia do mesmo. Esta avaliação deve ser atestada pelos auditores externos, a qual deve seguir os procedimentos das *Auditing Standards* (AS) emitidas pelo PCAOB. Os auditores externos pronunciar-se-ão

sobre a eficácia do Comité de Auditoria e a avaliação de controlo interno efetuada no decorrer da própria auditoria, bem como do próprio trabalho dos auditores internos, podendo, no final, optar pela utilização do trabalho destes ou não.

Secção 407: Especialista financeiro

Um dos membros do Comité de Auditoria deve ser um especialista financeiro.

Secção 409: Divulgações em tempo real

As empresas devem divulgar publicamente, de forma rápida, permanente e facilmente entendível, todas as alterações com impactos materiais na sua posição financeira ou nas suas operações.

Título VIII – Responsabilidades Criminais e da empresa por fraude financeira

Secção 802: Penalidades criminais por alteração de documentos

Impõe multas e sanções, bem como detenção até 20 anos, por alterar, destruir, falsificar documentos ou registos com a intenção de obstruir, impedir ou influenciar uma vistoria legal. Estabelece multas e sanções, ou ainda prisão até 10 anos, para violação da manutenção dos papéis de trabalho de auditoria ou revisão por um prazo mínimo de 5 anos.

Secção 806: Proteção para os whistleblowers

Introduz medidas de proteção civil contra ações de retaliação em caso de denúncia de fraude, aplicáveis para empregados e auditores.

Título IX - Aumento das penalidades para crimes de colarinho branco

Secção 906: Responsabilidades corporativas pelos reportes financeiros (numa perspetiva de fraude)

O CEO e o CFO devem certificar as demonstrações financeiras e as suas divulgações em como estas representam de forma verdadeira, em todos os aspetos materialmente relevantes, a posição financeira e os resultados da empresa.

A penalização máxima passa a ir aos 20 anos, por crimes de fraude, uso de informações privilegiadas, subornos e outras atividades ilícitas praticadas, nomeadamente em transações com títulos.

Título XI – Fraudes empresariais e responsabilidades

Secção 1105: Proibição de exercer cargos executivos e de direção

A SEC pode ainda requerer a inibição de pagamento de prémios aos administradores condenados e impedi-los de exercer funções de direção ou administração em outras empresas cotadas.

Em suma, a SOX veio não só requerer um maior rigor e uma maior transparência na divulgação dos resultados das empresas, como também obrigar a um maior envolvimento por parte dos seus executivos, quer pelas contas reportadas, quer pela implementação, manutenção e avaliação do controlo interno, responsabilizando-os criminalmente por fraude financeira. Paralelamente, vem regular a atuação dos auditores, atestando maior credibilidade aos relatórios de auditoria e, conseqüentemente, à profissão.

2.2.1 – A criação do PCAOB e a independência do auditor

A SOX introduziu uma mudança total no processo de emissão de normas de auditoria externa e de revisão do trabalho dos auditores. Criado na sequência desta lei, o PCAOB é o organismo responsável por autorregular e supervisionar os auditores das empresas emittentes de valores mobiliários, i.e., registados na SEC. Convém, no entanto, realçar que a SEC está acima do PCAOB e que as normas delineadas pelo PCAOB estão sujeitas à sua revisão.

Outro facto que gostaríamos de relevar é que, nos anos que antecederam esta lei, a independência do auditor foi passada para segundo plano. Moeller (2005) acredita que este desleixo se deveu, essencialmente, ao facto de as empresas de auditoria terem promovido os serviços de consultoria, pois estes eram mais rentáveis.

Nos seus primeiros títulos (I e II), a SOX refere-se à criação do PCAOB e às grandes mudanças de perspectiva na independência dos auditores, pelo que, para melhor compreendermos o que atrás foi relatado, convém, agora, fazer uma análise das principais secções abrangidas por estes títulos:

Título I – *Public Company accounting Oversight Board*

Secção 101: Criação do PCAOB

São definidas as regras para a criação do PCAOB, incluindo requisitos dos membros constituintes:

O PCAOB é constituído por 5 membros apontados pela SEC, os quais não podem ser membros do governo, dos quais 3 não CPA's (*Certified Public Accountant*), já que este organismo deve, também ele, manter a sua independência. Do mesmo modo, o presidente do PCAOB não pode ter sido membro CPA ou exercido atividade há menos de 5 anos. Defende que os seus membros devem ser maioritariamente advogados e ter conhecimentos de regulação.

As principais responsabilidades do PCAOB são:

- Aceitar ou rejeitar o registo das empresas de auditoria;
- Emitir ou adotar normas de auditoria que considerem, para além da qualidade dos controlos, a ética e independência dos auditores;
- Conduzir inspeções às empresas de auditoria registadas;
- Conduzir investigações e procedimentos disciplinares, impor sanções, quando justificável, às empresas de auditoria e às pessoas que com elas se relacionam;
- Exercer outras funções que lhe sejam mandatadas para melhorar as normas existentes e a qualidade das auditorias, com o intuito de proteger os interesses dos investidores e do público em geral.
- Reforçar o cumprimento das regras da SEC, que se encontram por trás da lei SOX.
- Definir um orçamento e gerir a sua atuação de acordo com os recursos humanos disponíveis.

Secção 103: Normas de Auditorias, de Controlo de Qualidade e Independência

O PCAOB deve desenvolver normas que contenham os seguintes requisitos:

- Retenção de papéis de trabalho de auditoria por um prazo nunca inferior a sete anos;
- Cada relatório de auditoria emitido deve ser aprovado pelo *partner* da empresa de auditoria de modo a que este dê a sua opinião e ateste que as conclusões da auditoria foram formadas de acordo com as normas de auditoria geralmente aceites (GAAS⁴);
- Cada relatório de auditoria deve descrever o âmbito e extensão dos testes de controlo interno, bem como os resultados destes;

⁴ *Generally Accepted Auditing Standards*

- Orientações para a revisão e avaliação dos controles internos. A versão final das normas emitidas pelo PCAOB, *Auditing Standards*, segue como modelo de controle interno o COSO. A avaliação de controle interno deve conter uma descrição das fraquezas materiais e dos requisitos não cumpridos detetados no decurso dos testes efetuados. Este ponto levanta a necessidade de os relatórios de controle interno serem mais detalhados e compreensíveis;
- Controlo de qualidade a serem adotados pelas empresas de auditoria, requisitos que, de acordo com a SOX, abrangem temas como a monitorização da ética profissional e independência, procedimentos para recorrer a consultores externos, a supervisão do trabalho de auditoria, o recrutamento, desenvolvimento profissional e carreira dos auditores, procedimentos para aceitação e continuação de auditorias (cartas-compromissos), realização de inspeções internas de qualidade, entre outros normas de qualidade previstas no PCAOB;
- Independência do Auditor, de acordo com o necessário e apropriado no interesse público e de proteção dos investidores (remete para o Título II)

Secção 104: Inspeções das empresas de auditoria registadas

As inspeções do PCAOB devem focar-se na *performance* das empresas de auditoria, para as auditorias selecionadas, e na revisão dos relatórios de auditoria respetivos. Estas revisões são potenciadas para identificar algum ato ou omissão que constitua uma violação das regras estabelecidas e para avaliar as políticas de controlo de qualidade dessas empresas de auditoria, devendo ocorrer com uma frequência anual para empresas que emitam mais de cem relatórios de auditoria por ano; nos casos, em que sejam emitidos cem relatórios ou menos, deve ser considerada uma regularidade de, pelo menos, uma inspeção em cada três anos (Moeller, 2005).

Secção 108: Normas de Auditoria

A SEC é a autoridade final reguladora da profissão do auditor, ou seja, está acima do PCAOB, já que lhe compete dar a aprovação final às normas, tem capacidade de modificar as ações do PCAOB e para destituir ou substituir os membros que o compõem.

Título II – Independência do Auditor

Secção 201: Serviços fora do âmbito do trabalho do auditor

Proíbe que as empresas de auditoria registadas prestem simultaneamente serviços de auditoria e não auditoria a um mesmo cliente, tais como, serviços de auditoria interna, contabilidade, de desenho e implementação de sistemas de informação, gestão de recursos humanos, serviços atuariais, aconselhamento jurídico-financeiro e bancário, consultoria de investimentos, entre outros.

Secção 202: Pré-aprovação de serviços por parte do Comité de Auditoria

O Comité de Auditoria deve aprovar todos os serviços de auditoria e não-auditoria antes da contratação dos mesmos. Os membros do Comité de Auditoria ficam expostos criminalmente ou perante os acionistas por permitirem ações ilícitas.

Secção 203: Rotação dos auditores externos

O *partner* responsável ou o *partner* revisor de uma empresa de auditoria não pode conduzir os trabalhos de auditoria por mais de 5 anos consecutivos, para um mesmo cliente.

Secção 204: Reporte dos auditores externos ao Comité de Auditoria

Os auditores externos devem reportar ao Comité de Auditoria, numa base permanente os resultados críticos do seu trabalho, no que se refere às políticas contabilísticas, boas práticas a serem implementadas, tratamentos contabilísticos alternativos discutidos com a gestão, mantendo o Comité de Auditoria informado de todas as ações a ser tomadas.

Secção 206: Conflitos de Interesse

Os auditores externos estão proibidos de prestar serviços de auditoria a uma empresa cujo CEO, CFO ou responsável da contabilidade tenha sido membro dessa empresa de auditoria, no ano anterior à auditoria.

Contudo, a normalização do PCAOB nem sempre foi pacífica, principalmente no que se refere ao uso das metodologias de risco que suportam a avaliação dos controlos internos. Como já foi dito, aquando da análise da *secção 404*, o auditor deve fazer uma revisão e avaliação do controlo interno, suportadas nas normas do PCAOB, particularmente na *Auditing Standard n.º 2 (AS2)* denominada “Uma auditoria ao controlo interno sobre o relato financeiro realizada em conjunto com uma auditoria às demonstrações financeiras”. Esta lei foi fortemente criticada, nomeadamente, na medida em que considerava o *COSO Framework* como a metodologia a ser usada para compreender e avaliar os controlos

internos. Apesar de reconhecida em todo o mundo, o COSO não era o único *Framework* e, talvez, nem o melhor ou o mais fácil de usar em alguns casos (Moeller, 2005). Era necessário, todavia, que o uso da metodologia fosse de encontro aos requisitos da SOX. Em resposta às várias reclamações dos seus utilizadores, a SEC e o PCAOB concordaram em rever esta norma e, em Maio de 2007, o PCAOB divulga uma nova norma, a AS5, com o título “Uma Auditoria ao Controlo Interno sobre o Relato Financeiro que está integrada com uma Auditoria às Demonstrações Financeiras”. Esta norma, na sua introdução, estabelece que

[o] auditor deve usar, no seu trabalho de auditoria aos controlos internos sobre os relatórios financeiros, o mesmo *framework* de controlo reconhecido como adequado e utilizado pela Gestão para a sua avaliação anual da eficácia dos mesmos⁵. (Moeller, 2008:58)

Esta nota preliminar vem alterar a filosofia que existia até então e corrigir alguns problemas do passado, já que reconhece o uso de outras metodologias de controlo, tais como, o ERM e o CobiT.

2.2.2 – Outros aspetos relevantes de *Corporate Governance*

Apesar de a preocupação primordial do PCAOB ter sido a regulação da profissão do auditor externo que lhe havia sido delegado pela SEC, não podemos ignorar o impacto que a SOX teve na profissão dos auditores internos, particularmente, nos das empresas cotadas em bolsa. Moeller (2005) refere a este propósito que, os auditores internos passam a ter de atuar de um modo diferente nas negociações com o Comité de Auditoria, os gestores séniores e os auditores externos. Este autor acrescenta ainda que, o auditor interno moderno deve compreender a generalidade das disposições impostas pela SOX. Assim, a lei SOX, determina, ao longo dos seus títulos, que a empresa deve ter uma função de auditoria competente e eficaz, para assegurar a monitorização e revisão de *compliance*.

As empresas estão, no entanto, cada vez mais, sujeitas ao cumprimento de requisitos regulatórios, quer estes sejam de controlo interno ao nível de processos internos de relato financeiro, quer em matéria de *Governance*. Como resultado, algumas dessas empresas adotaram uma função de *Chief Compliance Officer* (CCO) como parte integrante dos órgãos de gestão, com o intuito de verificar o cumprimento da SOX, bem como de outras

⁵ Tradução da autora. No original: *The auditor should use the same suitable, recognized control framework to perform his or her audit of internal control over financial reporting as management uses for its annual evaluation of the effectiveness of the company's internal control over financial reporting.*

leis e regulamentos que têm impacto no seu dia-a-dia. Esta é uma função que deverá atuar com independência e que privilegia de uma proximidade à Administração e ao Comité de Auditoria, tendo como objetivo assegurar que os quadros de direção, gestores séniores e os demais envolvidos estão a cumprir com as leis e regulamentos das entidades reguladoras, que as políticas e procedimentos da empresa estão a ser seguidos e que os comportamentos dentro da organização estão de acordo com o código de conduta. O CCO deve identificar áreas vulneráveis e de risco, rever políticas, procedimentos e o código de conduta sempre que estes se mostrem desajustados, tal como desenvolver e implantar medidas corretivas necessárias para resolver problemas de *compliance*. Para além disso, o CCO deve receber as comunicações das partes que queiram fazer denúncias ou reportar preocupações, após terem sido esgotados os outros canais para o efeito. Outra das suas responsabilidades é, juntamente com o responsável de Recursos Humanos, promover ações de formação aos funcionários. Deve providenciar regularmente à Administração relatórios sobre o seu trabalho, no entanto, tem também a obrigação de reportar violações ou potenciais violações às agências apropriadas.

2.3 – A internacionalização das normas de auditoria

A auditoria funciona para servir o interesse público mas também tem por objetivo melhorar as operações das empresas auditadas. A auditoria é uma profissão única (Rittenberg [et all], 2010).

Quando falamos de auditores, podemos estar a falar tanto de multinacionais de auditoria, como de um profissional único, especialista em finanças, auditores externos ou auditores internos, de modo que, não é difícil compreender que algumas organizações de profissionais e reguladoras tenham vindo a interessar-se pela regulação dos serviços de auditoria.

Conforme já referido anteriormente, antes da SOX, o AICPA era o organismo que formalmente tinha a responsabilidade pela profissão de auditoria nos EUA. As normas de auditoria eram baseadas em GAAS e eram denominadas *Statements of Auditing Standards* (SAS). Muitas delas eram apenas boas práticas de auditoria, resultando em diretrizes para a profissão. O código de conduta definido pelo AICPA estabelecia que os auditores deveriam seguir e cumprir com as SAS sempre que aplicáveis. AS GAAS e as SAS aceites pela SEC, constituíram os alicerces para uma revisão e testes necessários para a

certificação da profissão de auditor. Com a SOX, o processo de normalização de auditoria passa das mãos do AICPA para o PCAOB. No entanto, o AICPA continua a desenvolver normas de auditoria para entidades não-públicas. Administra ainda programas de formação contínua, dando especial atenção ao tema da fraude e prepara o exame para certificação de auditores.

Na mesma linha, o *International Federation of Accountants* (IFAC), uma organização internacional de contabilidade, composta por mais de 175 membros e associados em mais de 130 países, reorganizou o anterior *International Auditing Practices Committee* (IAPC), em 2002, e criou uma comissão permanente, o *International Auditing and Assurance Standards Board* (IAASB). Este é um organismo de normalização independente que serve o interesse público, estabelecendo padrões internacionais de alta qualidade para a auditoria e fornecendo orientações aos auditores sobre as novas exigências do mercado financeiro, através da emissão das *International Standards on Auditing* (ISA). O IAASB facilita a convergência da auditoria internacional e nacional e melhora a qualidade e consistência da sua prática em todo o mundo, fortalecendo, em simultâneo, a confiança pública na auditoria global e na profissão. O IAASB pretende harmonizar as normas de auditoria a nível internacional e trabalha diretamente com o AICPA e o PCAOB.

Em Setembro de 2012, a Comissão Europeia comunicou a sua intenção de que fossem aplicadas as ISA's no espaço europeu, medida essa que tem tido grande aceitação por toda a Europa., incluindo por Portugal.

O objetivo de uma auditoria às demonstrações financeiras é o de permitir que o auditor expresse uma opinião sobre se as demonstrações financeiras estão preparadas, em todos os aspetos materialmente relevantes, de acordo com as normas de relato aplicáveis, no intuito de aumentar a confiança aos utilizadores da informação financeira nas mesmas. As ISA's no seu conjunto estabelecem orientações para o trabalho do auditor de modo a que este possa cumprir este objetivo. Na condução de uma auditoria, o objetivo final do auditor é o obter segurança razoável sobre se as demonstrações financeiras, como um todo, estão isentas de distorções materiais, devido a erros ou fraude, e de garantir que o seu trabalho foi realizado, e o resultado deste reportado, de acordo com as normas de auditoria vigentes. Embora a Ordem dos Revisores Oficiais de Contas (OROC) tenha vindo a traduzir e a divulgar as ISA's, através do Manual do Revisor Oficial de Contas, nos últimos anos, houve necessidade, de constituir uma Comissão de Revisão da Tradução das ISA's que envolvesse ou consultasse, no processo de tradução das ISA, os *key stakeholders* tais como

as Sociedades de Revisores Oficiais de Contas (SROC), a OROC e o Conselho Nacional de Supervisão de Auditoria (CNSA) onde estão representadas as autoridades públicas.

As ISA's resumem-se então num documento denominado de “Normativo Técnico a Adotar pela União Europeia”, o qual iremos transpor na tabela 2.1, que se segue:

Table 2.1 O Normativo técnico de auditoria

<u>Normativo Técnico</u>
<i>ISA 200: Objetivos Gerais do Auditor Independente e a Condução de uma Auditoria de Acordo com as Normas Internacionais De Auditoria</i>
<i>ISA 210: Aceitar os Termos de Trabalhos de Auditoria</i>
<i>ISA 220: Controlo de Qualidade para Auditorias de Informação Financeira Histórica</i>
<i>ISA 230: Documentação de Auditoria</i>
<i>ISA 240: A Responsabilidade do Auditor Relativa à Fraude numa Auditoria de Demonstrações Financeiras</i>
<i>ISA 250: Consideração de Leis e Regulamentos numa Auditoria de Demonstrações Financeiras</i>
<i>ISA 260: Comunicações aos Encarregados da Governação</i>
<i>ISA 265: Comunicar Deficiências no Controlo Interno aos Encarregados da Governação e à Gerência</i>
<i>ISA 300: Planear uma Auditoria de Demonstrações Financeiras</i>
<i>ISA 315: Identificar e Avaliar os Riscos de Distorção Material por Meio da Compreensão da Entidade e do seu Ambiente</i>
<i>ISA 320: Materialidade no Planeamento e Execução de uma Auditoria</i>
<i>ISA 330: As Respostas do Auditor aos Riscos Avaliados</i>
<i>ISA 402: Considerações de Auditoria Relativas a Entidades que usem Organizações de Serviços</i>
<i>ISA 450: Avaliação de Distorções Identificadas Durante uma Auditoria</i>
<i>ISA 500: Prova de Auditoria</i>
<i>ISA 501: Prova de Auditoria - Considerações Adicionais para Itens Específicos</i>
<i>ISA 505: Confirmações Externas</i>
<i>ISA 510: Trabalhos de Auditoria Iniciais - Saldos de Abertura</i>
<i>ISA 520: Procedimentos Analíticos</i>
<i>ISA 530: Amostragem de Auditoria</i>
<i>ISA 540: Auditoria de Estimativas Contabilísticas, Incluindo Estimativas Contabilísticas do Justo Valor e Divulgações Relacionadas</i>
<i>ISA 550: Partes Relacionadas</i>
<i>ISA 560: Acontecimentos Subsequentes</i>
<i>ISA 570: Continuidade</i>
<i>ISA 580: Declarações Escritas</i>
<i>ISA 600: Considerações Especiais – Auditorias de Demonstrações Financeiras de Grupos (Incluindo o Trabalho do Auditor do Componente)</i>
<i>ISA 610: Considerar o Trabalho de Auditoria Interna</i>
<i>ISA 620: Usar o Trabalho de Um Perito do Auditor</i>
<i>ISA 700: Formar uma Opinião e Relatar sobre Demonstrações Financeiras</i>
<i>ISA 705: Modificações à Opinião no Relatório do Auditor Independente</i>
<i>ISA 706: Parágrafos de Ênfase de Matéria e Outros Parágrafos de Matéria no Relatório do Auditor Independente</i>
<i>ISA 710: Informação Comparativa – Números Correspondentes e Demonstrações Financeiras Comparativas</i>
<i>ISA 720: Outras Informações em Documentos que Contenham Demonstrações Financeiras Auditadas</i>
<i>ISQC 1: Controlo de Qualidade para Firmas que Executam Auditorias e Exames Simplificados de Informação Financeira Histórica, e Outros Trabalhos de Garantia de Fiabilidade e de Serviços relacionados.</i>

Fonte: Adaptado de “A Adopção das Normas Internacionais de Auditoria da IFAC”, Revisores e Auditores

No que se refere aos aspetos anteriormente abordados pela SOX, fica bem patente a harmonização internacional que existe em torno das normas de auditoria, particularmente

no que se refere à observância do requisito de independência do auditor, bem como à condução dos trabalhos, retenção da documentação e emissão dos relatórios. Adicionalmente, as ISA's também têm uma norma relativa à qualidade das auditorias realizadas por empresas de auditoria.

2.4 – O Committee of Sponsoring Organizations of the Treadway Commission: O Internal Control Integrated Framework e o Enterprise Risk Management

2.4.1 – O Internal Control - Integrated Framework

Apesar de o termo “controle interno” fazer, desde há muito, parte do nosso vocabulário empresarial é o COSO que vem conseguir uma definição de aceitação quase generalizada.

O COSO *Framework* define controle interno como

[u]m processo levado a cabo pelo Conselho de Administração, Direção e outro pessoal, desenhado para proporcionar segurança razoável com vista ao alcance dos objetivos nas seguintes categorias: (1) fiabilidade do relato financeiro, (2) aderência às leis e regulamentos aplicáveis, (3) eficácia e eficiência das operações.⁶ (Rittenberg [et al], 2010: 192)

Deste modo, o controle interno permite à organização alcançar os seus objetivos principais, assegurar que as operações relacionadas com a sua estratégia funcionam de modo efetivo, que atuam em conformidade com as leis e regulamentos aplicáveis, que os seus ativos se encontram protegidos de roubos ou fraudes e que a informação financeira é preparada e reportada com precisão, de modo a proporcionar aos seus investidores uma tomada de decisão sustentada e consciente. É, portanto, um processo desenhado para cumprir os objetivos da organização e que começa no topo desta, com os quadros de direção e de gestão a criar e reforçar a estrutura e harmonia dos controlos, contudo, envolve todas as pessoas da organização, indo além dos controlos internos de relato financeiro.

O COSO compreende cinco componentes que se interligam, devendo funcionar como um único processo, no cumprimento dos objetivos. Estes estão relacionados com o modo como a Gestão conduz o negócio e fazem parte integrante do processo de gestão:

⁶ Tradução da autora. No original: *a process, effected by an entity's board of directors, management and other personal, designed to provide reasonable assurance regarding the achievement of the objectives in the following categories: (1) reliability of financial reporting,(2) compliance with applicable laws and regulations, and (3) effectiveness and efficiency of operations*

- **Ambiente de controlo** – está relacionado com o modo como os líderes da organização, que devem ser pessoas íntegras, conscientes e competentes, determinam os limites de uma conduta aceitável através da divulgação clara de políticas, códigos de ética e de conduta, recrutamento de pessoal suficiente, idóneo e capaz, desenvolvimento estruturas de compensação pela promoção de bons controlos internos, entre outras. A organização deve estabelecer e reforçar o compromisso com a existência de controlos internos robustos e a Gestão deve demonstrá-lo nas suas ações (Rittenberg [et all], 2010).
- **Avaliação de riscos** – como parte integrante da avaliação do sistema de controlo interno, a organização deve ter um processo implementado que lhe permita identificar e analisar os riscos potenciais que possam ter impacto na prossecução dos seus objetivos. A análise de riscos pode ser crítica para o sucesso da organização. A avaliação de riscos inclui uma estimativa da significância do risco, uma avaliação da probabilidade ou frequência de ocorrência do risco e por ultimo a forma como este pode ser gerido e as ações a tomar com vista à sua mitigação. O processo de avaliação de riscos é da responsabilidade da Gestão.
- **Atividades de controlo** – são as políticas, procedimentos estabelecidos para atingir os objetivos e mitigar o risco, bem como para assegurar que as ações identificadas para responder aos riscos foram levadas a cabo. Inclui controlos físicos, controlos informáticos de validação, indicadores de *performance*, os *Key Risk Indicators* (KRI's), revisão dos resultados pela Gestão, segregação de funções para rever ou aprovar operações chave, entre muitos outros (Moeller, 2005). Os controlos podem ser preventivos, quando são executados *a priori*, para prevenir o risco ou detetivos, quando fazem parte da monitorização. As atividades de controlo devem existir a todos os níveis da organização e em muitos casos podem sobrepor-se.
- **Informação e comunicação** – A informação, sendo um canal bidirecional (Oliveira, 2011), deve fluir a todos os níveis da organização, dos níveis de topo para os níveis mais baixos e *vice-versa*, de maneira e em tempo útil que permita as pessoas cumprir as suas responsabilidades. A informação deve ser substantiva, atual, compreensível, consistente, tempestiva, apropriada e suportada em sistemas automáticos. Os sistemas de informação devem ser ajustados à dimensão, natureza e complexidade da atividade da empresa e suportar a tomada de decisão. Moeller (2005) refere ainda que é importante manter os sistemas de informação adequados

às necessidades organizacionais e compreender os processos suportados quer em sistemas manuais, quer em sistemas de tecnológicos.

- **Monitorização** – fornece informação de retorno sobre se os outros componentes funcionaram efetivamente e permitem alcançar os resultados desejados, devendo ser efetuada numa base contínua, como parte integrante das tarefas diárias da empresa, com o intuito de identificar deficiências e corrigir eventuais desvios, com vista ao alcance dos objetivos da organização. O processo de monitorização deve estar devidamente documentado. Rittenberg [et all] (2010), acrescenta que a monitorização pode ser feita através de avaliações autónomas, realizadas pelos auditores, clientes e reguladores, por exemplo, ou através de avaliações *ongoing*, com base em indicadores decorrentes das atividades recorrentes.

Segundo Rittenberg [et all] (2010), os componentes de controlo interno relacionam-se entre eles. O processo de controlo é um processo contínuo, pois a Gestão identifica objetivos, avalia os riscos que impactam no cumprimento destes, compreende o ambiente de controlo e identifica atividades de controlo que reduzam o risco para um nível aceitável, desenvolve um processo de informação e comunicação que funcione a todos os níveis da organização e monitoriza a efetividade do sistema de controlo interno (ibid.:1).

Todavia, ao longo desta última década verificou-se um aumento das exigências por parte dos supervisores de *Governance*, bem como uma mudança nas expectativas da competência dos profissionais de contabilidade. Para além disso, havia uma certa pressão, por parte de vários organismos, na prevenção e detenção da fraude. Por outro lado, os requisitos legais, aliados à crescente globalização de mercados e operações e a conseqüente complexidade que os negócios assumem, bem como o aumento significativo do uso das novas tecnologias, conduzem, no seu conjunto, à revisão do *Internal Control – Integrated Framework*. Estas mudanças, naturalmente, deram origem à identificação de novos riscos suscetíveis de ter impacto no cumprimento dos objetivos principais das organizações e, em 2013, é publicada uma nova edição do *COSO Framework* que pretendia ajustar-se às novas exigências do mundo dos negócios.

O novo *Framework* do COSO mantém as três categorias de objetivos anteriormente citadas, no entanto, o relato financeiro é substituído por relato, passando a ter uma

perspetiva mais abrangente, dado que passa a incluir não só o relato financeiro externo mas também os reportes internos e externos não financeiros.

Quanto aos componentes iniciais, a categoria de “monitorização” passa a “monitorização de atividades”. Esta alteração pretende que a monitorização seja vista como uma serie de atividades desencadeadas como parte de cada um dos restantes componentes.

Os conceitos fundamentais de cada um dos cinco componentes são articulados em 17 princípios de um controlo interno considerado eficaz e adequado. Uma entidade pode conseguir um controlo interno efetivo da aplicação destes princípios, pois estes representam os conceitos fundamentais de cada componente.

Os princípios enunciados pelo COSO apresentam-se, ao longo dos componentes, da seguinte forma (COSO, 2013):

Ambiente de controlo

- 1 - A organização demonstra ter um compromisso com os valores éticos e de integridade;
- 2 – Os quadros de direção são independentes dos de gestão e dos supervisores responsáveis pelo desenvolvimento e *performance* do controlo interno;
- 3 – A Gestão estabelece, juntamente com os quadros de supervisão, estruturas, linhas de reporte e níveis de delegação de competências e responsabilidades alinhadas com os objetivos da entidade;
- 4 – A Gestão compromete-se a atrair, desenvolver e reter o pessoal com as competências necessárias para o cumprimento dos objetivos;
- 5 – A organização tem pessoas responsáveis pelo controlo interno com vista ao alcance dos objetivos;

Avaliação de riscos

- 6 - A organização estabelece objetivos suficientemente claros para uma identificação e avaliação de riscos relacionados com os objetivos;
- 7 – A organização identifica riscos para alcançar os objetivos ao longo da entidade e analisa riscos como base para determinar a gestão dos mesmos;
- 8 – A organização considera a possibilidade de existência de fraude na avaliação dos riscos com impacto no alcance dos objetivos;
- 9 – A organização identifica e avalia alterações que possam ter impacto significativo no sistema de controlo interno;

Atividades de controlo

10 – A organização seleciona e desenvolve atividades de controlo que contribuem para a mitigação de riscos relacionados com os objetivos para níveis aceitáveis;

11 – A organização seleciona e desenvolve atividades de controlos gerais de tecnologias que suportem o alcance dos objetivos;

12 – A organização seleciona e desenvolve atividades e controlos através de políticas que estabelecem as suas expectativas e definem procedimentos que coloquem essas políticas em prática;

Informação e comunicação

13 – A organização obtém ou gere e usa informação de qualidade relevante para suportar o funcionamento do controlo interno;

14 – A organização comunica internamente informação, que inclui objetivos e responsabilidades de controlo interno, necessárias para suportar o funcionamento do controlo interno;

15 – A organização comunica com terceiras partes sobre a matéria que afeta o funcionamento do controlo interno;

Monitorização de atividades

16 – A organização seleciona, desenvolve e executa avaliações *on-going* e autónomas para certificar-se de que todos os componentes do controlo interno existem dentro da entidade e se estes se encontram a funcionar;

17 – A organização avalia e comunica as deficiências do controlo interno de forma atempada às partes responsáveis por tomar as medidas corretivas, incluindo aos gestores executivos e quadros de direção.

Por último, no que concerne à estrutura da organização, o novo *Framework* alinha-se como o Framework do COSO ERM de 2004, o qual considera toda a organização a todos os níveis funcionais.

A relação entre os objetivos, que é o que as entidades ambicionam alcançar, os componentes, que representam o que é necessário para os atingir, e a estrutura organizacional da entidade (unidades operativas, subsidiárias, outras unidades de negócio, entidades reguladoras, entre outras) pode ser representada num cubo, conforme se pode ver na Figura 2.1:

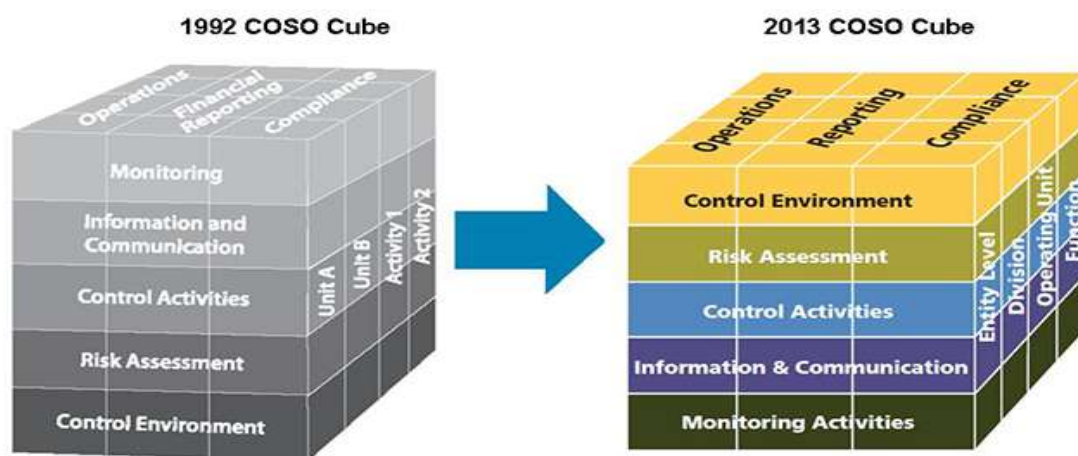


Figure 2.1 COSO Cube

Fonte: <https://www.google.pt/#q=COSO+cube+1992+versus+COSO+2013>

O novo documento do COSO considera as mudanças nos negócios e no ambiente operacional, amplia os objetivos relacionados com as operações e com o relato financeiro e inclui os controlos internos sobre tecnologias. Dá ainda uma abordagem adicional e exemplos de operações relevantes, de *compliance* e de reporte de informação não-financeira.

A abordagem por princípios permite uma maior flexibilidade no uso do *Framework* para múltiplos objetivos e para objetivos sobrepostos ao longo da organização. Deste modo, é mais fácil ver se todos estão cobertos e reduz a probabilidade de considerar algo irrelevante. O uso de princípios permite à Gestão compreender melhor a importância de especificar objetivos compatíveis, bem como dar ênfase aos riscos e aos controlos mais importantes para os atingir. Também permite-lhe focar-se nas áreas de risco que excedem o nível de aceitação ou que necessitam de ser geridos ao longo da organização, podendo reduzir esforços gastos na mitigação de riscos com menor significado. Selecionar, desenvolver ou descartar controlos para efetivar princípios pode também reduzir o número de controlos menos pertinentes. Ao avaliar a robustez e a gravidade das deficiências dos controlos internos, usa apenas o critério da relevância, conforme determinado no próprio *Framework* ou pelos reguladores ou outras fontes apropriadas.

Apesar de o controlo interno proporcionar uma segurança aceitável do cumprimento dos objetivos da entidade, existem limitações resultantes da adequação dos objetivos à entidade, como a existência de pré-conceitos no modo como o negócio é conduzido e os objetivos definidos, a realidade de que os julgamentos humanos na tomada de decisões

podem ser errados ou tendenciosos, existência de quebras ou falhas humanas, como simples erros, habilidade dos gestores em dominar os controlos internos, bem como a dos gestores, outro pessoal e terceiros em ultrapassar controlos através de conluios, além da possibilidade de ocorrência de eventos externos que a organização não controla.

2.4.2 – O *Enterprise Risk Management*

O modelo COSO apontava, contudo, para áreas em que havia conceitos ainda por explicar, nomeadamente, o de gestão de risco que, àquela altura, ainda era muito ambíguo. O COSO, em conjunto com uma empresa de auditoria, a Pricewaterhouse Coopers (Pwc), na tentativa de desenvolver um único conceito, acabou por desenvolver os principais tópicos em que se fundamenta o COSO ERM *Framework* (Moeller, 2011), doravante apenas COSO ERM ou simplesmente ERM.

A grande mudança que preconiza este novo modelo, face ao anterior surge da introdução do conceito de gestão de riscos em favor do cumprimento dos objetivos estratégicos da empresa. Ora, as empresas existem com a finalidade de criar valor aos seus *stakeholders*, quer estes sejam empregados, fornecedores, acionistas ou o Estado. Este valor deve ser criado, preservado ou pode mesmo ser deteriorado pelas decisões dos gestores, a todos os níveis da organização e em todas as atividades, desde as operações regulares do dia-a-dia, as quais passam por estabelecer estratégias para o futuro mas que estão sujeitas a riscos incertos (ibid.: 1).

O ERM *Framework* (2002: 2)⁷, começa por definir o conceito de gestão de riscos da empresa (*enterprise risk management*) como

[u]m processo efetuado pelos quadros de direção, gestão e outro pessoal da empresa, aplicado numa estratégia e transversal a toda a empresa, desenhado para identificar potenciais eventos que possam afetar a empresa e gerir os riscos de acordo com o seu apetite de risco, para proporcionar uma segurança razoável com vista ao cumprimento dos seus objetivos.⁸

Nesta linha, a gestão de riscos pressupõe a identificação de riscos, do seu impacto, a priorização dos riscos e planeamento de ações a tomar, bem como, o respetivo acompanhamento destas e dos seus resultados nos riscos.

⁷ O *Enterprise Risk Management – Integrated Framework – Executive Summary*

⁸ Tradução da autora. No original: *a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

Moeller (2011) sintetiza os pontos principais do COSO ERM, com base nos seguintes pressupostos:

- O processo de gestão de riscos corporativo não é estático. Os riscos potenciais devem ser revistos e avaliados, com base em documentação, e as ações devem ser tomadas tendo em conta uma leque de fatores ao longo de toda a empresa;
- O ERM é implementado pelo pessoal de toda a organização, os quais devem conhecer o risco para compreender os fatores que o envolvem e as suas implicações, de modo a poderem atuar sobre o mesmo;
- O ERM deve ter uma função de apoiar na escolha das estratégias da empresa;
- Deve considerar o apetite de risco, isto é, o nível de risco que a empresa e os seus gestores estão dispostos a aceitar para alcançar os seus objetivos. O apetite de risco pressupõe uma categorização dos riscos em baixo, médio e elevado;
- O ERM proporciona uma segurança razoável mas não efetiva na concretização dos objetivos. Por muito bem controlada que a empresa esteja, há sempre falhas imprevisíveis, como erros humanos, fraudes, ou até mesmo fatores naturais adversos;
- O ERM deve ajudar a atingir os objetivos comuns da empresa, como por exemplo, ter uma boa reputação junto de outras empresas e dos consumidores, divulgar relatórios financeiros credíveis e operar de acordo com leis e estratégias, através do uso das melhores práticas de controlo interno.

Assim, aos componentes apresentados pelo COSO, o COSO ERM vem acrescentar mais três componentes:

- **Definição de objetivos** – os objetivos estratégicos devem estar alinhados com a missão da empresa e cobrir as atividades operacionais, de reporte de informação e de cumprimento de normas e requisitos regulatórios – *compliance* (Moeller, 2011). As empresas enfrentam riscos resultantes de fatores internos e externos, sendo a fixação de objetivos um pré-requisito à identificação eficaz de eventos, à avaliação de riscos e à resposta aos mesmos. Os objetivos estratégicos devem estar alinhados com o apetite a risco e o nível de tolerância aos riscos determinados.
- **Identificação de eventos** – a Gestão identifica potenciais eventos, cuja ocorrência afete a organização, quer sejam através de identificação de oportunidades ou de

efeitos adversos que impactem na implementação adequada da estratégia e o alcance dos objetivos.

- **Resposta aos riscos** – após avaliar os riscos pertinentes é importante definir como se dará resposta a esses riscos. Essas respostas podem ser (i) evitar, (ii) reduzir, (iii) compartilhar ou (iv) aceitar os riscos. A resposta deve ser dada considerando a probabilidade de ocorrência, o efeito e impacto do risco, assim como os custos e benefícios, selecionando, dessa forma, uma resposta que mantenha os riscos residuais dentro das tolerâncias a risco desejadas.

À semelhança do que foi feito para o COSO, podemos representar o cubo do ERM do seguinte modo, atendendo ao que acabamos de referir:



Figure 2.2 COSO ERM Cube

Fonte: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Posto isto, Oliveira (2011) estabelece que, o ERM tem por objetivo permitir que o apetite de risco esteja alinhado com a estratégia da organização, apoiar a tomada de decisão face aos riscos de forma sustentada e, desta forma, reduzir o risco operacional e prevenir a ocorrência de eventos inesperados, aproveitando as oportunidades e otimizando os processos e os recursos existentes.

No entanto, os objetivos do ERM, por si só, de pouco valem, a menos que a forma como se organizam e estão estruturados permitam que a Gestão possa facilmente compreender como estes interagem e se relacionam entre si de modo multidimensional.

2.5 – O Control Objectives for Information and Related Technology

Nos tempos atuais, em que se verifica uma grande dependência da tecnologia, a informação é um recurso-chave para qualquer organização, já que, para serem competitivas, as empresas tornam os seus negócios cada vez mais complexos. As entidades devem demonstrar que possuem controlos eficientes e robustos. O *Control Objectives for Information and Related Technology* (CobiT), surge assim como um normativo de referência quer para as entidades, quer para os auditores ou seus utilizadores (Morais e Martins, 2013).

A estrutura do CobiT, apesar das suas semelhanças com o COSO, põe a sua ênfase essencialmente nos controlos em ambientes mais tecnológicos. O CobiT é um modelo criado, em 1996, pelo *Information Systems Audit and Control Association* (ISACA), um organismo sob a alçada do *Information Technology Governance Institute* (ITGI) uma entidade que atua desde 1969 que conta com 95 000 constituintes em 160 países, responsável por desenvolver normas de auditoria e controlo em sistemas de informação a nível internacional.

A primeira versão do CobiT era direcionada exclusivamente para a auditoria em TI. Em 1998 e 2000, surgem novas versões que tinham como focos o controlo em TI e gestão em TI, respetivamente. Só em 2005 é que este modelo introduz o *Governance* em TI e, a sua última versão, em 2012, está atualmente alinhada com a *Governance* organizacional em TI. Apesar de ser uma ferramenta de controlo interno, é muitas vezes utilizada para documentar, rever e compreender os controlos internos da SOX. A revisão das normas do CobiT é efetuada pela ISACA em consonância com *IT Governance Institute* (ITGI), apesar de que a ISACA estar mais envolvida com as orientações de auditoria de IT e o ITGI se foca nas normas de *Governance*.

Para melhor compreendermos a evolução desta ferramenta, convém referir que o *Governance* em IT inclui o desenvolvimento de processos para a tomada de decisão relacionada com o desenvolvimento da estratégia de TI, definição das prioridades face aos orçamentos, gestão dos projetos de TI, desenho e desenvolvimento de infraestruturas e a definição de políticas e procedimentos que governem a utilização organizacional das TI.

O CobiT5 – *The Governance and Management of Enterprise IT* -, é aplicável a organizações privadas ou públicas e é hoje reconhecido como a ferramenta de boas práticas que melhor se adequa ao cumprimento dos objetivos de governação e gestão das TI (ibid.: 1), na medida em que ajuda a organização a criar valor a partir do uso de Tecnologias de

Informação, uma vez que estas trazem vantagens competitivas e uma otimização da gestão dos riscos do negócio.

O atual modelo do CobIT foi desenvolvido, com base em 5 princípios básicos a considerar, para que as empresas atinjam um bom *Governance* em TI:

- Conhecer as necessidades dos *stakeholders*. As empresas têm como principal objetivo criar valor para os seus *stakeholders*, no entanto, as expectativas destes podem ser incompatíveis. Para tal, é necessário fazer uma “negociação” entre os diferentes interesses destes. A tomada de decisão deve ter em conta a resposta às questões: “quem recebe os benefícios?”, “quem corre o risco?” e “que recursos são necessários”.
- Cobertura dos processos *end-to-end*. Inclui o *Governance* e a gestão das tecnologias de informação de forma transversal e abrangente a toda a organização, cobrindo todas as funções e processos dentro da organização, não se focando apenas na função de IT, pelo contrário, trata os ativos relacionados com a informação como qualquer outro ativo na organização.
- Procura uma estrutura única integrada, na medida em que está alinhada com os requisitos de outros modelos de risco, como o COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000 e os relacionados com normativos de referência em TI, como a ISO/IEC 38500, ITIL, ISO/IEC 27000 series, entre outras;
- Considera uma abordagem holística dos elementos e a forma como estes se relacionam entre si, tendo em conta sete elementos que, isoladamente ou em conjunto, influenciam o cumprimento dos objetivos da organização: (i) descrição dos processos; (ii) estrutura organizacional; (iii) cultura, ética e comportamento; (iv) princípios, políticas e *frameworks*; (v) informação; (vi) serviços, infraestruturas e aplicações, incluindo os de informação e de tecnologias e (vii) recursos humanos existentes e as respetivas competências;
- Separa *Governance* e gestão, sendo que a primeira tem a ver com a responsabilidade dos executivos de um modo geral e está relacionado com a estratégia, e a outra, com a responsabilidade tácita do CEO.

O CobiT5, para hierarquizar o risco, compreende agora quatro dimensões comuns a cada um dos elementos anteriormente referidos, face às anteriores versões que compreendiam apenas três⁹, a saber:

- *Stakeholders* – cada elemento tem “partes” que executam as atividades ou têm interesse nas mesmas.
- Objetivos - cada elemento acresce valor quando os seus objetivos são alcançados. Os objetivos devem ser analisados em termos da qualidade em que os elementos operam, em termos de precisão, objetividade e resultados, assim como, em termos de acessibilidade e segurança. Cada elemento e os seus resultados devem ser relevantes, consistentes, apropriados e facilmente compreendidos e ir de encontro ao contexto em que operam.
- Ciclo de vida – considera um ciclo de vida para cada elemento, desde a sua criação, passando pela sua utilidade operativa até à sua eliminação. As fases do ciclo de vida consistem em planear, desenhar, construir ou implementar, utilizar, avaliar, monitorizar, atualizar ou eliminar.
- Boas práticas – podem ser definidas boas práticas que suportem o alcance dos objetivos definidos para cada elemento.

O CobiT5 dá exemplos de boas práticas para alguns dos elementos abordados, por exemplo, processos. As empresas, por sua vez, esperam bons resultados da aplicação destes e a sua monitorização implica que, regularmente e com base em métricas, sejam respondidas questões relativas aos mesmos, tais como: “as necessidades dos *stakeholders* encontram-se satisfeitas?”, “os objetivos de cada elemento foram cumpridos?”, “o ciclo de vida foi bem gerido?” e “as boas práticas foram implementadas?”

O CobiT 5 contempla 37 processos para os domínios de *Governance* e para a gestão de TI. É de realçar que, o modelo CobiT pode servir de orientação ao trabalho do auditor e que os mapas de controlo fornecidos auxiliam os auditores e os executivos da empresa quanto à avaliação dos controlos e se estes são suficientes para mitigar os riscos, permitindo assim uma hierarquização dos riscos.

⁹ As 3 dimensões anteriormente consideradas eram: recursos de TI, processos de TI e requisitos do negócio

3. O controlo interno nas instituições financeiras

3.1 - Enquadramento teórico

Conforme referido anteriormente, a existência de um bom controlo interno é preponderante para as organizações, indo de encontro às necessidades da gestão de controlar os processos e melhorar a eficácia e eficiência dos seus recursos, e às exigências de terceiros, na medida em que estes, precisam de confiar nas empresas, para poderem tomar as suas decisões de investimento. Assim, este é um conceito que está no centro das atenções de todos os intervenientes do mercado económico-financeiro.

Com a internacionalização da Banca e o crescimento dos mercados financeiros e derivados, surge a necessidade da existência de uma regulamentação mais estreita dos mercados bancários.

Em 1988, o *Basel Committee on Banking Supervision* introduz o Acordo Basileia¹⁰, adotado em mais de cem países, com o objetivo de criar exigências mínimas de capital a serem respeitadas pelos Bancos, bem como a adoção de medidas de prevenção contra o risco de crédito. Este documento punha o risco de crédito no seu foco, pois segundo Crouhy, Galai e Mark (2006), assumia que este era o fator de risco predominante nas instituições bancárias. Em Setembro de 1998, esse mesmo *Committee*, estruturou um sistema de controlo interno, publicado num documento, o *Framework for Internal Control Systems in Banking Organisations*, que veio a servir de base para um outro documento onde eram estabelecidos princípios de boas práticas com vista a mitigar o risco operacional, o *Sound Practices for the Management and Supervision of Operational Risk*¹¹. Em Junho de 2004, é publicado um novo acórdão em substituição do anterior, o Basileia II, o qual deveria ser implementado pelos Bancos em paralelo com os requisitos regulatórios específicos exigidos para cada país. Este documento havia sido pensado pelos reguladores de modo a que fosse suscetível de ser aplicado em qualquer instituição, independentemente do seu nível de complexidade e sofisticação. Contudo, novas regras conduziam à identificação de novos riscos e, conseqüentemente, exigiam a introdução de novos sistemas e abordagens, o que, necessariamente, leva o seu tempo. Assim, a implementação do Basileia II começou anos antes da sua entrada em vigor, em 2007. Este

¹⁰ Oficialmente designando por *International Convergence of Capital Measurement and Capital Standards*

¹¹ Emitido em Fevereiro de 2003

acórdão assentava em três pilares e 25 princípios básicos sobre contabilidade e supervisão bancária e tinha como objetivo principal assegurar uma capitalização adequada dos Bancos e encorajar estes a adotar as melhores práticas (*best practices*) de gestão de risco (ibid.:1). Estabelecia que as instituições deveriam desenvolver um sistema de gestão de riscos com vista a identificar, medir e monitorizar os seus riscos e que cobrisse todos elementos chave da estrutura de capital, conciliando o montante do capital interno com o seu perfil de risco, a sua estratégia e plano de negócios, de modo a garantir a existência de fundos próprios suficientes para fazer face à possibilidade de ocorrência dos riscos a que estão expostos no decurso da sua atividade. O Basileia II não deixava dúvidas quanto à importância da gestão de riscos, tendo servido de suporte também para a regulação de instituições não-financeiras.

Contudo, a crise recente na Banca, veio colocar em causa a estrutura regulatória vigente sobre os sistemas financeiros. Em Dezembro de 2009, o *Basel Committee on Banking Supervision*, reunia novamente e emitia duas propostas¹² com o objetivo de tornar a regulação global sobre capital e liquidez mais rigorosa e assim tornar o setor bancário internacional mais sólido, dando lugar, no segundo semestre de 2010 à formalização do Basileia III. Este novo acórdão procurava assegurar uma mais adequada detenção de fundos próprios, considerando restrições na alavancagem da atividade, e uma capacidade de resposta a situações de *stress* de liquidez, introduzindo rácios exigentes quer de curto prazo, quer de médio e longo prazo. O impacto que estas alterações tinham nas contas de exploração e nos modelos de negócio das instituições bancárias, bem como nos processos e sistemas de informação, levaram a uma regulação e supervisão ainda mais apertadas.

Com estes novos requisitos mínimos de capital e de rácios de cobertura de liquidez, o controlo do risco passou a estar no topo da pirâmide de prioridades das instituições financeiras, sendo fundamental que todos os colaboradores do Banco tenham presentes os riscos resultantes das suas decisões e do que estas representam em termos de capital e liquidez. Assim, é importante que os colaboradores estejam conscientes das suas restrições, quer sejam resultantes do próprio balanço do Banco, de financiamentos, quer dos requisitos regulatórios aplicáveis.

¹²*Strengthening the resilience of the banking sector e International framework for liquidity risk measurement, standards and monitoring*

Em Junho 2011, o *Basel Committee* lança ainda um documento *Principles for the Sound Management of Operational Risk and the Role of Supervision* em substituição do *Sound Practices* de 2003, o qual «incorpora a evolução das boas práticas e onze princípios de gestão do risco operacional que cobram o (1) *Governance*, (2) ambiente de gestão de risco e (3) responsabilidade de divulgação»¹³(2011: 1).

Paralelamente, o CEBS reconhece a necessidade de aumentar a cooperação na supervisão, de modo a evitar a falta de coordenação entre os diferentes supervisores e, conseqüentemente, duplicar o trabalho destes. Em Junho de 2006, publica um documento, o *Guidelines on the Application of the Supervisory Review Process under Pillar II*, que visava promover a convergência da supervisão e, complementarmente, uma abordagem consistente, tendo em conta as tendências dos mercados e as práticas de cada país. Este documento vem ainda divulgar algumas orientações em matéria de *Internal Governance* e estabelecer linhas orientadoras que servissem de suporte para obter uma maior consistência na avaliação de *Governance* das instituições, por parte dos supervisores.

Em Setembro de 2011, a *European Banking Authority* (EBA)¹⁴, emitiu um documento com 44 *guidelines*¹⁵ em substituição do anteriormente emitido pelo CEBS. O mesmo organismo, publica ainda, em Novembro de 2012, um outro documento destinado a avaliar questões como a idoneidade e competências profissionais dos membros dos órgãos de administração e de gestão, o *Guidelines on the assessment of the suitability of members of the management body and key function holders*.

Desde 2006 que, as instituições financeiras, em Portugal, ao abrigo do Aviso n.º 3 do Banco de Portugal, estão obrigadas a ter um sistema de controlo interno ajustado quer à sua dimensão, quer aos riscos que estão subjacentes ao exercício da sua atividade. Este normativo veio a ser revogado pelo Aviso n.º 5/ 2008, que, por sua vez, sistematiza uma série de princípios a seguir na implementação do sistema de controlo interno, suportado nos princípios básicos da metodologia do COSO e nos controlos recomendados pelo *Basel Committee* através do já referido *Framework*, bem como nas orientações em matéria de *Internal Governance* divulgadas pelo CEBS, pelo que passaremos a fazer o estudo destes últimos.

¹³ Tradução da autora. No original: (...) incorporates the evolution of sound practices and details eleven principles of sound operational risk management covering (1) governance, (2) risk management environment and (3) the role of disclosure

¹⁴ Autoridade Bancária Europeia, que substitui o anterior CEBS

¹⁵ EBA Guidelines on the Internal Governance (GL 44)

3.2 – Os pilares do controlo interno nas instituições financeiras

3.2.1 - O *Framework for Internal Control Systems in Banking Organizations*

Em 1998, decorrente de pressões internacionais e, conseqüentemente, da necessidade de obter controlos internos mais eficientes e mais eficazes o *Basel Committee on Banking Supervision*, emitiu originalmente, um documento que se designava por *Framework for Evaluation of Internal Control Systems*, o qual viria a ser ajustado ainda em Setembro desse ano, dando origem a um outro, o já referido *Framework for Internal Control Systems in Banking Organisations*. Este documento pretendia estabelecer orientações para a implementação de controlos adequados aplicáveis à generalidade das instituições financeiras, tendo em conta a natureza do negócio e a sua dimensão.

Este *Committee* estudou os problemas da Banca com o intuito de identificar as causas de maiores deficiências nos controlos internos. Os problemas detetados reforçaram a importância de terem uma estrutura de *Governance* apropriada, auditores internos e externos, bem como supervisores bancários focados na robustez do sistema de controlo interno e na avaliação contínua dos mesmos. Casos recentes demonstravam que controlos internos inadequados poderiam levar a perdas significativas para os Bancos.

A partir destas conclusões, este *Framework* define controlo interno e sintetiza alguns princípios básicos de controlo interno. Para o *Basel Committee*,

[u]m sistema eficaz de controlo interno constitui um componente crítica da gestão do Banco e uma base para a atividade sólida e segura das organizações bancárias. Um sistema robusto de controlos internos pode ajudar a assegurar que as metas e objetivos da organização bancária serão atingidos e que o Banco irá alcançar objetivos de rentabilidade de longo prazo e manter um processo de reporte financeiro e de gestão fiável. Um tal sistema assegura também que o Banco cumpre as leis e regulamentos aplicáveis, bem como políticas, planos e regras internas, e reduz o risco de perdas inesperadas ou danos na sua reputação.¹⁶(1998: 1)

¹⁶ Tradução da autora. No original: *A system of effective internal controls is a critical component of bank management and a foundation for the safe and sound operation of banking organisations. A system of strong internal controls can help to ensure that the goals and objectives of a banking organisation will be met, that the bank will achieve long-term profitability targets, and maintain reliable financial and managerial reporting. Such a system can also help to ensure that the bank will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damage to the bank's reputation.*

Este documento refere que o sistema de controlo interno a implementar deve assentar na delegação de competências e responsabilidades, segregação de funções, nomeadamente em funções relacionadas com assunção de responsabilidades perante terceiros, utilização de recursos financeiros e manuseamento de ativos e passivos, reconciliação dos processos principais, proteção de ativos e existência de auditores internos para verificar se os controlos se encontram *in place* e se as leis e regulamentos aplicáveis estão a ser cumpridos.

Neste documento são enunciados 13 princípios, os quais se encontram vinculados aos elementos de controlo interno também por ele citados. O *Committee* pretendia que estes princípios fossem de aceitação generalizada e que as próprias entidades supervisionadas utilizassem para avaliar se têm capacidade para monitorizar os sistemas de controlo interno dos Bancos:

Elemento 1: Supervisão pela Administração e cultura de controlo:

Princípio 1: O Conselho de Administração tem a responsabilidade de aprovar e de, periodicamente, rever as estratégias globais de negócios e políticas significativas do Banco; compreender os principais riscos, fixando níveis aceitáveis para estes riscos e garantir que a alta Administração toma as medidas necessárias para identificar, medir, monitorizar e controlar esses riscos; aprovar a estrutura organizacional e garantir de que a Administração está a monitorizar a eficácia do sistema de controlo interno. O Conselho de Administração é responsável por garantir que um sistema adequado e eficaz de controlos internos é estabelecido e mantido.

Princípio 2: A alta Administração deve ser responsável por implementar estratégias e políticas aprovadas pelo conselho; desenvolver processos que identifiquem, meçam, monitorizem e controlem os riscos incorridos pelo Banco; manter uma estrutura da organização onde estejam claramente definidas responsabilidades, autoridade e relações; assegurar que as responsabilidades delegadas são cumpridas; que existem políticas de controlo interno apropriadas e monitorizar a adequabilidade e eficácia do sistema de controlo interno.

Princípio 3: O Conselho de Administração e a direção são responsáveis por promover de padrões éticos e de integridade, e pela existência de uma cultura dentro da organização que enfatize e demonstre, ao longo de toda a hierarquia, a importância dos controlos internos.

Todos os colaboradores de uma organização bancária devem compreender o seu papel no processo de controlos internos e estar totalmente envolvidos no processo.

Elemento 2: Reconhecimento e avaliação de riscos

Princípio 4: Um sistema de controlo interno eficaz requer que os riscos materiais suscetíveis de afetar adversamente a realização dos objetivos do Banco sejam reconhecidos e continuamente avaliados. Esta avaliação deve cobrir todos os riscos enfrentados pelo Banco e/ ou pelo grupo bancário, (isto é, o risco de crédito, o país e a transferência de risco, risco de mercado, risco de taxa de juro, risco de liquidez, risco operacional, risco legal e risco de reputação). Os controlos internos podem necessitar de revisão de modo a incorporar riscos novos ou previamente não controlados.

Elemento 3: Atividades de Controlo e Segregação de Funções

Princípio 5: As atividades de controlo devem ser parte integrante das atividades diárias de um Banco. Um sistema de controlo interno eficaz requer que uma estrutura de controlos apropriados seja estabelecida, com atividades de controlo definidos a todos os níveis do negócio. Estes devem incluir: revisões a nível superior; controlos de atividades apropriados para diferentes departamentos; controlos físicos; verificação de conformidades relativas aos limites de exposição e acompanhamento das não-conformidades; um sistema de aprovações e autorizações; e um sistema de verificação e reconciliação.

Princípio 6: Um sistema de controlo interno eficaz exige que haja segregação adequada dos deveres e que não sejam atribuídas responsabilidades em conflito. Áreas de potenciais conflitos de interesse devem ser identificadas, minimizadas, e sujeitas a uma monitorização cuidada e independente.

Elemento 4: Informação e comunicação

Princípio 7: Um sistema de controlo interno eficaz requer um tratamento adequado de dados financeiros, operacionais e de conformidades internas, bem como informações externas de mercado sobre os eventos e condições que são relevantes para a tomada de decisão. A informação deve ser confiável, oportuna, acessível e fornecida num formato consistente.

Princípio 8: Um sistema de controlo interno eficaz requer que existam informações confiáveis e sistemas que cubram todas as atividades significativas do Banco. Estes sistemas, incluindo aqueles que registam e usam os dados em formato eletrónico, devem ser seguros, monitorizados de forma independente e devem ser mantidos planos de contingência adequados.

Princípio 9: Um sistema eficaz de controlo interno requer canais de comunicação eficazes para garantir que todos os funcionários compreendem e aderem às políticas e procedimentos relativos aos seus deveres e responsabilidades e que outras informações relevantes vão alcançar os colaboradores apropriados.

Elemento 5: Monitorização das atividades e correção de deficiências

Princípio 10: A eficácia global dos controlos internos do Banco deve ser continuamente monitorizada. A monitorização dos principais riscos deve ser parte das atividades diárias de qualquer instituição bancária, bem como avaliações periódicas pelas linhas de negócios, através da análise KRI's e de auditorias internas.

Princípio 11: Deve haver um departamento de auditoria interna que se pronuncie regularmente sobre a eficácia e abrangência do sistema de controlo interno. Os auditores internos devem ser independentes, devidamente formados e competentes. A função de auditoria interna, como parte da monitorização do sistema de controlo interno, deve reportar diretamente ao Conselho de Administração ou ao Comité de Auditoria.

Princípio 12: Deficiências de controlo interno que sejam identificadas pelas linhas de negócio, auditoria interna ou outro pessoal de controlo, devem ser prontamente comunicadas ao nível de gestão adequado e rapidamente solucionadas. Deficiências de controlo interno materiais devem ser relatadas à alta Administração e ao Conselho de Administração.

Elemento 6: Avaliação dos Sistemas de Controlo Interno pelas autoridades de supervisão

Princípio 13: Os supervisores devem exigir que todos os Bancos, independentemente do tamanho, possuam um efetivo sistema de controlo interno e que este seja consistente com a natureza, complexidade e risco financeiro e não-financeiro inerente às suas atividades, dentro ou fora do balanço, e que responda às mudanças no ambiente e nas condições do

Banco. Nos casos em que os supervisores determinem que o sistema de controlo interno não é adequado ou eficaz para o perfil de risco específico de um Banco (por exemplo, não cobre todos os princípios contidos neste documento), estes devem tomar as medidas adequadas.

Tendo em conta o conceito de controlo interno, os objetivos, elementos e princípios contidos neste documento, os Bancos, supervisores financeiros e auditores externos tinham uma base para avaliar a eficiência e eficácia dos sistemas de controlo interno e, a partir daí, melhorá-los.

3.2.2 – As orientações de *Internal Governance* divulgadas pelo *Committee of European Banking Supervisors*

Conforme já foi referido, o *Guidelines on the Application of the Supervisory of the Supervisory Review Process under Pillar II* vem determinar uma série de orientações de *Internal Governance*, as quais iremos estudar agora.

Antes de mais, à luz deste documento, convém distinguir os conceitos de *Internal Governance* e *Corporate Governance*, sendo que, o primeiro está relacionado com a estrutura organizacional e tem o seu foco nas responsabilidades dos órgãos de gestão, nomeadamente, na definição dos objetivos, do apetite de risco, como é que o negócio está organizado, delegação de responsabilidade e autoridade, das linhas de reporte e na informação que estas devem reportar, bem como a implementação do controlo interno; enquanto o segundo, o *Corporate Governance*, é um termo mais abrangente, onde estão incluídos também os acionistas e os outros *stakeholders*.

Para efeitos de controlo interno, os órgãos de gestão são responsáveis por garantir que a instituição é constituída por três áreas funcionais independentes e que permitem a existência de um sistema de controlo interno eficiente. Estas funções são as de gestão de riscos, *compliance* e auditoria interna.

Assim, da leitura do capítulo 2 do referido documento, verifica-se a existência de 21 orientações (IG's) às instituições, de modo a que estas compreendam o que é que os supervisores esperam delas quanto ao cumprimento dos requisitos de *Internal Governance*:

A – Estrutura corporativa e organização:

IG 1: As instituições devem ter uma estrutura corporativa transparente e organizada, quer para todos os funcionários, quer para os supervisores, de modo a promover e demonstrar uma gestão efetiva e prudente da instituição. Ressalva-se que, no caso em que a instituição pertença a um Grupo de empresas, o supervisor deve avaliar também o posicionamento desta face ao Grupo.

IG2: As linhas de reporte e a delegação de responsabilidades e autoridade devem ser claras, precisas, bem definidas, transparentes, coerentes e reforçadas dentro da organização, de modo a que os funcionários compreendam e adiram às políticas e procedimentos de acordo com os seus limites de responsabilidade e autoridade.

IG3: As instituições devem assegurar que a função de gestão de riscos está organizada de uma forma que facilite a implementação de políticas de risco e a gestão dos riscos da instituição.

As instituições com estruturas de maior dimensão, complexidade ou grau de sofisticação podem desenvolver funções de gestão de riscos que cubram cada uma das linhas de negócio relevantes.

A gestão de riscos inclui a identificação, a medição e avaliação de todos os riscos materiais que podem afetar adversamente o cumprimento dos objetivos da instituição. Os procedimentos de monitorização e de avaliação necessitam de ser atualizados permanentemente. Os órgãos de gestão¹⁷ devem estabelecer a estratégia de risco, a política de risco e a capacidade de risco da instituição.

B – Os órgãos de gestão:

IG4: As responsabilidades dos órgãos de gestão devem estar claramente definidas num documento escrito, incluindo as responsabilidades de definição de objetivos de negócio, estratégias de risco e perfil de risco e quais as políticas a adotar para atingir esses objetivos.

¹⁷ Os órgãos de gestão aqui referidos têm em consideração as funções de supervisão e gestão que lhes competem.

IG5: Os órgãos de gestão devem assegurar que as estratégias e políticas são comunicadas a todos os níveis relevantes da organização, através de orientações escritas, manuais ou outros meios.

IG6: Os órgãos de gestão devem sistemática e regularmente rever as suas estratégias e políticas para gerir os riscos da instituição.

IG7: Os órgãos de gestão devem desenvolver e manter sistemas de controlo interno robustos que assegurem a efetividade e eficiência das operações, um adequado controlo dos riscos, uma conduta prudente do negócio, a fiabilidade da informação financeira e não-financeira, da informação reportada, quer interna, quer externa, e do cumprimento das leis e regulamentos, bem como das políticas e procedimentos internos.

IG8: Os órgãos de gestão devem assegurar que o sistema de controlo interno exige uma adequada segregação de funções, de modo a prevenir conflitos de interesse.

IG9: Os órgãos de gestão devem estabelecer estratégias e políticas para manter, de forma permanente, uma distribuição do capital interno e dos fundos próprios adequada para cobrir os riscos da instituição, quer quanto ao tipo (capitais primários ou suplementares) quer quanto aos montantes. Convém notar que a distribuição de fundos próprios dentro de um Grupo deve obedecer a requisitos legais.

IG10: Os órgãos de gestão devem monitorizar e avaliar periodicamente a estrutura interna da instituição, nomeadamente através da revisão de políticas, tendo em conta a mudança de fatores internos ou externos que possam afetar a instituição.

IG11: Os órgãos de gestão devem atuar ativamente e de forma independente e ser capazes de explicar as suas decisões às entidades de supervisão, bem como a outras partes interessadas.

IG12: Os órgãos de gestão devem ter políticas para seleção, remuneração, monitorização e planos de sucessão para os seus principais executivos.

IG13: Os órgãos de gestão devem promover níveis elevados de ética e normas profissionais e uma cultura de controlo interno.

C – Controlo Interno:

IG14: As instituições devem estabelecer, tendo em conta o princípio da proporcionalidade, as três funções principais de controlo, de modo a implementar um efetivo e compreensivo sistema de controlo interno em todas as áreas da instituição: função de controlo de riscos, função de *compliance* e de auditoria interna. Estas três funções devem ser independentes das restantes linhas de negócio, da sua monitorização e controlo.

IG15: A função de controlo de riscos deve assegurar o cumprimento das políticas de risco. A função de controlo de riscos deve ter uma estrutura de controlo apropriada, incluindo políticas de controlo e procedimentos, e que permita verificação do seu cumprimento. Esta função é desenhada para abordar os riscos que a instituição identificou no processo de avaliação de riscos. Em instituições com estruturas de maior dimensão, complexidade ou grau de sofisticação, esta função deve ter como objetivo a monitorização de cada risco material a que a instituição esteja exposta. Os órgãos de gestão devem avaliar continuamente os riscos que afetam o cumprimento dos seus objetivos e devem reagir à alteração de circunstâncias e condições.

IG16: A função de *compliance* deve identificar e avaliar riscos de *compliance*.

É da competência do órgão de administração aprovar uma política que considere o risco de *compliance*, isto é, o risco de não cumprimento de normas legais ou regulamentares que se possam traduzir em perdas financeiras, por via de sanções, e/ ou danos reputacionais.

Os órgãos de gestão devem estabelecer e comunicar a política de *compliance* e assegurar de que esta é cumprida.

A função de *compliance* deve, no entanto, aconselhar os órgãos de gestão no cumprimento de leis, normas e regulamentos.

No caso de instituições mais pequenas ou menos complexas, a função de *compliance* pode ser executada pela função de controlo de riscos ou de auditoria interna.

IG17: A função de auditoria interna deve permitir os órgãos de gestão assegurar que a qualidade dos controlos internos é efetiva e eficiente.

Se, por um lado, o órgão de gestão é responsável por estabelecer um sistema de controle interno de acordo com os requisitos legais, é da responsabilidade da auditoria interna avaliar a adequabilidade dos controles internos (incluindo as funções de controle de riscos e de *compliance*) e reportar as suas conclusões à Administração. Para o efeito deve ter acesso ilimitado a documentos e informação necessários em todas as áreas de negócio. Deve avaliar o cumprimento das atividades de acordo com as políticas e procedimentos, bem como se estas se mantêm adequadas. As recomendações de auditoria devem ser formalmente acompanhadas pelo nível hierárquico específico de modo a garantir a sua resolução. O auditor interno deve ter livre acesso aos órgãos de gestão e/ ou ao Comité de Auditoria, quando aplicável.

IG18: Deve existir um sistema de controlo interno efetivo e um sistema de informação credível cobrindo todas as atividades significantes da instituição. Os sistemas de informação eletrónicos devem ser seguros, monitorizados com independência e devem existir planos de contingência adequados.

IG19: Os órgãos de gestão devem disponibilizar a todos os funcionários, mecanismos de alerta que estes podem utilizar para comunicar assuntos relativos a *Internal Governance*. Estes mecanismos (de reporte de *raising concerns* e/ ou *whistleblowing*) devem respeitar a confidencialidade daqueles cujas preocupações foram reportadas. Todos os funcionários têm assim oportunidade de reportar as suas preocupações fora das suas linhas de reporte.

D – Divulgação de informação pública e transparência:

IG20: As instituições devem cumprir os requisitos de transparência no seu negócio.

Para a maioria das instituições, as expectativas dos investidores, clientes, agências de *rating* e outros exigem um elevado grau de transparência, na medida em que necessitam de fazer uma avaliação verdadeira e apropriada da instituição. É desejável que haja informação pública sobre a constituição dos órgãos de gestão, estrutura organizacional básica, política de incentivos e natureza e alcance das transações com filiais e associadas. Pode ser ainda interessante que estas descrevam como está organizada a gestão de risco e as funções de controlo de riscos, *compliance*, auditoria interna, bem como as principais tarefas adstritas a estas áreas, como é monitorizada a *performance* das mesmas e como as melhorias necessárias, caso as existam, irão ser implementadas.

IG21: Cada instituição deve apresentar a sua posição atual e as perspetivas futuras de forma equilibrada, precisa e atempada.

A informação sobre a posição corrente deve cumprir com os requisitos legais de divulgação da informação. A informação deve ser exata, relevante, atempada e de fácil acesso, de modo a ir de encontro às necessidades dos supervisores, investidores, clientes, agências de *rating*, empresas externas de avaliação de crédito e do público em geral. Quando para assegurar um nível elevado de precisão, o prazo fique comprometido, deve ser feito um julgamento, tendo em conta a imagem verdadeira e apropriada da posição da instituição. Este não deve ser um motivo para a não entrega de informação regular, devendo ser dada uma explicação das circunstâncias que justifiquem a ocorrência de uma exceção. A informação divulgada deve incluir mas não estar limitada à informação material nos resultados financeiros e operacionais, fatores de risco previsíveis, estrutura de *Governance* e políticas.

Com a publicação deste documento, as empresas têm assim um conjunto de linhas orientadoras sobre qual a estrutura de *Governance* que devem adotar e, por outro lado, os supervisores, ao avaliar o *Governance* das instituições, beneficiam da existência de uma maior consistência entre elas.

3.3 - O Controlo Interno na Banca em Portugal

3.3.1 O Modelo de Avaliação de Riscos

O Pilar II do Acordo Basileia introduz o conceito de *Internal Capital Adequacy Assessment Process* (ICAAP) ao estabelecer que as instituições devem adotar sistemas e procedimentos adequados que permitam identificar e medir os riscos, bem como ajustar o capital interno ao seu perfil de risco, às suas estratégias e planeamento de modo a enfrentar as adversidades do negócio com fundos próprios. Por outro lado, numa abordagem prudencial, este acordo, atribui competências às autoridades de supervisão, não só pela avaliação destes sistemas e procedimentos, mas também pela imposição de medidas necessárias ao cumprimento de requisitos de ICAAP.

Estes princípios encontram-se incorporados na Diretiva 2006/48/CE, do Parlamento Europeu e do Conselho, de 14 de Junho de 2006, nos artigos 123.º e 124.º. Na sequência da publicação dos Decretos-Lei n.º103/2007 e 104/2007, de 3 de Abril, que resultam da incorporação destes artigos, são também introduzidas alterações ao Regime Geral das

Instituições de Crédito e das Sociedades Financeiras (RGICSF). Assim, em cumprimento dos artigos 14.º e 17.º do RGICSF, as instituições deverão adotar dispositivos sólidos de *Internal Governance*¹⁸, bem como implementar processos de avaliação do seu ICAAP, conforme previsto no artigo 28.º do Decreto-Lei n.º104/2007. Adicionalmente, o artigo 116.º do RGICSF vem determinar que cabe ao Banco de Portugal, enquanto autoridade de supervisão, analisar e avaliar se os dispositivos de *Internal Governance*, as estratégias, os processos e os mecanismos aplicados a que as instituições de crédito estão obrigadas são suficientes e adequados para aferir e gerir os riscos a que estão ou possam vir a estar expostas, assim como se os fundos próprios que detêm garantem uma gestão sólida e a cobertura dos seus riscos.

Para fazer face às responsabilidades que se impunham, o Banco de Portugal desenvolveu o MAR que consiste numa metodologia usada para avaliar o perfil de risco das entidades sujeitas a supervisão, em resultado da convergência dos princípios e práticas das autoridades de supervisão europeias, facilitando deste modo, a comunicação entre estas e o Banco de Portugal, bem como entre este e as instituições financeiras ou grupos económicos. O MAR foi desenvolvido a partir das orientações do Comité Basileia e do CEBS no que respeita a sistemas de avaliação de riscos, definindo claramente quais os riscos e controlos a avaliar, determinando a base da avaliação dos riscos e incluindo procedimentos com vista à obtenção de resultados objetivos e credíveis.

Assim, o MAR não é mais do que instrumento onde se encontram sistematizados critérios e os procedimentos de forma objetiva, que têm como missão apoiar o Supervisor, neste caso, o Banco de Portugal, na revisão e avaliação de riscos inerentes à atividade financeira de cada instituição (ou grupo financeiro) e da adequabilidade dos rácios de solvabilidade e de liquidez, assim como dos processos de gestão. A introdução deste modelo, veio ainda permitir aferir sobre a qualidade e robustez do *Governance* e conferir maior consistência aos critérios utilizados, promovendo a comparabilidade e transparência dos resultados, tornando possível a identificação atempada de deficiências, a atuação preventiva sobre as mesmas e definindo áreas de acompanhamento.

Da utilização deste modelo, resulta uma notação ao perfil de risco de cada instituição, suportada em riscos intrínsecos, ou seja, na probabilidade de ocorrências de factos que resultem de atividades relacionadas com a própria atividade, bem como uma análise do

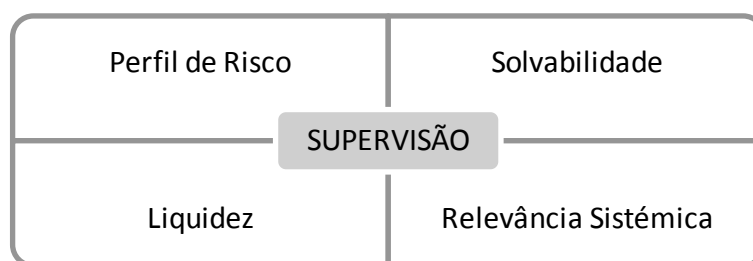
¹⁸ Este conceito, aqui, está relacionado não só com a organização e gestão como também com os processos implementados para avaliar, acompanhar e controlar os riscos

Governance, desde a definição de objetivos estratégicos, à identificação dos riscos e dos controlos implementados para os mitigar.

Adicionalmente, o MAR considera a avaliação e adequação da liquidez e solvabilidade das instituições, assim como a qualidade dos processos de gestão das mesmas.

A definição da intensidade e frequência das ações de supervisão, é determinada em função da análise do perfil de risco, da solvabilidade e liquidez, devendo respeitar o princípio da proporcionalidade a que se refere o artigo 116.º- A do RGICSF e considerar as características individuais de cada instituição, tais como a dimensão, a relevância sistémica das mesmas para o sistema financeiro, a natureza, o nível e a complexidade das atividades da instituição em causa, admitindo que esta periodicidade deve ser, no mínimo, anual.

Table 3.1 Supervisão



Fonte: Adaptado de MAR (2007), Banco de Portugal

O quadro acima (Quadro 3.1) ilustra bem o posicionamento da supervisão face aos indicadores acima referidos, estando a periodicidade com que os supervisores exercem a sua atividade relacionada com o resultado da análise destes.

3.3.1.1 – Avaliação das categorias de risco e de controlos

Para proceder à avaliação dos riscos, o MAR (2007) agrupa os riscos em categorias, distinguindo-os, quanto à sua natureza, em financeiros (risco de crédito, risco de mercado, risco de taxa de juro e risco de taxa de Câmbio) e não-financeiros (risco de estratégia, risco operacional, risco de sistemas de informação, risco reputacional e risco de *compliance*)¹⁹. Por outro lado, da análise dos dispositivos de *Governance* resultam três categorias de controlos: organização, gestão e controlos específicos de cada risco.

A organização, enquanto categoria de controlo, compreende toda a estrutura da instituição, considerando as funções de auditoria interna e externa, as linhas de reporte, a interação e dependência das áreas funcionais, assim como o sistema de informação.

¹⁹ Estes riscos serão abordados mais adiante, aquando do estudo do Aviso n.º 5/2008 do Banco de Portugal

A gestão, tem em conta a aptidão dos responsáveis de gestão para desempenhar com competência as suas funções, a sua atitude face ao risco e ao controlo interno, se a estrutura é ajustada à dimensão e complexidade da instituição, a clareza e objetividade do planeamento estratégico e o processo de decisão.

Dos controlos específicos fazem parte as políticas, procedimentos e boas práticas implementadas e em uso a todos os níveis da instituição, e que permitem a identificação, avaliação, acompanhamento e controlo de cada um dos riscos intrínsecos.

Para assegurar uma boa avaliação de cada uma das nove categorias de risco, da solvabilidade e liquidez das instituições, foram identificadas quatro etapas, a saber:

1. Descrição e análise financeira, a qual passa por reunir informação financeira e dados qualitativos para melhor compreender a instituição, nomeadamente, a sua atividade, estratégias, perspetivas e riscos intrínsecos ao negócio.
2. Decomposição da instituição em áreas funcionais, fase em que são inventariadas as principais unidades de negócio, as suas funções e interação, de modo a conseguir identificar e avaliar os riscos e controlos existentes em todos os níveis da instituição. Este processo permite identificar áreas de maior risco ou de maior debilidade nos controlos e facilita a ação dos supervisores ou outros, tais como auditores. O processo de decomposição de uma instituição em áreas funcionais passa pelos seguintes passos:
 - Identificação de todas as áreas funcionais da instituição;
 - Seleção das áreas funcionais a avaliar;
 - Atribuição de pesos às áreas funcionais significativas;
 - Determinação das categorias de risco e controlo relevantes e atribuição dos ponderadores;
 - Decisão pela avaliação integral ou simplificada das áreas funcionais.
3. Avaliação dos riscos e dos controlos, tendo por base os fatores específicos identificados para cada um deles, designados de rúbricas de referência, que influenciam cada um dos riscos ou a qualidade dos controlos existentes. A avaliação destes riscos reflete a opinião do supervisor sobre a probabilidade dos eventos, considerados para cada rúbrica, serem suscetíveis de ter impacto negativo no capital ou resultados da instituição, tendo por base a grelha de notações da Tabela 3.2 que se segue:

Table 3.2 Grelha de notações para avaliação de riscos

Avaliação do risco	Reduzido	Moderado	Material	Elevado
Notação correspondente	1	2	3	4

Fonte: Adaptado de MAR (2007: 24), Banco de Portugal

No que se refere à categoria dos controlos, a avaliação de cada rúbrica reflete, por sua vez, a opinião do supervisor sobre se o conjunto de fatores que constituem cada rubrica se encontram em condições de assegurar a mitigação dos riscos e se estão ajustados à dimensão e complexidade da atividade da instituição. Na Tabela 3.3 encontram-se espelhadas as notações referentes à avaliação de controlos.

Table 3.3 Grelha de notações para avaliação de controlos

Avaliação do controlo	Bom	Aceitável	Melhorável	Deficiente
Notação correspondente	1	2	3	4

Fonte: Adaptado de MAR (2007: 24), Banco de Portugal

4. Agregação e reporte dos resultados, tendo como ponto de partida um modelo matemático, onde são introduzidas as notações de cada uma das categorias de risco e de controlo de cada área funcional e da própria instituição ou grupo financeiro. O supervisor, no entanto, pode substituir o resultado da aplicação deste modelo, por um que julgue refletir melhor a realidade da instituição, desde que o justifique.

Em modo de conclusão, os supervisores beneficiam da utilização deste modelo, na medida em que este lhes permite planear a sua atividade e alocar os seus recursos, no pressuposto de que devem fazer um acompanhamento mais frequente e/ou mais exaustivo às instituições que apresentam notações mais baixas.

3.3.1.2 – Solvabilidade e liquidez

A avaliação da solvabilidade e a liquidez, em base individual ou consolidada, requer uma análise autónoma, dado que estes elementos avaliam a situação financeira de uma instituição. Assim, quanto à solvabilidade e à liquidez, é importante avaliar dois aspetos:

- Adequação atual e esperada destes indicadores face à instituição (ou grupo);
- Qualidade da gestão.

No que diz respeito à solvabilidade, a avaliação deste indicador vai no sentido de verificar se a instituição dispõe de fundos próprios para fazer face aos riscos decorrentes da sua atividade, tendo em conta a estratégia definida e os requisitos mínimos exigidos pelo Banco de Portugal. Assim, é preciso verificar se, à data de avaliação, o rácio de solvabilidade estava enquadrado com o rácio mínimo legal exigido, se era suficiente face às perspetivas futuras de negócio, compará-lo com o rácio anteriormente definido como objetivo da instituição, apurando a causa de eventuais desvios, e ajustá-lo face aos riscos projetados. Para além disso, torna-se necessário avaliar o ICAAP relativamente ao perfil de risco, aos controlos existentes, estratégia e planeamento definidos e às necessidades de capital interno.

A análise da qualidade de gestão da solvabilidade tem em vista verificar se o sistema de gestão de riscos é sólido, eficaz e adequado à dimensão e complexidade das atividades da instituição, com vista à identificação, avaliação, acompanhamento e controlo dos riscos relevantes e manutenção de níveis adequados de capital, em função desses riscos, tendo em conta os objetivos definidos e os requisitos regulamentares (MAR, 2007).

A análise da liquidez consiste em verificar se a entidade dispõe de fundos líquidos, disponíveis, para cumprir as suas obrigações financeiras atempadamente, sem criar constrangimentos ao desenvolvimento da sua atividade. O risco de liquidez decorre assim da incapacidade de a instituição cumprir com as suas obrigações. O risco de liquidez pode ser mitigado através da implementação de mecanismos de controlo e de gestão adequados. Constituem rubricas de referência à avaliação do risco de liquidez, por exemplo, a avaliação da estrutura de vencimentos entre ativos e passivos e a capacidade de a instituição obter fundos em condições que não sejam penalizadoras (ibid.:1)

3.3.2 - O Aviso n.º 5 do Banco de Portugal

Com vista a melhorar a regulação a que o Conselho Nacional de Supervisores Financeiros (CNSF) se propunha e face à relevância que o controlo interno assumia nas instituições, o Banco de Portugal veio rever os requisitos aplicáveis às instituições, através da emissão do Aviso n.º 5 do Banco de Portugal, de 25 de Junho de 2008²⁰, no sentido de harmonizar os relatórios de controlo interno, quanto às exigências, quer do Banco de Portugal, quer da CMVM, no que diz respeito à estrutura, ao conteúdo e prazo de reporte dos mesmos.

²⁰ Este veio rever o Aviso n. 3/2006, de 9 de Maio, do Banco de Portugal

Assim, a existência de um controlo interno adequado e eficaz, que assegurasse o cumprimento de requisitos legais e regulamentares a que estas estavam sujeitas, uma gestão de riscos apropriada, a sua estabilidade financeira, bem como a do próprio sistema financeiro, tornou-se uma preocupação primária das instituições.

Este novo regulamento, sistematiza princípios básicos que devem nortear a implementação de um controlo interno, com base no *Internal Control Integrated Framework*, publicado pelo COSO, nas recomendações do *Basel Committee on Banking Supervision*, através do *Framework for Internal Control Systems in Banking Organisations* e nas orientações de *Governance* do CEBS.

Com esta revisão, pretende-se estabelecer os requisitos mínimos do controlo interno e as responsabilidades da Administração quanto ao controlo interno, bem como dar resposta às condições impostas no artigo 14.º do RGICSF, nomeadamente, no que concerne à apresentação de uma estrutura organizativa clara, com linhas de responsabilidade bem definidas, transparentes e coerentes; à organização de processos eficazes de identificação, gestão, controlo e comunicação dos riscos a que as instituições estejam ou possam vir a estar expostas e ao dever de dispor de mecanismos adequados de controlo interno, incluindo procedimentos administrativos e contabilísticos sólidos.

Para além da harmonização dos relatórios de controlo interno, que permitiu que as instituições passassem a emitir um único relatório, estes passam a ser também mais simples, dando principal relevo às deficiências e às oportunidades de melhoria do sistema de controlo interno, em detrimento da descrição de procedimentos de controlo interno anteriormente em vigor pelo Aviso n.º 3/2006.

O Aviso n.º 5/2008 aplica-se às instituições de crédito, às sociedades financeiras e às sucursais de instituições de crédito e de sociedades financeiras com sede em países terceiros, às sociedades gestoras de participações sociais sujeitas à supervisão do Banco de Portugal ao abrigo do disposto no artigo 117.º do RGICSF, quando sejam consideradas empresas-mãe.

O artigo 2.º da legislação em estudo define sistema de controlo interno como «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 vista a garantir»:

- que o desempenho de médio e longo prazo são alcançados de forma eficiente e rentável, que os ativos e recursos são utilizados eficazmente, que a continuidade do negócio e a própria sobrevivência da instituição se encontram assegurados através de uma adequada gestão e controlo dos riscos da atividade, da prudente e adequada avaliação dos ativos e responsabilidades e da implementação de mecanismos de proteção contra utilizações não autorizadas, intencionais ou negligentes - objetivos operacionais;
- que a informação financeira e de gestão, que suporta as tomadas de decisão e os processos de controlo, cumprem os objetivos da informação (completa, pertinente, fidedigna e tempestiva) - objetivos de divulgação;
- que os requisitos legais e regulamentares aplicáveis são cumpridos, nomeadamente, no que diz respeito à prevenção do branqueamento de capitais e do financiamento do terrorismo, ao código de conduta e deontológico, das regras e procedimentos internos e estatutários e quanto às recomendações do *Basel Committee on Banking Supervision* e do CEBS, de modo a mitigar riscos reputacionais e financeiros (sanções) - objetivos de *compliance*.

O sistema de controlo interno deve ser consistentemente aplicado em todos os departamentos e sucursais e a todos os níveis da instituição, ajustado à dimensão desta e à natureza e complexidade da sua atividade, bem como, aos riscos daí resultantes. Por último, deve ajustar-se à própria estrutura de *Governance* da instituição e à delegação de competências.

A instituição deve planear, implementar e manter de forma adequada o seu sistema de controlo interno. Deve ainda ter as suas estratégias, sistemas, processos, políticas e procedimentos bem documentados, devendo estes ser atualizados sempre que se justifique, mantendo sempre um arquivo com todas as versões, anteriores e atuais, bem identificadas.

De acordo com o artigo 3.º, e à semelhança dos componentes que encontramos para o COSO, a implementação de um sistema de controlo interno assenta em princípios gerais, tais como a (i) existência de um ambiente de controlo adequado; (ii) existência de um sistema de gestão de riscos sólido; (iii) existência de um eficiente sistema de informação e comunicação e (iv) de um processo de monitorização efetivo, com vista a garantir os objetivos a que o controlo interno se propõe. A grande diferença na apresentação dos

princípios apontados pelo Banco de Portugal face ao COSO, vai no sentido em que este determina que um sistema de gestão de riscos pressupõe, não só, a identificação dos riscos, como a sua avaliação, acompanhamento e controlo destes, enquanto o COSO separa o componente da avaliação de riscos do das atividades de controlo. Posto isto, cabe-nos fazer uma análise mais detalhada ao sistema de gestão de riscos proposto pelo Banco de Portugal.

O sistema de gestão de riscos deve compreender um conjunto integrado de processos que permitam compreender a natureza e a magnitude dos riscos que afetam todas as atividades, processos e sistemas da instituição, tendo em vista a implementação e o cumprimento dos seus objetivos estratégicos e, em complemento, deve garantir que são tomadas as diligências necessárias com vista a neutralizar os respetivos desvios.

Um sistema de gestão de riscos robusto passa pela identificação, avaliação, acompanhamento e controlo de todos os riscos materiais a que a instituição está exposta, de modo a assegurar que estes não irão influenciar significativamente os seus resultados.

A identificação dos riscos deve ser executada com uma periodicidade, no mínimo anual, que permita a identificação tempestiva de novos fatores de risco e a revisão dos existentes bem como a hierarquização dos riscos.

A avaliação dos riscos consiste na mensuração dos mesmos, com base em informação adequada e fiável, através do uso de parâmetros, como por exemplo, a realização de testes de esforço^{21, 22} ou, quando tal não seja possível, em análises que permitam formar um juízo fundamentado sobre a respetiva materialidade.

As instituições fazem o acompanhamento da exposição às várias categorias de risco (que serão abordadas mais à frente), através da elaboração de relatórios periódicos e tempestivos, com informação clara, fiável e substantiva, relativos à atividade desenvolvida.

²¹ Testes de esforço ou *Stress Tests* - permitem a determinação, quer individualmente, quer de uma forma agregada, da probabilidade de a instituição cumprir os seus compromissos face ao desenvolvimento adverso, num dado horizonte temporal, para os diferentes fatores de risco.

²² A realização destes testes podem englobar diferentes níveis de sofisticação, desde a realização de análises de sensibilidade simplificadas à realização de testes de cenários adversos que envolvam a evolução conjunta de diferentes fatores de risco.

O processo de controlo de riscos começa pela garantia de que os objetivos definidos são atingidos e que são tomadas as ações necessárias para responder adequadamente aos riscos previamente identificados. Nesse sentido, as instituições devem definir e rever anualmente os objetivos globais e os objetivos específicos de cada área funcional, o perfil de risco e o grau de tolerância ao risco, bem como políticas e procedimentos que sistematizem as tarefas inerentes a cada função. Estes últimos devem, por sua vez, incluir procedimentos e controlos, com vista à prevenção de riscos ou, se tal não for possível, à sua deteção e remediação imediata, tais como: as decisões e operações devem estar devidamente documentadas em formulários próprios, a definição e aplicação de requisitos para aprovar ou renovar as operações, a segregação de funções entre a autorização ou revisão vs. a execução, registo e guarda de valores e outra documentação, o reporte, análise de desvios e decisões daí resultantes, a existência de indicadores de alerta variados e de limites de risco prudentes, a restrição de acessos físicos e informáticos, a realização de verificações e reconciliações periódicas e a implementação de um *Business Continuity Plans* (plano de continuidade de negócio) e de *Disaster Recovery Plans* (plano de recuperação de desastres).

3.3.2.1 - Riscos a considerar pelo sistema de gestão de riscos

O Banco de Portugal, no artigo 11.º do presente aviso, no seu n.º 3, refere que os Bancos devem ter em consideração dez categorias de risco: riscos de crédito, de mercado, de taxa de juro, de taxa de câmbio, de liquidez, de *compliance*, operacional, dos sistemas de informação, de estratégia e de reputação, bem como todos os outros riscos que em circunstâncias específicas possam vir a ser materiais. Para melhor compreendermos o que cada um destes riscos significa, fazemos abaixo uma breve referência a cada um deles, tendo em conta, não só as alíneas de a) a j) deste diploma, mas também o contemplado pelo MAR (2007) que, por seu turno, está em linha com os riscos identificados com as *Guidelines on the Application of the Supervisory review Process under Pillar 2*:

Risco de crédito²³ – resultam em eventuais impactos negativos devido à incapacidade de uma contraparte cumprir os seus compromissos financeiros, incluindo possíveis restrições

²³ O Decreto-Lei n.º 157/2014, de 24 de Outubro, que procede à alteração ao RGICSF, aprovado pelo Decreto-Lei n.º 298/92, de 31 de Dezembro, agrega o risco de crédito e o risco da contraparte, artigo 115.º N, e separa-os do risco de concentração, artigo 115.º P.

à transferência de pagamentos do exterior; tem em conta a exposição a uma contraparte, linha de crédito ou garantia, pelo que inclui risco de concentração²⁴.

Risco de mercado – pressupõe a ocorrência de movimentos desfavoráveis no preço de mercado dos instrumentos da carteira em negociação, provocados, nomeadamente, por flutuações em taxas de juro, taxas de câmbio, cotações de ações ou preços de mercadorias. O risco de mercado está associado às posições a curto prazo de títulos da dívida, por exemplo, de moedas, de mercadorias e derivados;

Risco de taxa de juro – é a probabilidade de ocorrência de impactos negativos nos resultados ou no capital, devido a movimentos adversos nas taxas de juro dos elementos da carteira bancária, por via de desfasamentos de maturidades ou de prazos, da ausência de correlação perfeita entre as taxas recebidas e pagas nos diferentes instrumentos, ou da existência de opções embutidas em instrumentos financeiros do balanço ou elementos extrapatrimoniais;

Risco de taxa de câmbio – expressa a possibilidade de existência de perdas financeiras decorrentes de movimentos adversos nas taxas de câmbio, provocados pela conversão das posições abertas em moeda estrangeira, ou pela alteração da posição competitiva da instituição devido a variações significativas das taxas de câmbio;

Risco de liquidez – reflete a probabilidade de ocorrência de impactos negativos nos resultados ou no capital, em resultado da incapacidade da instituição dispor de fundos líquidos para cumprir as suas obrigações financeiras, à medida que as mesmas se vencem;

Risco de *compliance* – aqueles cujos factos decorrem de violações ou da não conformidade relativamente a leis, regulamentos, determinações específicas, contratos, regras de conduta e de relacionamento com clientes, práticas instituídas ou princípios éticos que se materializem em sanções, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de contratos;

Risco operacional – aqueles que decorrem de falhas na análise, no processamento ou liquidação de operações, bem como de fraudes internas e externas, da utilização de recursos em regime de subcontratação que não cumpram o código de conduta da

24 Ao abrigo do artigo 115.ºP do RGICSF, risco de concentração é aquele que é «decorrente das posições em risco sobre cada contraparte individualmente considerada, incluindo contrapartes centrais, conjuntos de contrapartes ligadas entre si e contrapartes que atuam no mesmo setor económico ou na mesma região geográfica, ou decorrente da mesma atividade ou mercadoria, ou da aplicação de técnicas de redução do risco de crédito, nomeadamente do risco associado a grandes riscos indiretos, é tratado e controlado, designadamente por meio de políticas e procedimentos definidos por escrito»

instituição, de processos de decisão internos ineficazes, de recursos humanos insuficientes ou inadequados ou da inoperacionalidade das infraestruturas;

Risco de sistemas de informação - considera a probabilidade de ocorrência de impactos negativos nos resultados ou no capital, em resultado da inadaptabilidade dos sistemas de informação a novas necessidades, da sua incapacidade para impedir acessos não autorizados, para garantir a integridade dos dados ou para assegurar a continuidade do negócio em casos de falha, bem como devido ao prosseguimento de uma estratégia desajustada nesta área;

Risco de estratégia - aqueles que estão ligados com decisões estratégicas inadequadas, da deficiente implementação das decisões ou da incapacidade de resposta a alterações do meio envolvente ou a alterações no ambiente de negócios da instituição;

Risco de reputação - aqueles que têm impactos negativos na imagem pública da instituição, percecionados por clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral.

Quando tal se justifique e seja devidamente fundamentado, as instituições podem adotar as suas próprias definições de risco, desde que estes contemplem todos os fatores acima referidos.

Santos (2010) agrupa estas categorias de risco de acordo com as suas especificidades: a) riscos financeiros inerentes ao negócio bancários, onde inclui o risco de crédito, risco de mercado, risco de taxa de juro, risco de taxa de câmbio e o risco de liquidez; b) riscos de outra natureza, como o risco de *compliance*, risco operacional e o risco de sistemas de informação e c) riscos de natureza transversal, onde se pode incluir o risco de estratégia, que decorre de decisões estratégicas inadequadas ou da não implementação das mesmas e da falta de capacidade de resposta a alterações das condições externas ou do próprio ambiente de controlo da instituição, e o risco reputacional, que se prende com uma imagem negativa da instituição perante o público.

Os riscos de outra natureza têm sido objeto de grandes discussões e muito se tem feito em relação a estes, quer a nível nacional, através da criação de regulamentação específica, quer a nível internacional, por via da criação de normas e códigos de boas práticas (ibid.: 1).

Por outro lado, apesar do grande impacto que os riscos de estratégia e de reputação têm nas instituições, em termos de controlo interno e respetiva monitorização, é nestes que se tem vindo a verificar um menor investimento por parte das instituições.



Figure 3.1 Categorias de risco
Fonte: InforBANCA 83 (2010)

A Figura 3.1 acima ilustra a abordagem feita pelo controlo interno face às diversas categorias de risco consideradas.

3.3.2.2 – *Funções de controlo*

O Banco de Portugal é perentório ao determinar que as instituições de crédito identifiquem responsáveis de cargos que, não pertencendo aos órgãos de administração ou fiscalização, exerçam funções que lhes confirmam influência significativa na gestão das mesmas. Assim, no n.º 2 do artigo 33.ºA do Decreto Lei n.º 157/2014 que altera o RGICSF, institui a existência de três funções essenciais, a fazer parte do seu *Governance* das instituições financeiras: funções de *compliance*, auditoria interna, controlo e gestão de riscos.

O Aviso 5/2008 considera também, ao longo do seu conteúdo, a existência de uma função de gestão de riscos e uma função de *compliance*, como parte integrante do processo de gestão de riscos, e uma função de auditoria interna, integrada no processo de monitorização. Estas funções deverão ser desempenhadas por profissionais com as competências adequadas e que atuem de forma independente face às outras áreas funcionais da instituição, de modo a evitar conflitos de interesse. Porém, em consonância com o princípio da proporcionalidade já referido na IG14, existem exceções no que se refere a esta exigência, tendo em conta a dimensão das instituições, de modo a poder garantir que essas funções são executadas nas instituições de menor dimensão.

O artigo 16.º deste diploma estabelece que o responsável da área de gestão de riscos deve assegurar que o sistema de gestão de riscos é efetivo, fazendo o acompanhamento contínuo

do mesmo, verificando se este se mantém adequado e a funcionar eficazmente, bem como se as ações de remediação adotadas para corrigir eventuais deficiências se mantêm ajustadas.

O gestor de riscos aconselha o órgão de administração, elabora e apresenta a este e ao órgão de fiscalização um relatório de periodicidade, pelo menos, anual relativo à gestão de riscos, onde devem ser mencionadas as ações tomadas para corrigir eventuais fragilidades do sistema de controlo interno.

Os membros da equipa de gestão de riscos devem ter autonomia e liberdade para executar o seu trabalho, devendo, para tal, ter acesso a toda informação que se verifique ser necessária ao desempenho das suas funções. A remuneração destes não pode comprometer a objetividade que a função merece.

Contudo, note-se que o n.º 4 e 5 deste artigo, colocam uma exceção ao cumprimento do requisito de independência previsto, sempre que o número de colaboradores da instituição, excluindo os administradores, seja inferior a trinta e os proveitos operacionais no último exercício económico sejam inferiores a €20.000.000, no entanto, as instituições devem implementar mecanismos que assegurem um sistema de gestão de riscos efetivo.

Adicionalmente, o artigo 17.º do mesmo diploma, estabelece que compete ao *compliance* a função de, permanentemente, acompanhar e avaliar se os mecanismos existentes são adequados para detetar os riscos de não cumprimento das obrigações legais e dos deveres regulatórios a que as instituições estão sujeitas, bem como das medidas tomadas para corrigir eventuais deficiências encontradas. O *Compliance Officer* deve aconselhar os órgãos de administração e de gestão no que se refere a questões regulatórias e reportar quaisquer indícios de violação de obrigações legais, de regras de conduta e de relacionamento com clientes ou outros, que tenham por base um ato ilícito ou uma contraordenação. É o responsável pelo sistema de controlo interno de prevenção do branqueamento de capitais e do financiamento do terrorismo, bem pela comunicação destes às autoridades competentes. Para além disso, anualmente, deve apresentar ao órgão de administração e ao órgão de fiscalização um relatório anual onde identifique incumprimentos verificados e as respetivas ações corretivas adotadas.

O *Compliance Officer* deve ter poderes ajustados ao desempenho da sua função. Os membros da equipa de *compliance*, devem ter autonomia e liberdade para executar o seu trabalho, devendo, para tal, ter acesso a toda informação que se verifique necessária ao

desempenho das suas funções. A remuneração destes não pode comprometer a objetividade que a função merece.

As responsabilidades de *compliance* podem, no entanto, ser executadas pelo pessoal integrado em outras estruturas, desde que essa afetação se encontre devidamente justificada.

A exceção ao requisito da independência de *compliance*, prevista nos n.º 3 e 4 do presente artigo, é apenas considerada, para o caso das instituições cujo número de colaboradores (administradores não incluídos) seja inferior a seis e os proveitos operacionais do exercício anterior sejam inferiores a €1.000.000.

As avaliações autónomas efetuadas por um auditor interno ou subcontratado a entidades competentes fazem parte de um processo de monitorização efetivo. Porém, há exceções. Para o efeito, encontram-se dispensadas do cumprimento deste requisito, as entidades em que, face à sua natureza, dimensão e à complexidade da sua atividade, esta função não seja exequível, ou proporcional, como é o caso das instituições com um número de colaboradores (exclui administradores) inferior a trinta e em que os proveitos operacionais no último exercício tenham sido inferiores a €20.000.000, devendo neste caso estar sujeitas a procedimentos de monitorização adicionais.

Para a generalidade das instituições, no entanto, a função de auditoria interna é permanente e deve ser desenvolvida em conformidade com as normas internacionais de auditoria aplicáveis. Os membros do departamento de auditoria interna devem ter acesso ilimitado a toda a informação necessária à execução das mesmas, incluindo à relativa às sucursais.

A função de auditoria deve fazer parte da estrutura organizacional, com linha de reporte direto ao órgão de administração, devendo apresentar-lhe as deficiências identificadas, assim como as subsequentes recomendações, as quais devem estar oportunamente registadas e documentadas. As situações identificadas devem ser acompanhadas por forma a garantir que são tomadas as medidas corretivas necessárias.

O relatório de auditoria deve ser apresentado ao órgão de administração e ao órgão de fiscalização, com uma periodicidade anual, o qual deve conter uma síntese das principais deficiências detetadas nas ações de controlo.

No que se refere aos grupos financeiros, a empresa-mãe deve assegurar que as suas filiais implementam sistemas de controlo interno coerentes entre si e em conformidade com os requisitos definidos no Aviso, bem como estabelecer procedimentos apropriados no que

concerne aos requisitos relativos aos limites de realização de operações e de capital a que se referem os artigos 99.º, 100.º, e 113.º do RGICSF.

As instituições pertencentes ao mesmo grupo financeiro podem estabelecer serviços comuns para o desenvolvimento de tarefas no que concerne às funções de gestão de riscos, de *Compliance* e de auditoria interna.

3.3.2.3 – Responsabilidades do órgão de administração

O órgão de administração é o órgão responsável pela implementação e manutenção de um sistema de controlo interno adequado e eficaz que garanta o cumprimento dos objetivos a que se refere o artigo 2.º. Para tal, é necessário que estes estejam bem definidos, bem como os princípios em que deve assentar o sistema de controlo interno, os quais devem ser parte integrante da estratégia e estar refletidos nas políticas da organização. Para levar a cabo a implementação do sistema de controlo interno, é preciso que existam recursos materiais e recursos humanos suficientes e adequados, e, se necessário, promover ações de formação e consciencialização destes últimos.

O órgão de administração é responsável por definir a estratégia e garantir que a estrutura organizacional é ajustada à implementação do sistema de controlo interno, bem como por garantir que existe uma cultura de integridade e ética e um código de conduta devidamente divulgados e interiorizados por todos os colaboradores da instituição. Compete-lhe ainda tomar as ações necessárias caso sejam identificadas fragilidades na estrutura organizacional, incumprimentos da cultura organizacional ou eventuais desvios face à estratégia definida.

O órgão de administração é responsável por assegurar que todos os colaboradores dentro da instituição conhecem e compreendem o seu papel e de como podem contribuir positivamente para o controlo interno. Deve ainda certificar-se que dispõe de trabalhadores em número e com *know-how* necessários ao desempenho das suas funções e que os gestores de topo são suficientes e possuem conhecimentos, experiência e integridade necessários para o desempenho das suas funções. É responsável pelo processo de implementação de políticas de recursos humanos, nomeadamente as relativas ao recrutamento e seleção, avaliação de desempenho, compensação e benefícios e formação, bem como das medidas e sanções disciplinares. Deve identificar previamente eventuais

áreas de conflitos de interesse, eliminá-las ou, se tal não for totalmente possível, promover a sua monitorização.

Este órgão deve ter um conhecimento adequado dos tipos de riscos a que a instituição se encontra exposta e dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos, bem como das obrigações legais e dos deveres da instituição, sendo responsável pelo estabelecimento e manutenção de um sistema de gestão de riscos e de um sistema de controlo interno apropriados e eficazes.

Deve definir e rever a política de acordo com os objetivos globais e os objetivos específicos para cada área funcional, no que respeita ao perfil de risco e ao grau de tolerância face ao risco, bem como aprovar, previamente à sua introdução, os novos produtos e atividades da instituição e as políticas de gestão de risco que lhes estão associadas. Compete-lhes ainda verificar, de forma regular, o cumprimento dos níveis de tolerância ao risco e das políticas e procedimentos de gestão de riscos, avaliando a sua eficácia e contínua adequação à atividade da instituição, no sentido de possibilitar a deteção e correção de quaisquer deficiências.

O órgão de administração aprova políticas e procedimentos concretos, eficazes e adequados à identificação, avaliação, acompanhamento e controlo dos riscos a que a instituição está exposta, e ao processo de monitorização, assegurando a sua implementação e cumprimento. Solicita a elaboração e procede à apreciação de reportes periódicos, que sejam precisos e tempestivos, sobre os principais riscos a que a instituição se encontra exposta e que identifiquem os procedimentos de controlo implementados para gerir esses riscos, bem como os reportes sobre a adequação e a eficácia do sistema de controlo interno, no sentido de possibilitar a deteção e correção de quaisquer deficiências.

Deve assegurar a efetiva implementação das orientações e recomendações resultantes destes relatórios, no sentido de introduzir correções e/ ou ações de melhoria no sistema de gestão de riscos e de controlo interno.

É da competência do órgão de administração, nomear os responsáveis pelas funções de gestão de riscos, de *compliance* e auditoria interna, bem como assegurar que estas funções têm autonomia e autoridade suficientes para desempenhar as suas funções de forma objetiva e independente, e que possuem os recursos, materiais e humanos, necessários ao desempenho das respetivas tarefas, devendo ainda pronunciar-se sobre os relatórios elaborados por estes, nomeadamente sobre as recomendações para a adoção de medidas corretivas.

O órgão de administração é responsável pela implementação e manutenção de processos de informação e de comunicação adequados à atividade e aos riscos da instituição.

3.3.2.4 – O relatório de controlo interno

O artigo 25.º do aviso refere-se aos requisitos do relatório individual a ser remetido ao Banco de Portugal, estabelecendo que, o órgão de administração da instituição deve remeter-lhe anualmente, e até ao final de Junho, o já referido relatório de controlo interno. Este deve conter uma descrição da estratégia de negócio da instituição e perspetivas futuras, o organograma com identificação das áreas funcionais e seus responsáveis e as atividades e funções desempenhadas por empresas subcontratadas e identificação destas.

Quanto às funções de *compliance*, de gestão de riscos e auditoria interna, os seus responsáveis devem estar devidamente identificados. No relatório, devem ainda encontrar-se descritas as deficiências detetadas por cada uma destas funções, quer tenham sido identificadas em relatórios anteriores ou desde o último relatório e que ainda se encontrem por corrigir, até 30 dias antes da data do seu envio, bem como a respetiva informação sobre a categoria e grau de risco associados, impactos previstos, medidas corretivas em curso e prazo previsto para a regularização das mesmas (ver Apêndice I).

A não adoção de uma destas funções por parte das instituições, obriga a que estas justifiquem que reúnem os requisitos necessários para serem abrangidas pelas exceções previstas e que, para o caso da função de gestão de riscos, descrevam os mecanismos alternativos implementados com vista a garantir a existência de um sistema de gestão de riscos efetivo.

O relatório deve incluir a opinião global do órgão de administração, sobre a adequabilidade e eficácia do sistema de controlo interno, até 15 dias antes do envio do relatório ao Banco de Portugal, e ser acompanhado de um parecer do órgão de fiscalização da instituição sobre a adequação e eficácia do sistema de controlo interno e do Revisor Oficial de Contas (ROC) sobre o sistema de controlo interno subjacente à preparação e divulgação do relato financeiro. No que se refere às Caixas de Crédito Agrícola Mútuo (CCAM) integrantes do Sistema Integrado do Crédito Agrícola Mútuo (SICAM), em caso de inexistência do revisor, o parecer deve ser elaborado pelo órgão de fiscalização. Nos casos em que as instituições tenham um fiscal único, este deve emitir parecer sobre a adequação e eficácia do sistema de controlo interno e sobre a eficácia deste na preparação e divulgação das demonstrações financeiras.

O artigo 26.º do presente aviso, apresenta as disposições relativas aos relatórios de controlo interno de grupos financeiros. Assim, a empresa-mãe deve enviar anualmente um relatório sintético sobre o controlo interno do grupo onde apresente a sua estrutura organizativa, bem como as atividades e funções exercidas centralmente. Deve ainda incluir uma descrição de eventuais deficiências detetadas pela função de auditoria da empresa-mãe, com indicação da categoria, grau de risco, das suas potenciais implicações e medidas em curso ou a adotar para corrigir ou prevenir a sua ocorrência, bem como prazo previsto para resolução das mesmas. Adicionalmente, deve apresentar relatórios individuais de cada uma das entidades sujeitas a supervisão em base consolidada, ou não, e respetivos pareceres, à semelhança do previsto para as instituições individuais. Os pareceres sobre a adequabilidade e eficácia dos controlos internos podem ser emitidos pelo órgão de fiscalização para cada uma das filiais e pelo ROC da empresa-mãe em relação ao processo de preparação e divulgação da informação financeira consolidada. Os prazos para envio destes relatórios mantêm-se inalterados face aos relatórios individuais.

É de notar que, as alíneas b) e c) do n.º 2 do mesmo artigo excluem da obrigatoriedade de apresentação dos relatórios aqui referidos, as filiais no estrangeiro sem atividade relevante e que não influenciem o perfil de risco do grupo e aquelas cuja atividade se limite a um “escritório de representação”.

3.3.3 – A supervisão prudencial do Banco de Portugal

O Banco de Portugal exerce a função de supervisão 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 protecção dos interesses dos clientes.

As atribuições e competências do Banco de Portugal enquanto autoridade de supervisão encontram-se definidas na sua Lei Orgânica n.º 5/98, de 31 de Janeiro, no RGICSF e no Regime Jurídico relativo ao acesso à atividade das Instituições de Pagamento e à Prestação de Serviços de Pagamento (RJIPSP).

Está nas competências do Banco de Portugal o exercício da supervisão comportamental no domínio dos mercados de produtos e serviços bancários de retalho, tendo em vista mitigar a informação imperfeita que caracteriza os produtos e serviços financeiros e salvaguardar a equidade e eficiência daqueles mercados. No sentido de tornar toda a divulgação clara e

suficiente sobre os seus produtos e serviços, as instituições de crédito estão obrigadas a prestar informação aos seus clientes sobre as condições dos mesmos, ao abrigo do artigo 77.º do RGICSF.

Todavia, este normativo também assume um papel central na regulamentação prudencial portuguesa, com base na transposição das diretivas comunitárias existentes sobre esta matéria. No entanto, quando a harmonização não é possível, são as próprias autoridades de supervisão que definem as regras de atuação das instituições, por exemplo, como no caso dos requisitos de controlo interno estabelecidos pelo Aviso n.º 5/2008.

A nível macroeconómico e, no âmbito da sua função de manter a estabilidade financeira, o Banco de Portugal avalia e monitoriza os riscos emergentes nos mercados e no sistema financeiro, procurando identificar fragilidades (conceito de risco sistémico). Esta atividade envolve a análise global da situação e da evolução de todo o sistema financeiro, e implica a identificação e a probabilidade de incidentes e as respetivas consequências sobre a estabilidade do sistema. Neste contexto, o Banco de Portugal publica o relatório de Estabilidade Financeira e faz a análise sobre o sistema financeiro português.

A nível microeconómico, visa a salvaguarda da solvabilidade e liquidez das instituições e grupos financeiros, tendo em vista a proteção de valores que lhes estão confiados, e contribuindo, por essa via, para a estabilidade do sistema como um todo. O Banco de Portugal faz a manutenção de registo de elementos e acontecimentos obrigatórios e faz o acompanhamento da atividade e da situação financeira das instituições, isto é, analisa e avalia os riscos que podem afetar a solvabilidade (risco de crédito, risco de mercado, risco da taxa de juro, risco cambial, risco operacional, entre outros).

Assim, compete ao Banco de Portugal autorizar a constituição de instituições de crédito, sociedades financeiras e instituições de pagamento, acompanhar sistemática e continuamente a atividade destas, vigiar a observância das normas prudenciais que disciplinam a atividade das instituições, tais como os rácios, limites prudenciais e outros requisitos normativos, emitir recomendações e determinações específicas para resolução de irregularidades e aplicar sanções de não cumprimento às infrações praticadas. O Banco de Portugal exerce ainda funções de prevenção e fiscalização ao branqueamento de capitais e financiamento ao terrorismo, competindo-lhe em caso de infrações, instaurar processos de contra-ordenações e aplicar coimas e sanções acessórias. Constituem infrações neste âmbito, o não cumprimento dos deveres de exame e comunicação de operações suspeitas, bem como a não adoção e aplicação de um sistema de controlo interno destinado à

prevenção do branqueamento de capitais e financiamento ao terrorismo, por parte das instituições.

A monitorização da atividade das instituições financeiras pode ser efetuada por via da compreensão e análise da informação reportada periodicamente pelas instituições (supervisão *off-site*) e da realização de exames e inspeções (supervisão *on-site*).

- Supervisão *off-site*

O Banco de Portugal, para além da análise dos relatórios de contas apresentados, analisa outra informação, nomeadamente, com detalhe sobre a evolução das carteiras de crédito, das respetivas imparidades, a mensuração dos riscos e dos requisitos de capital. São ainda analisados os relatórios de controlo interno.

- Supervisão *on-site*

A supervisão *on-site* inclui a verificação do cumprimento dos montantes mínimos estabelecidos por lei para o capital social, os requisitos mínimos de fundos próprios para cobertura dos riscos de crédito, de mercado e operacional, os limites à concentração de riscos e as regras de provisionamento.

Existem outras medidas de controlo de riscos:

- Imposição de limites à concentração das posições credoras assumidas perante um cliente ou grupo de clientes “ligados entre si” e que não podem exceder determinada percentagem dos fundos próprios da instituição;
- Limites de participações em outras sociedades;
- Limites à concessão de empréstimos a acionistas e a membros dos órgãos de administração ou fiscalização;
- Verificação de rácios de liquidez e solvabilidade;
- Exigência de níveis mínimos de provisionamento de créditos vencidos.

Estas regras prudenciais têm em vista uniformizar a atuação das instituições financeiras, não podendo substituir a existência de sistemas de avaliação, gestão e controlo de riscos.

As instituições são responsáveis pela existência de um sistema de gestão de riscos interno.

Em consequência da crise financeira iniciada em 2007, o Banco de Portugal, apostou numa supervisão mais intrusiva dos Bancos (de que são exemplo os programas transversais de inspeções), adotou novos mecanismos de avaliação da situação de solvabilidade e de

liquidez dos oito principais grupos bancários - Banco Comercial Português, Banco BPI, Caixa Geral de Depósitos, Banco Espírito Santo, Caixa Económica Montepio Geral, Santander Totta, Banco Internacional do Funchal (Banif) e Grupo Crédito Agrícola -, baseados em planos de financiamento e de capitalização apresentados trimestralmente, e desenvolveu um novo indicador de risco (rácio do crédito em risco).

Assim, o Banco de Portugal desde 2011 passou a realizar inspeções periódicas e transversais à carteira global de crédito ou classes de ativos expostas a desenvolvimentos de mercado ou macroeconómicos que mereçam particular atenção nos tais Bancos. No que diz respeito aos programas transversais de inspeções, temos os Programas Especiais de Inspeções (SIP – *Special Inspections Programme*) e o Programa de Inspeções *On-site* (OIP – *on-site Inspections Programmes*).

Estas inspeções transversais permitem assegurar que as instituições estão a utilizar critérios suficientemente fortes e prudentes para calcular as imparidades das suas carteiras de crédito e, se for caso disso, solicitar o seu reforço. Essas inspeções têm em vista verificar:

- Base de cálculo das imparidades - para avaliar a base de cálculo das imparidades, as instituições devem definir alertas, tais como, a existência de cheques devolvidos, a reestruturação das operações de crédito, uma redução material dos *cash flows* estimados do devedor ou uma redução substancial do *rating* do devedor. Como tal, pode haver situações em que, apesar da inexistência de crédito vencido, é constituída uma provisão (imparidade) para cobertura parcial ou total da exposição em causa (dependendo do valor da garantia associada). Nas suas inspeções, o Banco de Portugal definiu alertas bastante exigentes, tendo sido selecionados créditos que ainda não se encontravam vencidos.
- Nível de cobertura do crédito em risco - pretende avaliar se a parte da carteira de crédito em risco que não foi contabilizada como imparidades se encontra coberta por colaterais associados aos créditos.
- Crédito vencido - considera o crédito vencido (capital e juro vencido há mais de 90 dias), crédito em incumprimento ao abrigo do Aviso 3/95 do Banco de Portugal e desde Setembro de 2011 o indicador de crédito em risco²⁵, introduzido pela Instrução 22/2011 do Banco de Portugal.

²⁵ NPL – *Non Performing Loans*

- Revisão dos ativos ponderados pelo risco²⁶ (RWA) - Prende-se com uma validação do cálculo dos requisitos de capital dos oito maiores grupos bancários nacionais, nomeadamente de fundos próprios para risco de crédito.
- Quanto ao método *Internal Ratings Based-approach* (IRB)^{27,28}, o Banco de Portugal tem adotado uma abordagem mais prudente aquando da autorização destes IRB's, procurando assim dar cumprimento aos requisitos da *Capital Requirements Directives* do *Basel Committee*, que culminou na Diretiva 2013/36/EU do Parlamento Europeu e do Conselho, de 26 de Junho, transposta para a Lei n.º 46/2014, de 28 de Julho.

Paralelamente, passa também a fazer uma análise da situação do capital e da liquidez, levando em linha de consideração perspectivas futuras, através da análise do modelo de negócio e dos planos de financiamento e de capital para os 2 ou 3 anos subsequentes.

O Banco de Portugal passou também a realizar *stress tests* para os esses mesmos grupos bancários, no intuito de avaliar se as instituições têm capacidade para suportar cenários económicos e financeiros adversos e, ainda assim, manterem rácios de capital *Core Tier 1*²⁹ acima de 6%, bem como pronunciarem-se sobre a robustez das metodologias e dos parâmetros utilizados pelos Bancos nesses exercícios.

No que respeita ao *Internal Governance* das instituições, desde 22 de Maio de 2013, o Banco de Portugal e as instituições deverão obedecer a um conjunto de orientações aprovadas em Novembro de 2012 pela EBA, num documento destinado a avaliar questões como a idoneidade, competências profissionais dos membros dos órgãos de administração e de gestão, o *Guidelines on the assessment of the suitability of members of the management body and key function holders*. Assim, ao abrigo dos artigos 30.º e 31.º do RGICSF, o Banco de Portugal, enquanto autoridade de supervisão deve, em base permanente e contínua, avaliar se os membros dos órgãos de administração e fiscalização

²⁶ RWA – *Risk-weighted asset*

²⁷ Os Bancos podem desenvolver os próprios modelos para o cálculo dos montantes de requisitos de fundos próprios para cobertura do risco de crédito e do risco de redução dos montantes a receber, em alternativa aos modelos padrão previstos nos artigos 10.º a 13.º do Decreto-lei 104/2007, contudo, estes terão que ser autorizados pelo supervisor em conformidade com o artigo 14.º do mesmo diploma

²⁸ Estes modelos devem ser aplicados às diferentes classes de risco estimar indicadores como PG (*probability of default*), EAD (*exposure at default*) e LGD (*loss given default*) e outros parâmetros para o cálculo do RWA. O capital mínimo é calculado com base numa percentagem do RWA

²⁹ Rácio que mede a adequabilidade dos capitais próprios aos ativos ponderados pelo risco. Quociente entre o conjunto de fundos próprios, designado de “core” e as posições ponderadas em função do seu risco.

possuem características de idoneidade, qualificação profissional, independência e disponibilidade para assegurar uma gestão sã e prudente das instituições de crédito e, deste modo, que o sistema financeiro e os interesses dos respetivos agentes de mercado se encontram salvaguardados. Esta avaliação ocorre no momento da autorização da criação da instituição e no decurso da sua atividade, quando exista um novo mandato ou uma alteração dos órgãos sociais, ou ainda, sempre que ocorram novos factos que impactem nos critérios anteriormente referidos. Esta avaliação é feita com base no modo como os membros da administração gerem as atividades da instituição e exercem a profissão, sendo ponderada a capacidade de decisão, se os comportamentos preservam os interesses dos *stakeholders* e do mercado e se estes cumprem com as suas obrigações.

A supervisão prudencial do Banco de Portugal constitui a quarta linha de defesa de uma instituição financeira, sendo a primeira, a estrutura de *Internal Governance*, seguida dos próprios sistemas de controlo interno e, em terceiro, a auditoria interna e externa. A Figura 3.2 ilustra o que aqui foi dito:

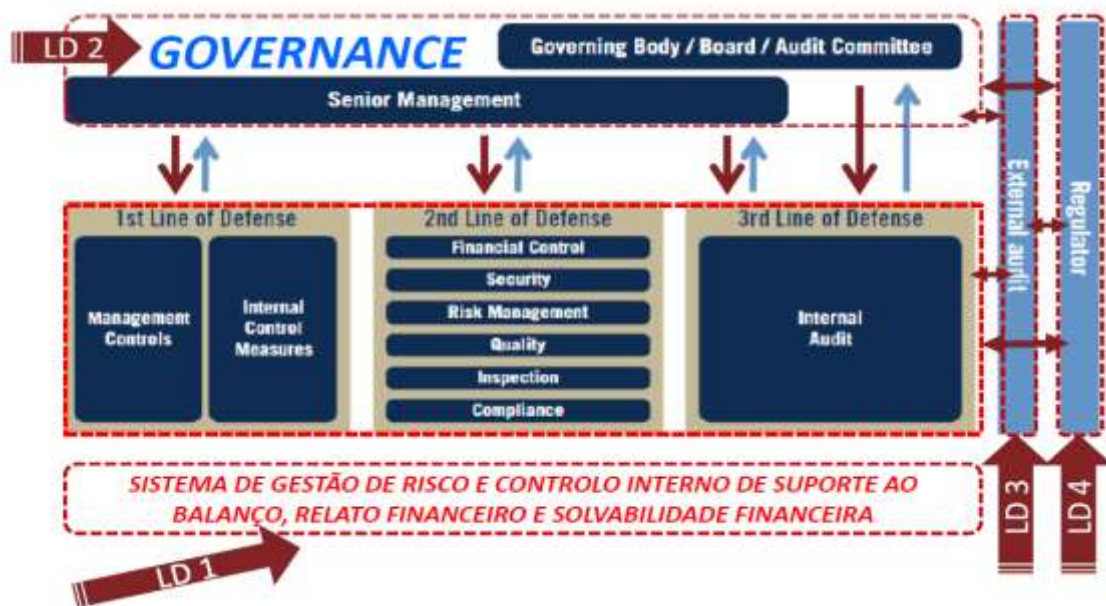


Figure 3.2 As quatro linhas de defesa das instituições financeiras

Fonte: XIII Conferência sobre Auditoria, Risco e *Governance* (2014), Banco de Portugal

O que atrás foi dito reforça a obrigatoriedade de que as instituições disponham de dispositivos de *Governance* sólidos, que incluam uma estrutura organizativa clara, com linhas de reporte e responsabilidades bem definidas, transparentes e coerentes. A existência

de sistemas de gestão de riscos adequados e eficazes e os respetivos mecanismos de controlo interno, incluindo procedimentos administrativos e contabilísticos, deverão também ser ponderados.

Quanto aos mecanismos de controlo interno, as exigências do Banco de Portugal, estão alinhadas com Aviso n.º 5 do Banco de Portugal, publicado em 2008.

Os auditores externos deveriam ter, no entanto, uma maior responsabilidade, na medida em deveriam assumir um papel mais interventivo, já que estes são independentes e, apesar de fazerem parte integrante do *Internal Governance*, devem pronunciar-se sobre a forma como este está implementado.

Cabe ao Banco de Portugal atuar de modo a reduzir a probabilidade de que as instituições financeiras possam vir a colocar em causa a estabilidade do sistema financeiro e a proteção dos investidores. O supervisor tem, então, que concentrar as suas ações nos riscos potenciais e no que as instituições representam para o sistema financeiro, ajustando a intensidade e intrusividade das mesmas em função da sua relevância sistémica.

Assim, a atuação prudencial do supervisor é exercida de modo intrusivo, prospetivo e com base nos principais fatores de risco para a estabilidade financeira, levando em conta a avaliação dos membros dos órgãos sociais das instituições de crédito e os mecanismos internos e externos de controlo do risco e de auditoria das instituições supervisionadas.

4. Estudo empírico

4.1 – Apresentação do Problema da Investigação

Os especialistas neste tema defendem que um bom controlo interno, a par de uma gestão de riscos eficiente, permite identificar riscos e transformá-los em oportunidades, minimizando os riscos de não cumprimento dos objetivos da organização. Do mesmo modo, uma das fases do trabalho do auditor consiste, precisamente, em obter uma compreensão do controlo interno da entidade, de modo a poder fazer um planeamento adequado da auditoria, permitindo-lhe, através da avaliação do risco de controlo, determinar a profundidade e extensão dos testes de controlos e substantivos (Costa, 2010). Assim, mais do que uma ferramenta de suporte à tomada de decisão, a utilização de um modelo de gestão de riscos pode servir de apoio à realização do trabalho do auditor, pelo que, podemos deduzir que a utilização destes modelos potencia um elevado grau de fiabilidade ao controlo interno das organizações, o que se traduz, conseqüentemente, numa melhoria da qualidade das auditorias e dos resultados das mesmas. Dito isto, a questão central deste trabalho é saber se esta realidade se verifica e responder à questão levantada: “o uso de um modelo de gestão de risco está positivamente relacionado com o resultado das auditorias?”. Levantado o problema de investigação, este estudo tem por objetivo estabelecer uma relação entre o uso de modelos de gestão de risco, enquanto ferramenta para obter um bom sistema de controlo interno, e o resultado das auditorias. Dado que, as instituições financeiras, através do Aviso n.º 5/2008, do Banco de Portugal se encontram obrigadas à adoção de um sistema de controlo interno suportado no COSO, iremos direcionar o nosso estudo e as respetivas conclusões para a área financeira, considerando que, ao abrigo do n.º 3 do artigo do 115.º do RGICSF, as instituições sujeitas à supervisão do Banco de Portugal devem publicar as suas contas nos termos e com a periodicidade definidas em aviso do Banco de Portugal, podendo este exigir a respetiva certificação legal³⁰. Pretende-se com este estudo, perceber se, a partir do uso de modelos de gestão de risco nas instituições financeiras portuguesas, estas conseguem uma informação mais transparente e credível, de tal forma que, o auditor possa atestar a veracidade da informação financeira divulgada.

³⁰ Esta redação foi introduzida pelo artigo 12.º do Decreto-Lei n.º 201/2002

4.2 – Apresentação do desenvolvimento e desenho da investigação

Uma vez formulada a questão a que se pretende responder com este estudo, será apresentado o desenho da investigação e a abordagem adequada para reunirmos informação necessária que nos permita chegar a conclusões. Este estudo incidirá sobre as entidades registadas no Banco de Portugal.

Após encontrarmos o nosso universo, iremos determinar a amostra. Para o efeito, é necessário definir o método de amostragem e a dimensão da amostra que iremos analisar.

No nosso estudo, gostaríamos de incluir algumas das principais instituições bancárias portuguesas e, como tal, entendemos que a seleção da nossa amostra deve ser efetuada não tanto pela “representatividade” (Vicente, Reis e Ferrão, 2001), descartando à partida o uso de uma técnica de amostragem aleatória, mas sim pela utilização de uma técnica de amostragem não aleatória, a amostra direcionada ou intencional, a qual tem por base o julgamento do investigador na escolha dos itens a serem testados, em função das características que esses elementos possuem, relativamente ao objetivo do estudo (Barañano, 2004). Numa amostra deste tipo, o investigador é que determina o tamanho da amostra que quer analisar, de acordo com os resultados que pretende obter, contudo, isso posicionar-nos-ia num espaço vazio, pois haveria o constrangimento de não conseguirmos fundamentar devidamente a nossa escolha e, uma vez que esta seria suportada numa opinião pessoal, a mesma poderia conduzir-nos a uma avaliação diferente da dos demais interessados neste estudo. Posto isto, para suportar a decisão da dimensão da amostra, baseamo-nos na recomendação de Freixo (2011), o qual considera que, não obstante o investigador dever considerar o objetivo do estudo e a homogeneidade do fenómeno, a dimensão mínima de uma amostra deverá ser de 30 itens.

4.3 – Seleção da amostra

Para encontrarmos o universo de entidades, fomos ao *site* do Banco de Portugal. Das instituições autorizadas, verificamos as que se encontravam abrangidas pelo Aviso n.º 5/2008, tendo excluído à partida as instituições com sede na União Europeia (EU) ou em países terceiros / estrangeiros, pelo facto de as suas Certificações Legais de Contas (CLC) não se encontrarem publicadas, já que, as filiais de instituições de crédito abrangidas pela supervisão do Banco de Portugal, que se encontrem sedeadas em países terceiros, estão sujeitas, para todos os efeitos legais, à supervisão em base individual pela autoridade de

supervisão desses países. O Banco de Portugal, nos casos em que seja a autoridade de supervisão responsável pela supervisão em base consolidada, atua em colaboração com essas autoridades no desempenho das competências de supervisão, em regime de reciprocidade (artigos 82.º e 138.º do RGICSF). Assim, na Tabela 4.1, está representado o universo das 170 instituições, consideradas por tipo de instituição:

Table 4.1 Entidades supervisionadas obrigadas a apresentar relatório de controlo interno

	TIPO DE INSTITUIÇÃO	REGISTOS NO BP
INSTITUIÇÕES DE CRÉDITO	Bancos	35
	Caixas Económicas	4
	Caixa Central de Crédito Agrícola Mútuo	1
	Instituições Financeiras de Crédito	15
	Sociedades de Garantia Mútua	4
	Sociedades de Investimento	2
	Sociedades de Locação Financeira	1
	Sociedades de Factoring	3
SOCIEDADES FINANCEIRAS	Sociedades Financeiras de Corretagem	2
	Sociedades Corretoras	5
	Sociedades Gestoras de Patrimónios	11
	Sociedades Gestoras de Fundos de Investimento	45
	Agências de Câmbios	10
	Sociedades Gestoras de Fundos de Titularização de Créditos	3
	Sociedades Administradores de Compras em Grupo	2
	Outras Sociedades Financeiras	1
SOCIEDADES GESTORAS DE PARTICIPAÇÕES SOCIAIS	Sociedades Gestoras de Participações Sociais (do Sector Financeiro)	26

Como já foi atrás referido, a metodologia que nos propomos seguir, passa pelo uso de uma amostra direcionada, já que pretendemos incluir determinadas instituições na nossa análise, atendendo à relevância que estas assumem no sistema financeiro português, razão pela qual admitimos enviesar a amostra. A nossa posição, aliás, corrobora com a do Banco de Portugal quando determinou que o programa de inspeções especiais seria direcionado para os oito maiores grupos bancários, ou seja, considerando a relevância sistémica destes para o sistema financeiro. Assim, embora não possamos deixar de admitir a subjetividade deste critério, é nossa opinião, todavia, que a amostra selecionada é típica da população.

A nossa análise será efetuada, para o ano de entrada em vigor do referido aviso (2008) e o último exercício, sobre as CLC emitidas pelos auditores externos das 30 instituições que a seguir apresentamos, na Tabela 4.2, onde incluímos as oito instituições anteriormente citadas:

Table 4.2 Nome e tipo de instituição a analisar

NOME DA INSTITUIÇÃO	TIPO DE INSTITUIÇÃO
BANCO ESPIRITO SANTO, SA	Bancos
BANCO BPI, SA	Bancos
BANCO SANTANDER TOTTA, SA	Bancos
BANCO BILBAO VIZCAYA ARGENTARIA (PORTUGAL), SA	Bancos
PEDRO ARROJA - GESTÃO DE PATRIMÓNIOS, SA	Sociedades Gestoras de Patrimónios
BANCO ACTIVOBANK, SA	Bancos
OPTIMIZE INVESTIMENTO - SGPS, SA	Sociedades Gestoras de Participações Sociais (do Sector Financeiro)
BANCO COMERCIAL PORTUGUES, SA	Bancos
CAIXA GERAL DE DEPOSITOS, SA	Bancos
CAIXA ECONOMICA MONTEPIO GERAL	Caixas Economicas
BANIF - BANCO INTERNACIONAL DO FUNCHAL, SA	Bancos
CAIXA CENTRAL - CAIXA CENTRAL DE CREDITO AGRICOLA MUTUO, CRL	Caixa Central e Caixas de Credito Agricola Mutuo
BANCO POPULAR PORTUGAL, SA	Bancos
BANCO FINANTIA, SA	Bancos
UNICÂMBIO - AGÊNCIA DE CÂMBIOS, SA	Agências de Câmbios
BANCO L.J. CARREGOSA, SA	Bancos
BANCO PRIMUS, SA	Bancos
FINCOR - SOCIEDADE CORRETORA, SA	Sociedades Corretoras
MERCEDES-BENZ FINANCIAL SERVICES PORTUGAL - INSTITUICAO FINANCEIRA DE CREDITO, SA	Instituicoes Financeiras de Credito
BNP PARIBAS FACTOR - INSTITUICAO FINANCEIRA DE CREDITO, SA	Instituicoes Financeiras de Credito
BANCO BNP PARIBAS PERSONAL FINANCE, SA	Bancos
BANCO CREDIBOM, SA	Bancos
NORGARANTE	Sociedades de Garantia Mútua
OREY FINANCIAL - INSTITUICAO FINANCEIRA DE CREDITO, S.A.	Instituicoes Financeiras de Credito
S. P. G. M. - SOCIEDADE DE INVESTIMENTO, SA	Sociedades de Investimento
FINANGESTE - EMPRESA FINANCEIRA DE GESTÃO E DESENVOLVIMENTO, SA	Outras Sociedades Financeiras
PORTUCALE, SGFTC, SA	Sociedades Gestoras de Fundos de Titularização de Créditos
GOLDEN ASSETS - SOCIEDADE GESTORA DE PATRIMÓNIOS, SA	Sociedades Gestoras de Patrimónios
SONAEGEST - SOCIEDADE GESTORA DE FUNDOS DE INVESTIMENTO, SA	Sociedades Gestoras de Fundos de Investimento Imobiliário
BANCO BIC PORTUGUÊS, SA	Bancos

4.4 – Recolha, análise e tratamento de dados

Em complemento ao n.º 3 do artigo 115.º do RGICSF, os Avisos n.º 6/2003 e 4/2006, vêm determinar que as instituições que se encontram sujeitas à supervisão do Banco de Portugal devem publicar o relatório de contas em base individual e consolidada, bem como os seus balanços trimestrais no *site* do Banco de Portugal, no Diário da República ou num jornal não-oficial de grande circulação.

Assim, a recolha de dados foi efetuada em *sites* públicos, nomeadamente no *site* do Banco de Portugal e da CMVM.

Reunida a documentação, foi efetuado o tratamento dos dados a fim de se poder avançar com a sua análise e posterior retirada de conclusões.

Antes de apresentarmos os dados obtidos, convém ainda lembrar que a CLC exprime a opinião do ROC de que as demonstrações financeiras apresentam (ou não), de forma verdadeira e apropriada, a posição financeira da empresa, bem como os resultados das suas operações, relativamente à data e ao período a que as mesmas se referem.

A Diretriz de Revisão / Auditoria (DRA) 700 estabelece que o ROC pode emitir os seguintes modelos de CLC:

- Opinião não-qualificada:

- CLC sem reservas e sem ênfases ou Certificação Limpa;
- CLC sem reservas mas com ênfases;
- Opinião qualificada (com reservas):
- Opinião com reservas por limitação de âmbito, quando existam limitações para emitir opinião, que possam ser materiais mas não profundas;
- Opinião com reservas por desacordo, quando exista desacordo suscetível de provocar distorções materiais mas não profundas;
- Opinião adversa, quando exista desacordo por distorções materiais e profundas;
- Escusa de Opinião, quando as limitações de âmbito são profundas;
- Declaração de impossibilidade de CLC, quando se lhe deparam situações de inexistência ou de insuficiência significativa ou até mesmo de ocultação de matéria de apreciação.

Após esta breve nota, estamos em condições de avançar com os dados obtidos sobre as CLC das instituições de crédito e sociedades financeiras em análise, transpostos para a Tabela 4.3:

Table 4.3 Resultados das auditorias

NOME DA INSTITUIÇÃO	MODELOS DE CLC	
	2008	2013
BANCO ACTIVOBANK, SA	Certificação Limpa	Certificação Limpa
BANCO BIC PORTUGUÊS, SA (ex- BPN, SA)	CLC com reservas por limitação de âmbito	CLC sem reservas mas com ênfases
BANCO BILBAO VIZCAYA ARGENTARIA (PORTUGAL), SA	Certificação Limpa	CLC sem reservas mas com ênfases
BANCO BNP PARIBAS PERSONAL FINANCE, SA (ex- CETELEM, SA)	CLC sem reservas mas com ênfases	Certificação Limpa
BANCO BPI, SA	Certificação Limpa	Certificação Limpa
BANCO COMERCIAL PORTUGUES, SA	Certificação Limpa	Certificação Limpa
BANCO CREDIBOM, SA	Certificação Limpa	Certificação Limpa
BANCO ESPIRITO SANTO, SA	Certificação Limpa	CLC sem reservas mas com ênfases
BANCO FINANTIA, SA	Certificação Limpa	Certificação Limpa
BANCO L.J. CARREGOSA, SA	Certificação Limpa	CLC sem reservas mas com ênfases
BANCO POPULAR PORTUGAL, SA	Certificação Limpa	Certificação Limpa
BANCO PRIMUS, SA	CLC sem reservas mas com ênfases	Certificação Limpa
BANCO SANTANDER TOTTA, SA	CLC sem reservas mas com ênfases	CLC sem reservas mas com ênfases
BANIF - BANCO INTERNACIONAL DO FUNCHAL, SA	Certificação Limpa	CLC sem reservas mas com ênfases
BNP PARIBAS FACTOR - INSTITUICAO FINANCEIRA DE CREDITO, SA	Certificação Limpa	Certificação Limpa
CAIXA CENTRAL - CAIXA CENTRAL DE CREDITO AGRICOLA MUTUO, CRL	CLC sem reservas mas com ênfases	CLC sem reservas mas com ênfases
CAIXA ECONOMICA MONTEPIO GERAL	CLC sem reservas mas com ênfases	Certificação Limpa
CAIXA GERAL DE DEPOSITOS, SA	Certificação Limpa	Certificação Limpa
FINANGESTE - EMPRESA FINANCEIRA DE GESTÃO E DESENVOLVIMENTO, SA	Certificação Limpa	Certificação Limpa
FINCOR - SOCIEDADE CORRETORA, SA	CLC com reservas por desacordo	CLC sem reservas mas com ênfases
GOLDEN ASSETS - SOCIEDADE GESTORA DE PATRIMÓNIOS, SA	Certificação Limpa	Certificação Limpa
MERCEDES-BENZ FINANCIAL SERVICES PORTUGAL - INSTITUICAO FINANCEIRA DE CREDITO, SA	Certificação Limpa	Certificação Limpa
NORGARANTE	Certificação Limpa	Certificação Limpa
OPTIMIZE INVESTIMENTO - SGPS, SA	Certificação Limpa	CLC sem reservas mas com ênfases
OREY FINANCIAL - INSTITUICAO FINANCEIRA DE CREDITO, S.A.	CLC sem reservas mas com ênfases	Certificação Limpa
PEDRO ARROJA - GESTÃO DE PATRIMÓNIOS, SA	Certificação Limpa	Certificação Limpa
PORTUCALE, SGFTC, SA	Certificação Limpa	Certificação Limpa
S. P. G. M. - SOCIEDADE DE INVESTIMENTO, SA	Certificação Limpa	Certificação Limpa
SONAEGEST - SOCIEDADE GESTORA DE FUNDOS DE INVESTIMENTO, SA	Certificação Limpa	Certificação Limpa
UNICÁMBIO - AGÊNCIA DE CÂMBIOS, SA	Certificação Limpa	Certificação Limpa

Em esquema, podemos, ainda, representar os dados nas Tabelas 4.4 e 4.5, para os anos de 2008 e 2013, respetivamente:

Table 4.4 Resultados das auditorias de 2008

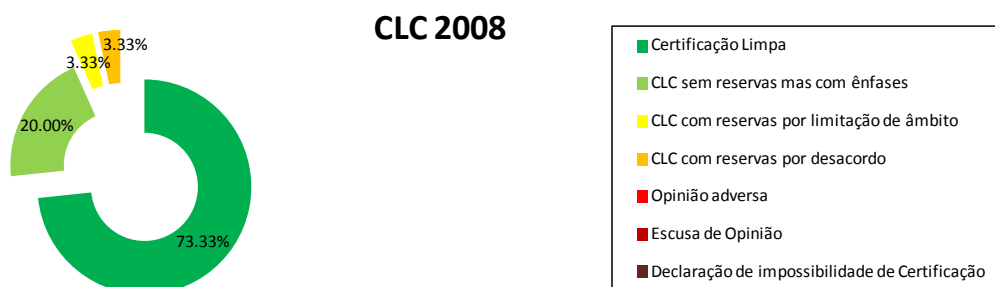
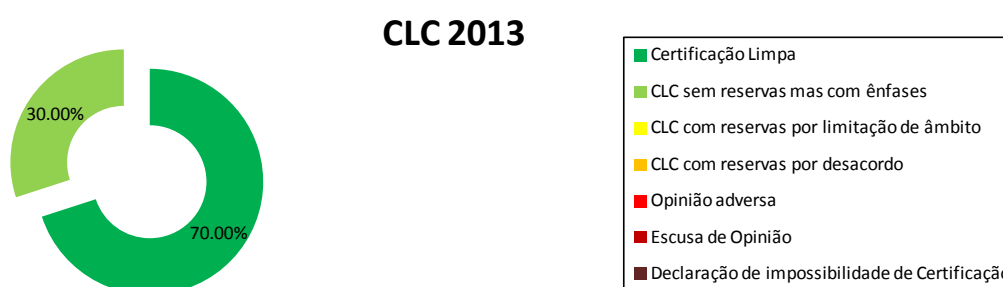


Table 4.5 Resultados das auditorias de 2013



Da leitura destas tabelas, podemos verificar que existe uma evolução nos resultados das CLC, pois em 2008, duas das entidades analisadas apresentavam CLC com reservas, situação que não se verificou em 2013. Além disso, apesar de as Certificações Limpas terem reduzido em cerca de 5%, qualitativamente, isto é, em termos de opinião não qualitativa, regista-se um aumento relativo de 7%. Para melhor nos podermos pronunciar acerca destes dados, propomos ainda uma análise das observações emitidas pelos ROC's, as quais se encontram espelhadas nas Tabelas 4.6 e 4.7, respetivamente, para os anos de 2008 e 2013.

Note-se apenas que, para esta análise, foram consideradas para 2008, no Banco BIC Português, S.A. (BIC), as contas do Banco Português de Negócios, S.A. (BPN), e no Banco BNP Paribas Personal Finance, as do Banco Cetelem S.A..

Table 4.6 Ênfases e Reservas das CLC relativas a 2008

NOME DA INSTITUIÇÃO	2008		
	MODELOS DE CLC	ÊNFASES	RESERVAS POR DESACORDO
BANCO BIC PORTUGUÊS, SA (ex-BPN, SA)	CLC com reservas por limitação de âmbito	- Não comparabilidade com exercícios anteriores - Provisões de imparidades; - Continuidade	- Impossibilidade de fazer circularização de saldos e respetivos registos contabilísticos
BANCO BNP PARIBAS PERSONAL FINANCE, SA (ex-CETEM SA)	CLC sem reservas mas com ênfases	- Provisões por imparidades	-
BANCO PRIMUS, SA	CLC sem reservas mas com ênfases	- Perda de 50% do capital (art. 35.º CSC)	-
BANCO SANTANDER TOTTA, SA	CLC sem reservas mas com ênfases	- Refere contas consolidadas em separado	-
CAIXA CENTRAL - CAIXA CENTRAL DE CREDITO AGRICOLA MUTUO, CRL	CLC sem reservas mas com ênfases	- Refere contas consolidadas em separado - Registos contabilísticos de acordo com especificidades jurídicas das CCAM	-
CAIXA ECONOMICA MONTEPIO GERAL	CLC sem reservas mas com ênfases	- Alteração de Políticas	-
FINCOR - SOCIEDADE CORRETORA, SA	CLC com reservas por desacordo	- Diminuição de resultados	- Acções com tribunais ou clientes não provisionadas - Perda de 50% do capital (art. 35.º do CSC), pondo em causa da continuidade - Impossibilidade de fazer circularização de saldos e respetivos registos contabilísticos
Orey FINANCIAL - INSTITUICAO FINANCEIRA DE CREDITO, S.A.	CLC sem reservas mas com ênfases	- Não comparabilidade com exercícios anteriores - Contabilização das participadas	-

Table 4.7 Ênfases das CLC relativas a 2013

NOME DA INSTITUIÇÃO	2013	
	MODELOS DE CLC	ÊNFASES
BANCO BIC PORTUGUÊS, SA (ex-BPN, SA)	CLC sem reservas mas com ênfases	- Remete para Anexo às DR
BANCO BILBAO VIZCAYA ARGENTARIA (PORTUGAL), SA	CLC sem reservas mas com ênfases	- Continuidade - Refere contas consolidadas em separado - Contabilização de participadas (reforço da das políticas contabilísticas aplicáveis)
BANCO ESPIRITO SANTO, SA	CLC sem reservas mas com ênfases	- Remete para Anexo às DR
BANCO L.J. CARREGOSA, SA	CLC sem reservas mas com ênfases	- Alteração de Políticas
BANCO SANTANDER TOTTA, SA	CLC sem reservas mas com ênfases	- Refere contas consolidadas em separado - Contabilização de participadas (reforço da das políticas contabilísticas aplicáveis)
BANIF - BANCO INTERNACIONAL DO FUNCHAL, SA	CLC sem reservas mas com ênfases	- Contabilização de participadas - Continuidade
CAIXA CENTRAL - CAIXA CENTRAL DE CREDITO AGRICOLA MUTUO, CRL	CLC sem reservas mas com ênfases	- Refere contas consolidadas em separado
FINCOR - SOCIEDADE CORRETORA, SA	CLC sem reservas mas com ênfases	- Registos contabilísticos
OPTIMIZE INVESTIMENTO - SGPS, SA	CLC sem reservas mas com ênfases	- Contabilização de participadas

Das causas que originaram ênfases nas CLC das entidades analisadas, podemos destacar:

- Perda de 50% do capital social, ao abrigo do artigo 35.º do Código das Sociedades Comerciais (CSC), com subsequentes aumentos de capital;
- Contabilização das participadas, ao custo de aquisição, em caso de aquisição ou fusão, ou por perdas registadas ao justo valor de uma participada para venda, no caso do Banif;
- Provisões por imparidades, por defeito ou em excesso;
- Alteração de políticas contabilísticas;
- Ressalva de registos contabilísticos com impacto em resultados;
- Não comparabilidade com exercícios anteriores, como é o caso da Orey Financeira SGPS, S.A. que incorporou a Orey Valores – Sociedade Corretora, S.A., dando origem à Orey Financeira – Instituição Financeira de Crédito, S.A. e do caso do

BPN, em 2008 (Banco BIC), quando foram corrigidas situações com impacto significativo nas Demonstrações Financeiras resultantes da investigação, no âmbito da Operação Furacão, desencadeada pelo Ministério Público;

- Continuidade da empresa, para o BPN, em 2008, para o Banif, que, em 2013, se encontrava sujeito à aprovação, por parte do Ministério das Finanças, do Plano de reestruturação atualizado do Banif – Grupo Financeiro, e para o Banco Bilbao Vizcaya Argentaria (Portugal), S.A., que, também em 2013, apresentava resultados negativos nos quatro últimos exercícios e que dependia do apoio do Banco Bilbao Vizcaya Argentaria, através de aumentos de capital e financiamento de parte das operações.

Algumas das ênfases das CLC vão apenas no sentido de alertar para a apresentação de contas consolidadas em separado³¹ e especificidades jurídicas das instituições, como é o caso da Caixa Central de Crédito Agrícola Mútuo (CCCAM) e do Banco Santander S.A., as quais se referem a registos contabilísticos efetuados em resultado da aplicação das especificidades jurídicas e das políticas contabilísticas aplicáveis para as instituições. Outras limitam-se apenas a esclarecer ou reforçar questões relativas às contas, remetendo para as notas ao Anexo e Demonstrações de Resultados. É o caso do Banco Espírito Santo, S.A. (BES), onde o revisor, na CLC de 2013, faz alusão à Nota 40 (ver Anexo I) que descreve a expectativa de reembolso de instrumentos da dívida emitidos pela Espírito Santo Internacional, S.A. (ESI) aos clientes do BES que subscreveram instrumentos da dívida desta entidade, apesar de esta ênfase ser controversa.

As reservas emitidas em 2008, para as duas instituições, tiveram origem no escândalo do BPN, em Junho desse ano, entretanto nacionalizado em 20 de Novembro de 2008, ao abrigo da Lei n.º 62-A/2008 de 11 de Novembro.

Os registos da atividade operacional da Fincor – Sociedade Corretora, S.A., enquanto entidade do grupo BPN, eram desenvolvidos nos sistemas operacionais deste. Com a nacionalização do BPN e conseqüente saída do grupo, os impactos desta situação na continuidade da Fincor ainda não haviam sido apurados, à data de 31/12/2008. Adicionalmente, a esta data, o capital social desta instituição encontrava-se perdido em 50%, pelo que o ROC recomendava a adoção de uma das medidas previstas no já referido

³¹ A CCCAM, que apresenta a consolidação das contas individuais das CCAM

artigo 35.º do Código das Sociedades Comerciais (CSC), entre as quais, redução ou aumento de capital e/ ou dissolução da sociedade. Deste modo, o ROC considerava que o princípio da continuidade que havia estado na base da elaboração das Demonstrações Financeiras, não estava salvaguardado. Existiam ainda faturas não registadas pelo facto de a Administração não estar de acordo com as mesmas. Estas situações foram integradas na CLC como reservas, no entanto, o ROC chama ainda a atenção, numa ênfase, para uma diminuição do negócio da instituição e ao conseqüente decréscimo nos resultados face a 2007.

Em 2013, a Fincor já havia reconfigurado o seu sistema operativo, existindo ainda um projeto em curso para otimização dos sistemas de informação. Os procedimentos de conciliação bancária necessitavam ainda de melhorias, mantendo-se ainda um elevado número de operações por reconciliar, bem como a confirmação de saldos de clientes. A situação descrita integra as ênfases da CLC da entidade.

A CLC emitida pela Deloitte & Associados, SROC S.A., às contas do BPN de 31/12/2008 (posterior à nacionalização), inclui uma reserva por limitação de âmbito. O ROC reconhece a incapacidade de se pronunciar sobre a existência de responsabilidades ou passivos do Banco, na medida em que não obteve resposta ao pedido de confirmação de saldos por parte de um número significativo de advogados ou entidades relacionadas. Do mesmo modo, não foi possível fazer a confirmação de saldos de clientes relativos a títulos depositados, não se podendo pronunciar sobre a razoabilidade dos montantes registados. Recorde-se que, um dos esquemas fraudulentos do BPN que envolvia clientes, consistia na captação de fundos para depósitos, sob a forma de aplicações em títulos, com perspectiva de elevadas rentabilidades, fundos esses que eram encaminhados para *offshores* em nome dos titulares desses fundos, sem o seu conhecimento. É de notar que, deste esquema, perdeu-se o rasto a milhões de euros.

As ênfases efetuadas diziam respeito a imparidades e provisões para crédito concedido efetuadas durante o ano de 2008 e que levaram à apresentação, em anexo, das contas de 2007 refeitas, fazendo ainda referência ao facto de a continuidade da instituição se encontrar dependente do sucesso do plano de viabilização que se encontrava em aprovação.

A ênfase do BIC, relativa às contas de 2013, refere-se, ainda, ao acordo assinado com o Estado português, em 2011, para aquisição do capital social do BPN, cuja operação só se

concretizou em Março de 2012, remetendo para as demonstrações financeiras os impactos relativos ao referido acordo.

Após fazer a recolha dos dados e análise dos dados, passaremos então às conclusões dos mesmos.

4.5 – Resultados e conclusões

Os resultados obtidos da análise dos modelos de CLC emitidos para os anos de 2008 e 2013 registam um aumento relativo de 10% nas Certificações Limpas emitidas. Com estes dados, poderíamos avançar com uma conclusão otimista sobre o nosso estudo. Analisando os números, numa perspetiva simplista, para o caso das instituições financeiras, admitindo que estas se encontram a cumprir a exigência do Banco de Portugal no que concerne à adoção de um sistema de controlo interno que obedeça aos princípios e requisitos mínimos do Aviso n.º 5/2008, o qual segue os conceitos definidos pelo COSO, poderíamos afirmar que a utilização de modelos de gestão de riscos, tem um impacto positivo no resultado das auditorias.

Todavia, esta questão é um pouco mais complexa e merece uma maior reflexão. Em Julho deste ano, rebenta um novo escândalo no sistema financeiro português. A Espírito Santo Financial Group (ESFG), a *holding* através da qual a família Espírito Santo controlava o BES, com sede no Luxemburgo (ver Anexo II), apresentou o pedido de gestão controlada e, na sequência deste, proteção contra credores. O Tribunal do Luxemburgo recusou o pedido, tendo esta, em Outubro declarado insolvência. Na base do processo, estavam triangulações entre o Banco e empresas do grupo, a existência de operações com veículos sedeados em zonas *off-shore*, entre outras situações.

A questão que se coloca é, como é que todas as transações e riscos passaram ao lado dos auditores externos, já que estes, de acordo com a ISA 550, devem rever as operações com as partes relacionadas, bem como o cumprimento dos requisitos a que estas instituições estão obrigadas pelo Banco de Portugal, nomeadamente, relativamente ao *Governance*. O facto é que, esta situação não terá passado despercebida, pelo menos, não na totalidade.

Segundo Lourenço (2014), em 2002, a Pwc era a sociedade encarregue de fazer auditorias ao BES (e ao grupo). Em resultado de alterações regulamentares que se faziam sentir na época, um *partner* da mesma sociedade de auditoria, de Londres, veio analisar as contas do

Banco. Tendo verificado situações pouco claras, de entre as quais, a existência de operações com *off-shores*, pediu esclarecimentos. O Banco ficou de regularizar as situações pendentes, no entanto, isso não impediu a revogação do contrato de prestação de serviços de auditoria, por parte da Pwc. Uma outra empresa de auditoria também terá recusado substituir a Pwc, alegadamente pelos mesmos motivos (ibid.1).

A KPMG, enquanto sociedade responsável pela emissão do relatório de auditor externo e pela CLC³², emitiu, em 2012, uma Certificação Limpa, e, em 2013, uma CLC sem reservas mas com a ênfase já referida acima (ver Anexo I) aquando do tratamento do conteúdo das certificações das instituições analisadas. Esta ênfase fazia referência a uma situação patrimonial grave detetada na ESI, a *holding* que integrava os ramos financeiro e não financeiro do Grupo Espírito Santo (GBES), em Novembro de 2013, no decurso de exercícios transversais realizados pelo Banco de Portugal com recurso a auditores externos independentes. A situação patrimonial reportada era derivada de um acréscimo significativo do passivo financeiro da ESI, todavia, não era suficiente para antecipar os acontecimentos recentes.

Em acréscimo, num comunicado do Banco de Portugal que visava fornecer esclarecimentos relacionados com a situação do BES - Compilação de esclarecimentos prestados relacionados com a situação do Banco Espírito Santo -, datado de 25 de Julho, este vem clarificar que a supervisão em base consolidada do Grupo BES, era efetuada através da ESFG, ao abrigo dos artigos 131.º e 132.º do RGICSF, o qual determina que a supervisão deve incidir sobre a situação financeira da empresa-mãe, ainda que esta tenha sede noutro estado-membro da União Europeia (U.E.) e que, sendo esta uma companhia financeira, ficam as filiais e instituições de crédito com sede em diferentes estados-membros, sujeitas à supervisão exercida pela autoridade de supervisão que autorizou a instituição de crédito cujo total do balanço seja mais elevado. Esta situação deixou de se verificar a partir de 30 de Junho, altura em que o BES deixou de se qualificar como filial da ESFG, fruto da redução da participação desta última e das alterações de *Governance* daí resultantes. No que diz respeito às entidades do ramo não financeiro do grupo, descarta ainda a responsabilidade da supervisão das mesmas, uma vez que, estas «não integram o

³² O ROC é responsável pela revisão legal de contas, a qual consiste no exame das contas com vista à sua CLC, bem como pelo exercício de quaisquer outras funções de interesse público que a lei lhes atribua, enquanto o artigo 245.º do Código dos Valores Mobiliários, obriga à apresentação de um relatório de auditoria, a ser efetuado por auditor registado na CMVM, instituindo a figura do auditor externo para a realização de trabalhos de auditoria e outros relacionados com o mercado de capitais

perímetro prudencial do grupo bancário sujeito à supervisão do Banco de Portugal na medida em que não são consideradas empresas-mãe ou filiais de instituição de crédito» (2014: p.5). Refere ainda que, o exercício de supervisão prudencial com base nas demonstrações financeiras consolidadas «permite obter informação completa sobre o conjunto das atividades e resultados das empresas que integram o grupo e fornece uma visão global dos riscos assumidos pelo grupo» (ibid.: 1: p.6), com vista a assegurar um equilíbrio entre o perfil de risco, o capital e liquidez do grupo.

Quanto às participações em empresas do grupo, apesar de a aquisição de entidades não-financeiras, por parte das instituições de crédito, não carecerem de autorização prévia do Banco de Portugal, estas estão sujeitas ao cumprimento dos artigos 100.º e 101.º do RGICSF, pelo que não podem deter uma participação cujo montante ultrapasse 15% dos seus fundos próprios e o montante global em participadas não pode exceder os 60%, nem deter, direta ou indiretamente, numa sociedade, por prazo seguido ou interpolado, superior a três anos, uma participação que lhes confira mais de 25% dos direitos de voto, correspondentes ao capital da sociedade participada³³.

As operações realizadas entre grupos bancários supervisionados e entidades do ramo não financeiro estão sujeitas ao cumprimento dos requisitos relativos a concentração de riscos, à avaliação de risco de crédito e do risco reputacional. No caso do BES, a ESFG estava isenta de limites de grandes riscos e, como tal, o Grupo BES também se encontrava isento. Quanto à avaliação da idoneidade de *Governance* do Banco de Portugal, esta baseia-se em factos a que tenham acesso e informação relevante que lhe seja disponibilizada. Em resultado dos factos desencadeados, o Presidente do Grupo está na iminência de ser inibido de exercer funções na Banca, a família perdeu os direitos de voto no grupo e foram suspensos três administradores.

Contudo, esta situação não é inédita. Nos últimos 7 anos, tem-se verificado outros casos de fraude, com impacto negativo na credibilidade do trabalho realizado pelos auditores.

Aquando do já referido caso BPN, Freches, Lima e Antunes (2012), afirmam que os relatórios das inspeções do Banco de Portugal realizadas nos anos de 2002, 2005 e 2007, revelavam deficiências que poderiam ter servido de alerta, uma vez que ficaram por esclarecer situações que já preconizavam indícios de fraude. Com efeito, estes reportavam

³³ Relativamente às participações indiretas detidas através de sociedades de capital de risco e de sociedades gestoras de participações sociais, o prazo é de 5 anos

já a recusa de respostas a questões efetuadas, a existência de uma excessiva exposição de crédito imobiliário e de processos de crédito sem garantias, o recurso a *Excellence Asset Funds* para cobrir riscos de crédito, inexistência de restrições à concessão de créditos, o que contrariava o acordo Basileia, a sobrevalorização de resultados consolidados, bem como várias deficiências de controlo interno, nomeadamente no que concerne às transações entre as empresas de grupo. Apesar do conteúdo dos relatórios, ficaram por tomar as respetivas medidas que os factos exigiam, ao abrigo da legislação vigente à data no RGICSF. As irregularidades detetadas, por si só, seriam suficientes para instaurar processos de contraordenação e para a nomeação de administradores provisórios, bem como para requerer uma auditoria externa.

No que diz respeito aos relatórios de auditoria, o relatório final da Assembleia da República (2009) refere que entre 1998 e 2003 o BPN foi auditado por quatro empresas. Nos relatórios de contas dos exercícios dos anos de 1999, 2000, 2001, 2002 e 2003, foram consideradas reservas e ênfases pelo fiscal único e pelo ROC, relativamente às empresas do grupo, nomeadamente, por inexistência, insuficiência e contabilização incorreta de provisões para recuperação de crédito, incumprimento dos créditos securitizados e cobertura de riscos, bem como riscos de concentração do crédito imobiliário.

Em 2003, houve uma mudança do auditor externo, passando estas auditorias a serem realizadas pela BDO Binder & CO., que no seu relatório afirmava que as questões subjacentes às reservas evidenciadas haviam sido ultrapassadas durante o exercício. Só em 2007 é que as contas individuais do Banco haviam sido objeto de reservas.

O CNSA levou a cabo ações inspetivas para apurar eventuais falhas ou irregularidades dos auditores e dos ROC's. Também o Banco de Portugal questionou a BDO. Ao ROC da instituição, a sociedade J. Monteiro & Associados, foi deduzida acusação por factos ocorridos entre 2000 e 2006. Foi decidido o cancelamento do registo de dois ROC's desta última, de entre os quais, um sócio gerente, por alegada falta de idoneidade, violação de um conjunto de comportamentos e normas, como a independência, a objetividade e a isenção. O CNSA considerou que os ROC's não haviam adotado os procedimentos adequados e não denunciaram factos que comprometiam a veracidade e adequabilidade das demonstrações financeiras.

Quanto ao BCP, em 2008, um acionista fez uma denúncia ao Banco de Portugal e à CMVM por suspeita de atos de gestão ilícitos e gestão danosa, de entre os quais, falsificação de documentos, perdão de créditos a acionistas, em particular os que se

destinavam à compra de ações do próprio Banco, bem como a concessão de créditos a familiares de administradores. Estes factos remontam ao período compreendido entre 1999 e 2007 e incluem a utilização de *off-shores* na compra de ações do BCP, por via de financiamento do próprio Banco, de modo a influenciar os valores de mercado e o *rating* das ações do BCP. O BCP ocultou estas entidades *off-shore* nas suas contas, no entanto, o Banco de Portugal tinha conhecimento das mesmas, já que estas se encontravam registadas em nome de um acionista do Banco. Durante 7 anos, as contas do BCP encontravam-se falseadas, apresentando resultados manipulados e cotação de títulos emolpadas, com vista à obtenção de elevadas remunerações, por parte dos seus administradores.

A supervisão durante esse período não detetou erros, omissões ou fraudes contra o mercado.

A KPMG, SROC responsável pela emissão da CLC e do relatório de auditoria externa a que a CMVM obriga, atestou as contas da instituição, não tendo apurado quaisquer irregularidades nas mesmas. É de notar que, o administrador António Rodrigues já havia passado pela KPMG, ao longo da sua vida profissional.

No caso do BPP, que veio à tona em 2009, três administradores terão falsificado registos contabilísticos e ocultado «responsabilidades assumidas perante clientes» (Caneco, 2014) que ascendiam a 450 milhões de euros, entre 2006 e 2008, com o intuito de ludibriar o Banco de Portugal e manterem os cargos que ocupavam, aparentando que a instituição tinha um bom *Governance* (ibid.:1). Lesaram, ainda, em mais de 40 milhões de euros, 100 clientes da Privado Holding, a *holding* que funcionava como veículo de investimento do Banco.

Para além dos crimes fiscais e de branqueamento de capitais, os administradores do BPP, foram acusados de crimes de falsidade informática, falsificação de documentos, violação de normas contabilísticas e ocultação de informações que terão posto em causa a veracidade da posição financeira da empresa apresentada nos relatórios de contas e demonstrações financeiras. Em suma, as irregularidades financeiras nas contas do BPP consistiam em falta de provisões, insuficiência de capital e existência de contratos de retorno absoluto.

Também para o caso do BPP, o CNSA levantou uma ação inspetiva, no sentido de perceber se a Deloitte, a SROC que exercia cumulativamente as funções de auditor e revisor do Banco desde a sua fundação, tinha como identificar as irregularidades existentes

e estaria a ser conivente com a situação, ou se, pelo contrário, desconhecia efetivamente as mesmas. Não foi reconhecida a responsabilidade dos auditores, até à data.

Do que aqui acabámos de relatar, podemos concluir que, não obstante os modelos de gestão de risco permitirem obter um sistema de controlo interno efetivo e de fornecerem à Gestão uma segurança razoável de que os riscos inerentes ao negócio serão contornados e os seus objetivos atingidos, estes por si só, só funcionam em pleno se os objetivos pessoais dos gestores de topo se enquadrarem com os interesses da entidade. Para tal, assume-se que os gestores são profissionais idóneos, íntegros e capacitados para o exercício das suas funções e que a sua única finalidade é gerir as entidades em que trabalham com competência.

Estes modelos, não só não evitam erros de má gestão, como oferecem limitações quando consideramos a capacidade da Gestão ultrapassar os controlos existentes, em benefício próprio, e a existência de conluíus ao longo das organizações.

Foi o que aconteceu nos casos acima descritos em que se verificou ter havido, claramente, má conduta dos membros que integram o *Governance* das referidas entidades, com o intuito de obter vantagens pessoais, os quais conduziram estas entidades a situações financeiras graves, com impactos significativos no sistema bancário português, bem como na economia e finanças do país.

Por outro lado, estas situações não tendo sido detetadas pelas auditorias fazem-nos questionar o facto de as mesmas SROC's exercerem funções de ROC e de auditor externo, em simultâneo, pondo em causa a qualidade e objetividade dos trabalhos dos auditores. Mais grave ainda é que, muitas vezes, estas SROC's fazem auditorias a várias empresas do mesmo grupo com vista à emissão das respetivas CLC e relatórios de auditoria em base consolidada. Em resultado, os honorários que usufruem são substancialmente altos e, naturalmente, as SROC's tornam-se mais permissivas para não perderem esses clientes. Este facto traz à discussão temas como a independência, idoneidade e integridade, bem como a competência do auditor. A separação destas duas funções obrigaria ambos (revisor e auditor) a serem mais profissionais e diligentes no seu trabalho, contribuindo para a qualidade das auditorias.

Outra questão, que não pode ser de todo descurada, é o facto de estes auditores terem necessidades de formação contínua, face às alterações regulamentares permanentes que o setor bancário tem vindo a sofrer. O auditor / revisor deve possuir um conhecimento

profundo da atividade bancária, da sua complexidade, especificidades e requisitos legais a que o negócio e as instituições devem obedecer.

4.5.1 – Limitações

A revisão da literatura, que serviu como ponto de partida a este estudo, foi, no que concerne às instituições financeiras, maioritariamente fundamentada em normativos legais. Talvez por este ser um tema que ainda está em desenvolvimento, dadas as ações regulamentares em curso, a bibliografia que existe sobre o controlo interno neste tipo de organizações é escassa.

O caso empírico ficou aquém do que se ambicionava. De início foi complicado encontrar um universo, uma vez que não existe uma lista de todas as entidades que possa facilmente ser extraída. No *site* do Banco de Portugal, na seção “Instituições Autorizadas”, foi efetuado um filtro por tipo de instituição, considerando as que estavam no âmbito do nosso estudo, e procedeu-se à contagem das mesmas, manualmente. Apesar de todo o cuidado, esta contagem é suscetível de conter erros.

Teria sido interessante se pudéssemos ter tido acesso aos relatórios de controlo interno a que o artigo 25.º do Aviso n.º 5/2008 do Banco de Portugal se refere, porém, tal não foi possível, pois os mesmos não estão publicados nos *sites* públicos, nem da CMVM, nem do Banco de Portugal, já que não se encontram obrigados à sua divulgação, ao abrigo do artigo 144.º da Diretiva 2006/48/CE, transposto para o artigo 93.º- A do RGICSF. Por outro lado, os resultados das inspeções *on-site* também não estavam disponíveis para consulta no respetivo *site*, nem tão pouco o das avaliações de riscos do MAR. Assim, foi de todo impossível ampliar a nossa análise e contrabalançar os resultados obtidos com as ações previstas pelo Banco de Portugal, no âmbito das funções de supervisão prudencial que lhe conferem.

Contactado o Banco de Portugal, via telefone e *e-mail*, no sentido de obter a informação referida, não houve respostas.

5. Conclusão

É um facto que o controlo interno é, cada vez mais, um tema que merece a atenção de todos os agentes de mercado. O uso dos modelos de gestão de risco vem responder às exigências dos diversos *stakeholders*, tornando-se uma ferramenta de uso generalizado e aceite quer por parte dos auditores, na medida em que lhes permitem obter um maior rigor e uma maior qualidade na realização do seu trabalho, quer por parte da gestão, não só por servirem de suporte à tomada de decisão, minimizando os riscos, mas também por conferirem maior qualidade e transparência à informação financeira, reforçando a imagem da organização e captando o interesse dos investidores.

Com o aumento da concorrência, regulação e globalização dos mercados, também na atividade bancária se tem vindo a verificar transformações. Estes desafios aumentam a importância da gestão do risco efetivo na distribuição de resultados e nos processos de *Governance* e *compliance*. A administração das instituições, o controlo interno e a supervisão das instituições financeiras passam a estar centrados numa perspetiva de avaliação do perfil de risco com um fim preventivo.

Considerando que as instituições tinham um plano estratégico e, como tal, necessidade de gerir riscos, e que estas deveriam ter uma estrutura de *Governance* clara e ajustada à dimensão e complexidade do negócio, encontravam-se reunidas as condições para a implementação de um sistema de controlo interno que fosse aplicável às instituições financeiras. O Aviso n.º 5/2008 do Banco de Portugal, não é mais do que a sistematização de riscos comuns, integrando todos os envolvidos no controlo interno. Através das orientações aqui decretadas, as instituições poderão criar um bom ambiente de controlo e a gestão e o controlo das operações passam a ser efetuados adequadamente e de forma prudente.

A Diretriz de Revisão / Auditoria, DRA 860, orienta o auditor no sentido de dar cumprimento às suas responsabilidades quanto à emissão dos pareceres sobre a adequação e a eficácia da parte do sistema de controlo interno subjacente ao processo de preparação e de divulgação de informação financeira, conforme previsto no n.º 5 do artigo 25.º do referido aviso. Contudo, na sequência dos últimos acontecimentos em Portugal, protagonizados pelo BES, existe uma forte possibilidade de que esta venha a ser revista e venham a ser introduzidas mudanças na verificação dos requisitos relativos à independência, integridade, competência, assim como de formação contínua, resultantes da necessidade de atualização permanente por parte destes profissionais face às alterações

regulamentares sucessivas que se têm vindo a verificar neste setor, e que se adivinha não ficarem por aqui.

Por outro lado, estes escândalos financeiros aliados à revisão do *Framework* de controlo interno do COSO, em 2013, aos princípios de boas práticas emanadas pelo *Basel Committee* em 2011, à expectativa existente de que os Bancos melhorem continuamente a sua abordagem ao risco operacional e às orientações relativas a *Internal Governance* publicadas pelo EBA, em substituição das anteriormente emitidas pelo CEBS, têm decretado a necessidade de se ir revendo o controlo interno nas instituições financeiras, pelo que se espera uma revisão do Aviso n.º5 que incorpore estas atualizações, assim como outros requisitos que os reguladores e supervisores julguem ser determinantes para a evolução do controlo interno. Uma revisão deste aviso, no entanto, estará sempre relacionada com a evolução dos mercados financeiros e com os resultados que a regulação atual venha a atingir, em termos de controlo interno. Neste contexto, caso a legislação em vigor se venha a revelar insuficiente ou desajustada, o Banco de Portugal poderá vir a emitir novas medidas, fazer mais exigências e impor restrições.

Referências Bibliográficas

- ALVES, Ana do Carmo Miranda Raposo – **A Evolução da Auditoria Interna após a Lei SOX: Impactos indiretos no caso português**, Tese de mestrado, 2009, Instituto Superior de Contabilidade e Administração da Universidade de Aveiro [em linha] [Consult. 9 Jun. 2014]. Disponível em URL: <http://oatd.org/oatd/record?record=handle%5C:10773%5C%2F3261>
- ARENS, Alvin A., ELDER, Randal J., BEASLEY, Mark S. - **Auditing and Assurance Services: an integrated approach**. 15th Edition, Pearson Education, Inc., 2013, ISBN 978-0-13-312563-4
- ASSEMBLEIA da Republica- **Comissão de Inquérito sobre a situação que levou à nacionalização do BPN e sobre a supervisão bancária inerente**. Lisboa, 2009 [Em linha]. [Consult. 15 Dezembro. 2014]. Disponível em: http://www.dn.pt/DNMultimedia/DOCS+PDFS/BPN/RelatorioBPN_final.pdf
- Aviso do Banco de Portugal n.º 3/2006, de 9 de Maio, [em linha] [Consult. 14 Mai. 2014]. Disponível em URL: <http://www.bportugal.pt/sibap/application/app1/docs1/avisos/textos/3-2006a.pdf>
- Aviso do Banco de Portugal n.º 4/2006, de 8 de Agosto, [em linha] [Consult. 10 Dez. 2014]. Disponível em URL: <http://www.bportugal.pt/sibap/application/app1/docs1/avisos/textos/4-2006a.pdf>
- Aviso do Banco de Portugal n.º 5/2008, de 25 de Junho, [em linha] [Consult. 14 Mai. 2014]. Disponível em URL: <http://www.bportugal.pt/sibap/application/app1/docs1/avisos/textos/5-2008a.pdf>
- Aviso do Banco de Portugal n.º 6/2003, de 15 de Janeiro, [em linha] [Consult. 26 Dez. 2014]. Disponível em URL: <http://www.bportugal.pt/sibap/application/app1/docs1/avisos/textos/6-2003a-c.pdf>
- AZEVEDO, Mário – **Teses, relatórios e trabalhos escolares: sugestões para estruturação de escrita**. 7ª Edição, Lisboa: Universidade Católica Editora, 2009. ISBN 978-972-54-0247-4
- Banco de Portugal [em linha] [Consult. 17 Mai. 2014]. Disponível em URL: <http://www.bportugal.pt/pt-PT/Supervisao/Paginas/default.aspx>
- Banco de Portugal, **XIII Conferência sobre Auditoria, Risco e Governance (2014)**, Banco de Portugal. [em linha] [Consult. 28 Out. 2014]. Disponível em URL: <http://www.bportugal.pt/pt-PT/OBancoeoEurosistema/Eventos/Paginas/XIIIConferenciaAuditoria.aspx>
- Banco de Portugal, **Modelo de Avaliação de Riscos (2007)**, [em linha] [Consult. 10 Set. 2014]. Disponível em URL: https://www.bportugal.pt/pt-PT/OBancoeoEurosistema/ConsultasPublicas/Documents/Consulta_BP

- Banco de Portugal, **Compilação de esclarecimentos prestados relacionados com a situação do Banco Espírito Santo**, [em linha]. (25 Jul. 2014) [Consult. 23 Dez. 2014]. Disponível em URL: http://www.bportugal.pt/pt-PT/OBancoeoEurosistema/Esclarecimentospublicos/Documents/Compilacao_esclarecimentos_sobre_o_BES.pdf
- BARAÑANO, Ana Maria – **Métodos e Técnicas de Investigação em Gestão**. 1.ª Edição, Lisboa: Edições Sílabo, 2004. ISBN 972-618-312-X
- Basel Committee on Banking Supervision - **Framework for Internal Control Systems in Banking Organisations**. [em linha]. [Consult. 2 Jun. 2014]. Disponível em URL: <http://www.bis.org/publ/bcbs40.pdf>
- Basel Committee on Banking Supervision - **Principals for the Sound management of Operational Risk and the Role Supervision**. [em linha] [Consult. 4 Jun. 2014]. Disponível em URL: http://www.nbb.be/doc/cp/nl/bo/circ/pdf/NBB_2011_05NL_annexe.pdf
- Basel Committee on Banking Supervision - **Sound practices for the management and supervision of Operational Risk**. [em linha] [Consult. 4 Jun. 2014]. Disponível em URL: <http://www.bis.org/publ/bcbs96.pdf>
- BEJA, Rui, **Risk Management - Gestão, Relato e Auditoria dos Riscos de Negócio**. Lisboa: Áreas Editora, 2004, ISBN 972-8482-69-2
- BELL, Judith - **Como realizar um projecto de investigação: Um guia para a pesquisa em Ciências Sociais e da Educação**. Lisboa: Gradiva, 1997. ISBN 972-23-1290-1.
- CÂMARA, Paulo, MAGALHÃES, Manuel - **O Novo Direito Bancário**. Editora Almedina, 2012. ISBN 978- 972-403-855-1
- Código das Sociedades Comerciais, 3.ª Edição, Lisboa: Almedina, 2012. ISBN 978-972-40-4862-8
- Comissão de Mercados de Valores Mobiliários, [em linha] [Consult. 24 Mai. 2014]. Disponível em URL: <http://www.cmvv.pt/>
- Committee of European Banking Supervisors - **Guidelines on the Application of the Supervisory Review Process under Pillar II**. [em linha] [Consult. 24 Mai. 2014]. Disponível em URL: <https://www.eba.europa.eu/documents/10180/16094/GL03.pdf/9705f895-fbfa-4e39-bac9-3def3127f545>
- Committee of Sponsoring Organizations of the Treadway Commission - **Internal control – Integrated framework (1992)**
- Committee of Sponsoring Organizations of the Treadway Commission. **Internal control – Integrated framework (2013)**, [em linha] [Consult. 10 Dez. 2014]. Disponível em URL: http://coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

- Committee of Sponsoring Organizations of the Treadway Commission, **Enterprise Risk Management – Integrated Framework – Application Techniques** (2004), [em linha] [Consult. 24 Set. 2014]. Disponível em URL: <http://www.coso.org/-ERM.htm>
- CORDEIRO, A. MENEZES - **Manual de Direito Bancário**. 4.^a ed., Almedina, Coimbra, 2010, ISBN 9789724040806
- CORREIO da Manhã – **Accionista do BCP denuncia 23 casos suspeitos**. [em linha]. (6 Jan. 2008) [Consult. 24 Set. 2014]. Disponível em URL: <http://www.cmjornal.xlpt/nacional/economia/detalhe/accionista-do-bcp-denuncia-23-casos-suspeitos.html>
- COSTA, Carlos Baptista da - **Auditoria Financeira – Teoria & Prática**. 9^a Edição: Rei dos Livros, 2010. ISBN 978-989-8305-11-4.
- COUTINHO, Clara Pereira - **Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática**. Almedina, 2013, ISBN 978-972-405-137-6
- CROUHY, Michel; GALAI, Dan; MARK, Robert – **The Essentials of Risk Management**. McGraw-Hill Companies, Inc., 2006. ISBN 0-07-142966-2
- D'OLIVEIRA, Teresa – **Teses e Dissertações: recomendações para a elaboração e estrutura de trabalhos científicos**. Editora RH, 1.^a Edição, Lisboa, 2002. ISBN 972-98823-2-0
- Decreto-Lei n.º 103/2007, 3 de Abril. [em linha] [Consult. 1 Dez. 2014]. Disponível em URL: <http://www.bportugal.pt/pt-PT/Legislacaoenormas/Documents/DL103ano2007.pdf>
- Decreto-Lei n.º 104/2007, de 3 de Abril. [em linha] [Consult. 1 Dez. 2014]. Disponível em URL: <http://www.bportugal.pt/pt-PT/Legislacaoenormas/Documents/DL104ano2007.pdf>
- Diretiva 2006/48/CE do Parlamento Europeu e do Conselho, de 14 de Junho de 2006, [em linha] [Consult. 1 Dez. 2014]. Disponível em URL: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0048&from=PT>
- Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, [em linha] [Consult. 28 Dez. 2014]. Disponível em URL: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32013L0036>
- Diretriz de Revisão/Auditoria 700. [em linha] [Consult. 28 Dez. 2014]. Disponível em URL: <http://www.infocontab.com.pt/download/dra/dra700.pdf>
- Diretriz de Revisão/Auditoria 860. [em linha] [Consult. 28 Dez. 2014]. Disponível em URL: <http://www.infocontab.com.pt/download/DRA/DRA860.pdf>

European Banking Authority - **Guidelines on the assessment of the suitability of members of the management body and key function holders**. [em linha] [Consult. 2 Dez. 2014]. Disponível em URL: <https://www.eba.europa.eu/documents/10180/106695/EBA-GL-2012-06--Guidelines-on-the-assessment-of-the-suitability-of-f-persons-.pdf>

European Banking Authority – **EBA Guidelines on the Internal Governance (GL 44)**. [em linha] [Consult. 2 Dez. 2014]. Disponível em URL: [https://www.eba.europa.eu/documents/10180/103861/EBA-BS-2011-116-final-EBA-Guidelines-on-Internal-Governance-\(2\)_1.pdf](https://www.eba.europa.eu/documents/10180/103861/EBA-BS-2011-116-final-EBA-Guidelines-on-Internal-Governance-(2)_1.pdf)

FRECHES, Sílvia; LIMA, Rodrigues Carlos; ANTUNES, Rui Pedro; SIMÕES, Sónia – **O Escândalo do BPN**. Diário de Notícias, Gradiva, 2012. ISBN 978-989-616-484-3

FREIXO, Manuel João Vaz – **Metodologia Científica: Fundamentos, Métodos e Técnicas**. 3.^a Edição, Lisboa: Instituto Piaget, 2011, ISBN 972-98823-2-0

LOUÇÃ, Francisco – Relatório acerca do caso BCP. Grupo Parlamentar Bloco de Esquerda. , [em linha] [Consult. 29 Dez. 2014]. Disponível em URL: http://www.esquerda.net/sites/default/files/relatorio_bcp_0.pdf

International Federation of Accountants, [em linha] [Consult. 24 Mai. 2014]. Disponível em URL: <http://www.ifac.org/auditing-assurance/about-iaasb>

INSTITUTO PORTUGUÊS DE *CORPORATE GOVERNANCE* - **Código de Governo das Sociedades** (2014)

IT Governance Institute - **COBIT 4.1 Framework, Control Objectives, Management Guidelines** -, Maturity Models - 2007, USA, ISBN 1-933284-72-2

ISACA - **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**. [em linha] [Consult. 10 Out. 2014]. Disponível em URL: www.isaca.org/cobit

CANECO, Sílvia – **BPP: Rendeiro acusado de falsear contabilidade para não ficar sem cargo**. Jornal i, [em linha] (28 Jun.2014) [Consult. 10 Out. 2014]. Disponível em URL: <http://www.ionline.pt/artigos/dinheiro/bpp-rendeiro-acusado-falsificar-contabilidade-nao-ficar-sem-cargo>

Lei 46/2014, de 26 de Julho, [em linha] [Consult. 28 Dez. 2014]. Disponível em URL: <https://dre.pt/application/conteudo/55021030>

Lei Orgânica nº 5/98 de 31 de Janeiro, [em linha] [Consult. 26 Dez. 2014]. Disponível em URL: <https://www.bportugal.pt/pt-PT/Legislacaoenormas/Documents/Lei5ano98.pdf>

LOURENÇO, Camilo – **Irresponsáveis**. 1.^a Edição, Lisboa: Matéria-Prima Edições, 2014. ISBN 978-989-769-001-3

MOELLER, Robert R. - **Brink's Modern Internal Auditing** -, John Wiley & Sons, 6th Edition, New Jersey, 2005. ISBN 0-471-67788-4

- MOELLER, Robert R. - **COSO enterprise risk management: establishing effective Governance, risk, and compliance processes.** 2nd Edition, New Jersey: John Wiley & Sons, 2011. ISBN 978-0-470-91288-1
- MOELLER, Robert R. - **Sarbanes-Oxley internal controls: effective auditing with AS5, Cobit and ITIL.** New Jersey: John Wiley & Sons, 2008. ISBN 978-0-470-17092-2
- MORAIS, Georgina, MARTINS, Isabel - **Auditoria Interna – Função e Processo.** Lisboa: Áreas Editora, 2013. ISBN 978-989-8058-81-2
- OLIVEIRA, José - **Modelo Integrado para uma Gestão Eficiente e Controlo do Risco.** Porto: Vida Económica, Editorial, 2011. ISBN 978-972-788-431-5
- PICKETT, K. H. Spencer - **Auditing the risk management process.** John Wiley & Sons, Inc. New Jersey, 2005, ISBN 978-0-471-69053-5
- PICKETT, K. H. Spencer - **The Essential Guide to Internal Auditing.** John Wiley & Sons, Inc. New Jersey, 2011, ISBN 978-0-470-74693-6
- PIRES, Ana Isabel Marinho – **Impacto da Lei Sarbanes-Oxley no Sistema do Controlo Interno das Empresas cotadas nos EUA – O Caso Português.** [Em linha]. (2008) [Consult. 10 Dez. 2014]. Disponível em: https://repositorioaberto.uab.pt/bitstream/10400.2/586/1/TMCA_AnaPires.pdf
- Public Company Accounting Oversight Board, [em linha] [Consult. 10 Mar. 2014]. Disponível em URL: <http://pcaobus.org/About/Pages/default.aspx/>
- Regime Geral das Instituições de Crédito e Sociedades Financeiras. [em linha] [Consult. 07 Mai. 2014]. Disponível em URL: <https://www.bportugal.pt/pt-PT/Legislacaoenormas/Documents/RegimeGeral.pdf>
- Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de Junho. [em linha] [Consult. 12 Dez. 2014]. Disponível em URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0001:0337:PT:PDF>
- RITTENBERG, Larry E.; JOHNSTONE, Karla M.; GRAMLING, Audrey A. - **Auditing: A Risk-Based Approach to Conducting a Quality Audit.** 9th Edition, South-Western: Cengage Learning. ISBN-13: 978-1-133-93915-3
- RITTENBERG, Larry E.; JOHNSTONE, Karla M.; GRAMLING, Audrey A. - **Auditing: A Business Risk Approach.** 7th Edition, South-Western: Cengage Learning, 2010. ISBN-13: 978-0-324-65804-4
- SANTOS, Rui Almeida – **Sistema de Controlo Interno das Instituições Financeiras: uma nova filosofia de supervisão.** InforBANCA 83 (2010) 12-14
- A Adopção das Normas Internacionais de Auditoria da IFAC – Revisores e Auditores (Jan-Mar 2009) [em linha] [Consult. 10 Out. 2014]. Disponível em URL: <http://www.oroc.pt/fotos/editor2/Revista/JanMar2009/Foco.pdf>

- SILVA, A. S.; VITORINO, A.; ALVES, C. F.; CUNHA, J. A.; MONTEIRO, M. A. - **Livro branco sobre o Corporate Governance em Portugal.** [em linha] (2006) [Consult. 15 Mai. 2014]. Disponível em URL: <http://www.cgov.pt/>
- The Sarbanes-Oxley Act 2002, [em linha] [Consult. 30 Mai. 2014]. Disponível em URL: <http://www.soxlaw.com/>
- The Sarbanes-Oxley Act 2002, [em linha] [Consult. 13 Dec. 2014]. Disponível em URL: <http://www.sox-online.com/soxact.html#sec806>
- Updated COSO Internal Control Framework; FAQs 2nd Edition; Protiviti, [Em linha]. [Consult. 19 Set. 2014]. Disponível em: <http://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf>
- VICENTE, Isabel – **BPN:auditores debaixo de fogo. Expresso Economia.** [em linha] (2. Dez. 2010) [Consult. 15 Dez. 2014]. Disponível em URL: <http://expresso.sapo.pt/bpn-auditores-debaixo-de-fogo=f618946>
- VICENTE, Paula; REIS, Elizabeth; Ferrão, Fátima – **A amostragem como factor decisivo de qualidade.** 2.^a Edição, Lisboa: Edições Sílabo, 2001. ISBN: 972-618-246-8

Apêndices

I – Exemplo da estrutura de um relatório de controlo interno:

DESCRIÇÃO	DESCRIÇÃO DA DEFICIÊNCIA (ARTIGO 25.º, n.º 2, b))	
IMPLICAÇÕES	DESCRIÇÃO DAS POTENCIAIS IMPLICAÇÕES DA DEFICIÊNCIA (ARTIGO 25.º, n.º 2, b), iii)	
CATEGORIA DE RISCO	CATEGORIA DE RISCO (ARTIGO 25.º, n.º 2, b), iii)). CASO NÃO SEJA UTILIZADA A CLASSIFICAÇÃO PREVISTA NO ARTIGO 11.º, DEVEM SER INDICADAS (EM ANEXO) AS DEFINIÇÕES DE RISCO UTILIZADAS PELA INSTITUIÇÃO E A SUA CORRESPONDÊNCIA AOS FACTORES DE RISCO ASSOCIADOS	
GRAU DE RISCO	GRAU DE RISCO ATRIBUÍDO PELA INSTITUIÇÃO (ARTIGO 25.º, n.º 2, b), iii)). DEVEM SER INDICADOS OS CRITÉRIOS PARA A DIFERENCIAÇÃO DOS GRAUS DE RISCOS	
DATA DA DETECÇÃO	DATA DA DETECÇÃO DA DEFICIÊNCIA (ARTIGO 25.º, n.º 2, b), ii))	
DATA DA COMUNICAÇÃO	DATA DA COMUNICAÇÃO DA DEFICIÊNCIA AO ÓRGÃO DE ADMINISTRAÇÃO (ARTIGO 25.º, n.º 2, b), ii))	
MEDIDAS CORRECTIVAS	DESCRIÇÃO	DESCRIÇÃO DAS MEDIDAS EM CURSO OU A ADOPTAR PARA CORRIGIR AS DEFICIÊNCIAS DETECTADAS E PREVENIR A SUA OCORRÊNCIA FUTURA (ARTIGO 25.º, n.º 2, b), iv))
	PRAZO DE IMPLEMENTAÇÃO	PRAZO ESTABELECIDO PARA A IMPLEMENTAÇÃO DAS MEDIDAS CORRECTIVAS (ARTIGO 25.º, n.º 2, b), iv)). NO CASO DE CORRESPONDER A UMA DEFICIÊNCIA IDENTIFICADA EM RELATÓRIOS ANTERIORES, DEVE SER APRESENTADA JUSTIFICAÇÃO, CASO APLICÁVEL, PARA O NÃO CUMPRIMENTO DO CALENDÁRIO INICIALMENTE PREVISTO

GRAUS DE RISCO (EXEMPLO)

ELEVADO (REQUER A ATENÇÃO IMEDIATA DOS ÓRGÃOS DE GESTÃO):

ASPECTO GRAVE QUE PODERÁ LEVAR A: I) PERDAS SUBSTANCIAIS POSSIVELMENTE EM CONEXÃO COM OUTRAS FRAQUEZAS NO CONTROLO ORGANIZACIONAL OU RELATIVO A OUTRO PROCESSO, II) VIOLAÇÃO GRAVE DA ESTRATÉGIA DA INSTITUIÇÃO, POLÍTICAS E VALORES, III) DANOS NA REPUTAÇÃO/PRESTÍGIO DA INSTITUIÇÃO, IV) INCUMPRIMENTO DAS DISPOSIÇÕES LEGAIS E REGULAMENTARES APLICÁVEIS (DESIGNADAMENTE DAS REGRAS PRUDENCIAIS OU DOS PRAZOS DE REPORTE, INCLUINDO A EXISTÊNCIA DE INCORRECÇÕES OU FALTA DE INTEGRIDADE DOS REPORTES ENVIADOS À AUTORIDADE DE SUPERVISÃO) E V) CONSEQUÊNCIAS ADVERSAS, TENDO EM CONTA O QUADRO REGULATÓRIO EXISTENTE.

MÉDIO (REQUER A ATENÇÃO PERIÓDICA DOS ÓRGÃOS DE GESTÃO):

ASPECTO QUE PODERÁ LEVAR A: I) PERDAS FINANCEIRAS, II) PERDA DE CONTROLO DENTRO DA INSTITUIÇÃO OU RELATIVO A UM DETERMINADO PROCESSO, III) DANOS NA REPUTAÇÃO/PRESTÍGIO DA INSTITUIÇÃO, IV) INCUMPRIMENTO DAS REGRAS PRUDENCIAIS OU DOS PRAZOS DE REPORTE, INCORRECÇÕES OU FALTA DE INTEGRIDADE DOS REPORTES ENVIADOS À AUTORIDADE DE SUPERVISÃO E V) CONSEQUÊNCIAS ADVERSAS, TENDO EM CONTA O QUADRO REGULATÓRIO EXISTENTE.

BAIXO (RECOMENDA-SE A ATENÇÃO DOS ÓRGÃOS DE GESTÃO):

ASPECTO CUJA SOLUÇÃO PODERÁ ORIGINAR UMA MELHORIA DA QUALIDADE/EFICIÊNCIA DA ORGANIZAÇÃO OU DO PROCESSO. OS RISCOS PARA A INSTITUIÇÃO SÃO MUITO LIMITADOS.

Fonte:

PT/OBancoeEurosisistema/Eventos/Paginas/XIIIConferenciaAuditoria.aspx

<http://www.bportugal.pt/pt->

Anexos

I – Certificação Legal de Contas 2013 (Banco Espírito Santo, S.A.)



**KPMG & Associados - Sociedade de Revisores
Oficiais de Contas, S.A.**
Edifício Monumental
Av. Pires de Várzea, 71 - A, 11.^o
1069-005 Lisboa
Portugal

Telefone: +351 210 110 000
Fax: +351 210 110 121
Internet: www.kpmg.pt

CERTIFICAÇÃO LEGAL E RELATÓRIO DE AUDITORIA DAS CONTAS CONSOLIDADAS

Introdução

- 1 Nos termos da legislação aplicável, apresentamos a Certificação Legal das Contas e Relatório de Auditoria sobre a informação financeira consolidada contida no Relatório de gestão e nas demonstrações financeiras consolidadas anexas do exercício findo em 31 de Dezembro de 2013 do **Banco Espírito Santo, S.A.**, as quais compreendem o Balanço consolidado em 31 de Dezembro de 2013 (que evidencia um total de 80.608.016 milhares de euros e um total de capital próprio atribuível aos accionistas do Banco de 6.246.693 milhares de euros, incluindo um resultado líquido negativo atribuível aos accionistas do Banco de 517.558 milhares de euros), a Demonstração consolidada dos resultados, a Demonstração consolidada do rendimento integral, a Demonstração consolidada das alterações nos capitais próprios e a Demonstração consolidada dos fluxos de caixa do exercício findo naquela data, e os correspondentes Anexos.

Responsabilidades

- 2 É da responsabilidade do Conselho de Administração:
 - a) a preparação de demonstrações financeiras consolidadas de acordo com as Normas Internacionais de Relato Financeiro tal como adoptadas na União Europeia ("IFRS"), que apresentem de forma verdadeira e apropriada a posição financeira do conjunto das empresas incluídas na consolidação, o resultado consolidado das suas operações, o rendimento integral consolidado, as alterações nos capitais próprios consolidados e os fluxos de caixa consolidados;
 - b) que a informação financeira histórica, preparada de acordo com as IFRS seja completa, verdadeira, actual, clara, objectiva e lícita, conforme exigido pelo Código dos Valores Mobiliários;
 - c) a adopção de políticas e critérios contabilísticos adequados;
 - d) a manutenção de um sistema de controlo interno apropriado; e,
 - e) a informação de qualquer facto relevante que tenha influenciado a actividade do conjunto das empresas incluídas na consolidação, a sua posição financeira ou resultados.



- 3 A nossa responsabilidade consiste em verificar a informação financeira consolidada contida nos documentos de prestação de contas acima referidos, designadamente sobre se é completa, verdadeira, actual, clara, objectiva e lícita, conforme exigido pelo Código dos Valores Mobiliários, competindo-nos emitir um relatório profissional e independente baseado no nosso exame.

Âmbito

- 4 O exame a que procedemos foi efectuado de acordo com as Normas Técnicas e as Directrizes de Revisão/Auditoria da Ordem dos Revisores Oficiais de Contas, as quais exigem que o mesmo seja planado e executado com o objectivo de obter um grau de segurança aceitável sobre se as demonstrações financeiras consolidadas estão isentas de distorções materialmente relevantes. Para tanto o referido exame incluiu:
- a verificação das demonstrações financeiras das empresas incluídas na consolidação terem sido apropriadamente examinadas e, para os casos significativos em que o não tenham sido, a verificação, numa base de amostragem, do suporte das quantias e divulgações nelas constantes e a avaliação das estimativas, baseadas em juízos e critérios definidos pelo Conselho de Administração, utilizadas na sua preparação;
 - a verificação das operações de consolidação e da aplicação do método da equivalência patrimonial;
 - a apreciação sobre se são adequadas as políticas contabilísticas adoptadas e a sua divulgação, tendo em conta as circunstâncias;
 - a verificação da aplicabilidade do princípio da continuidade;
 - a apreciação sobre se é adequada, em termos globais, a apresentação das demonstrações financeiras consolidadas; e,
 - a apreciação se a informação financeira consolidada é completa, verdadeira, actual, clara, objectiva e lícita.
- 5 O nosso exame abrangeu ainda a verificação da concordância da informação financeira consolidada constante do Relatório de gestão com os restantes documentos de prestação de contas, bem como as verificações previstas nos números 4 e 5 do artigo 451.º do Código das Sociedades Comerciais.
- 6 Entendemos que o exame efectuado proporciona uma base aceitável para a expressão da nossa opinião.



Fonte: Relatório Individual de Contas 2013



Opinião

- 7 Em nossa opinião, as referidas demonstrações financeiras consolidadas apresentam de forma verdadeira e apropriada, em todos os aspectos materialmente relevantes, a posição financeira consolidada do **Banco Espírito Santo, S.A.** em 31 de Dezembro de 2013, o resultado consolidado das suas operações, o rendimento integral consolidado, as alterações nos capitais próprios consolidados, e os fluxos consolidados de caixa no exercício findo naquela data, em conformidade com as IFRS tal como adoptadas na União Europeia e a informação nelas constante é completa, verdadeira, actual, clara, objectiva e lícita.

Ênfase

- 8 Sem afectar a nossa opinião expressa no parágrafo anterior, chamamos à atenção para a Nota 46, a qual descreve a situação relativa à subscrição, pelos clientes do Grupo BES, de instrumentos de dívida emitidos pela Espírito Santo International, S.A. ('ESI') e refere a expectativa do Conselho de Administração do Banco quanto aos possíveis meios de reembolso dos mesmos através da implementação do plano de desalavancagem dos activos da ESI, do apoio dos seus accionistas e da capacidade da ESI para a obtenção ou renovação de linhas de crédito nos mercados financeiros e ainda do eventual apoio que possa vir a ser necessário por parte do Grupo ESFG e do BES.

Relato sobre outros requisitos legais

- 9 É também nossa opinião que a informação constante do relatório de gestão é concordante com as demonstrações financeiras consolidadas do exercício e o relatório do governo das sociedades inclui os elementos exigíveis nos termos do artigo 245.º-A do Código dos Valores Mobiliários.

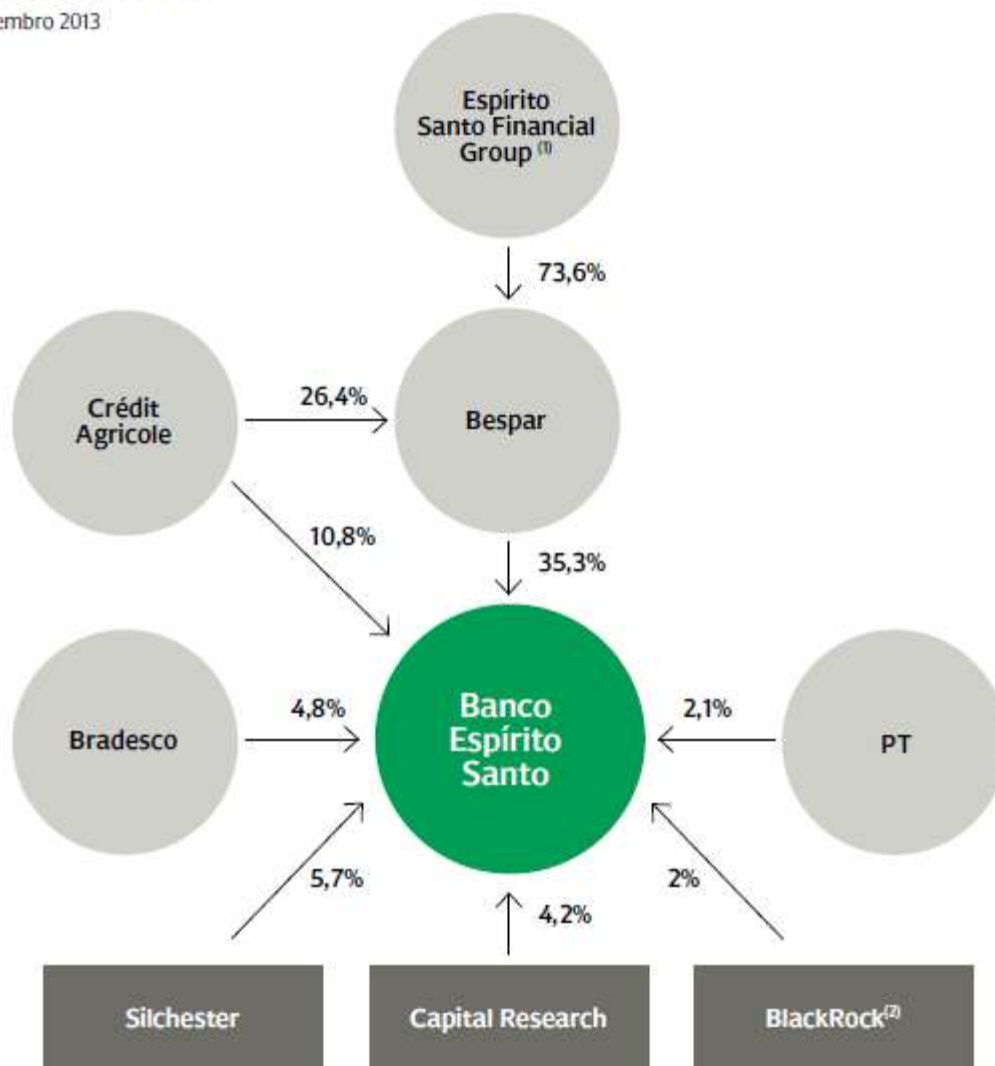
Lisboa, 9 de Abril de 2014

KPMG & Associados
Sociedade de Revisores Oficiais de Contas, S.A. (n.º 189)
representada por
Silvia Cristina de Sá Velho Corrêa da Silva Gomes (ROC n.º 1131)

II – Estrutura do Grupo 2013 (Banco Espírito Santo, S.A.)

Principais Acionistas

31 dezembro 2013



(1) Participação direta e indireta da ESFG na Bespar.

(2) A BlackRock aumentou a participação para 5,1% a 13 de fevereiro 2014.

Fonte: Relatório de Contas 2013, Grupo Espírito Santo