O CONTROLO INTERNO E A GESTÃO DE RISCO NAS EMPRESAS DA ÁREA METROPOLITANA DO PORTO

Malvina Maria dos Santos

Dissertação de Mestrado

Mestrado em Auditoria

Porto – 2013

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

O CONTROLO INTERNO E A GESTÃO DE RISCO NAS EMPRESAS DA ÁREA METROPOLITANA DO PORTO

Malvina Maria dos Santos

Dissertação de Mestrado
apresentado ao Instituto de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação da Doutora Alcina Augusta de Sena Portugal Dias

Porto – 2013

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

Resumo

Desde o final do século XX que se tem assistido a inúmeros escândalos financeiros com consequências dramáticas para as economias mundiais. Para dar resposta à falta de credibilidade dos mercados financeiros, à insegurança e à desconfiança dos investidores, várias instituições reguladoras dos mercados financeiros e organismos internacionais reviram as suas directrizes relativamente a procedimentos de controlo interno e de gestão de risco. O objectivo foi restaurar a confiança dos *stakeholders* na fiabilidade das demonstrações financeiras através do reforço do nível de exigência da informação divulgada para o mercado e na padronização e aperfeiçoamento de normas de controlo financeiro e de gestão de risco. Desde então, foram publicadas normas e desenvolvidos vários modelos de controlo interno e de gestão de risco.

Face à evolução e ao papel relevante que o controlo interno e a gestão de risco tem assumido como ferramenta de gestão é cada vez mais crítico que as organizações possuam adequados sistemas de gestão do risco e controlo interno, alinhados entre si e integrados na sua cadeia de valor e nos seus processos de negócio.

Com este estudo pretendemos analisar a forma, o grau de implementação e os procedimentos e mecanismos de controlo interno e de gestão de risco que as empresas implementaram nas suas organizações e a opinião e o nível de conhecimentos dos responsáveis pela estruturação, implementação e supervisão destas duas ferramentas de gestão. O estudo foi feito com base num inquérito enviado às empresas sedeadas na Área Metropolitana do Porto sendo que os principais resultados apurados indicaram que a maioria das empresas divulgam ter procedimentos e mecanismos de controlo interno e de gestão de risco e que a existência de auditoria interna na empresa não está positivamente relacionada com a existência destas duas ferramentas de gestão.

Palavras-chave: Controlo Interno, Gestão de Risco, Auditoria Interna, COSO ERM

Abstract

Since the end of XX century the world has witnessed numerous financial scandals with dramatic. To address the lack of credibility of the financial markets, insecurity and the distrust of investors, several regulatory agencies and international financial markets reviewed their internal control and risk management procedures guidelines. The aim was to restore stakeholder's confidence in the reliability of financial statements by strengthening the quality of the disclosed information to the market and standardizing and improving internal control and risk management rules. Since then, several standards have been published and various models of internal control and risk management have been developed.

According to the evolution and the role that internal control and risk management have assumed as a management tool, it is increasingly critical that organizations have adequate systems of risk management and internal control, integrated and aligned with each other in their value chain and their business processes.

This study intends to examine the degree of implementation of the procedures and internal control mechanisms and risk management that companies have implemented. Besides the opinion and the level of knowledge of those responsible for structuring, implementation and supervision of these two tools administration is also important. The study was based on a survey sent to companies based in the Porto Metropolitan Area. The main results obtained showed that most companies disclose implemented procedures and internal control and risk management mechanisms and that the existence of internal audit in the company is not positively related to the existence of these two management tools.

Keywords: Internal Control, Risk Management, Internal Audit, COSO ERM

Agradecimentos

A realização desta dissertação foi conseguida graças ao apoio e motivação incondicional de algumas pessoas, sem as quais este projecto não seria possível executar. Assim, uma enorme gratidão:

Á Doutora Alcina Dias Portugal, pela sua orientação, disponibilidade, atenção e compreensão que manifestou para a orientação deste trabalho;

Aos meus pais e ao Jorge pela ajuda, compreensão, incentivo e alento que sempre me dispensaram;

Aos meus amigos e colegas que sempre demonstraram a sua disponibilidade e apoio;

A todos aqueles que, directa e indirectamente, contribuíram para a realização desta dissertação, cujos nomes não foram mencionados mas que sempre serão lembrados.

Lista de abreviaturas

AICPA – American Institute of Certified Public Accountants

AS5 – Auditing Standard n.º 5

AS/NZS 4360 – Norma Australiana / Neozelandesa AS/ NZS 4360 de 2004

CEO – Chief Executive Officer

CFO – Chief Financial Officer

COBIT – Control Objectives for Information and Related Technology

COCO – Criteria of Control Framework

COSO – Committee of Sponsoring Organizations of the Treadway Commission

DRA – Directriz de Revisão/Auditoria

FERMA – Federation of European Risk Management Associations

IFAC – International Federations of Accountants

IIA – Institute of Internal Auditors

ISA 315 – International Standard on Auditing nº 315

ISO – International Organization for Standardization

ISO 31000 – International Organization for Standardization nº 31000

NYSE – New York Stock Exchange

PAIB – Professional Accountants in Business Committee

PCAOB – Public Company Accounting Oversight Board

PWC – PricewaterhouseCoopers

SAS – Statements on Auditing Standards

SEC – Securities and Exchange Commission

SCI – Sistema de Controlo Interno

SOX – Lei Sarbanes-Oxley

Índice geral

Índice de quadros

Índice de figuras

Índice de gráficos

Introdução

A crise financeira que se tem observado nas últimas décadas demonstrou que as economias e os mercados financeiros estão cada vez mais expostos à crescente globalização e complexidade da economia, à agressividade dos mercados, à rápida evolução tecnológica, entre outros factores. Associados a estes factores, as sucessivas falências fraudulentas, a ganância de certos gestores e accionistas e os inexistentes ou ineficazes sistemas de controlo estão a expor as organizações a cada vez maiores riscos.

Os progressos ao nível da *corporate governance* têm estado na origem de normativos e modelos de controlo interno e de gestão de risco como os Treadway, Cadbury, Turnbull, COCO (Criteria of Control Framework), COSO (Committee of Sponsoring Organizations of the Treadway Commission), COBIT (Control Objectives for Information and Related Technology), Sarbanes-OxleyAct (SOX), ao nível do controlo interno, e o COSO-ERM, a norma AS/NZS 4360 (2004) (Norma Australiana / Neozelandesa AS/ NZS 4360, de 2004), a Norma de Gestão de Risco – FERMA e a ISO 31000 (2009) (International Organization for Standardization n.º 31000), ao nível da gestão de risco.

Os riscos a que as empresas estão sujeitas podem assumir várias formas e o seu impacto pode ter consequências desastrosas. Deste modo, as empresas devem conhecer os riscos que ameaçam o seu negócio de modo a implementar sistemas de controlo interno e de gestão de risco adequados que atenuem ou eliminem esses riscos ou que impeçam a concretização das metas e objectivos definidos. Sistemas de controlo interno e de gestão de risco eficazes são determinantes para proteger e fortalecer as organizações e prevenir ou diminuir o impacto negativo de crises futuras.

Sendo um tema actual é neste contexto complexo e dinâmico que entendemos ser relevante conhecer a forma, o grau de implementação e os procedimentos e mecanismos de controlo interno e de gestão de risco que as empresas adoptaram e implementaram nas suas organizações e a opinião e o nível de conhecimentos dos responsáveis pela estruturação, implementação e supervisão destas duas ferramentas de gestão.

Tendo como base a revisão da literatura pretendeu-se fazer um estudo que respondesse a questões sobre os sectores de actividade que evidenciam uma maior implementação de sistemas de controlo interno e de gestão de risco, em que medida a auditoria interna é um factor preponderante para que as empresas adoptem estas duas ferramentas de gestão, qual o papel e a função da auditoria interna no processo de controlo interno e de gestão de risco e qual à importância dada à análise, reavaliação e ajustamento contínuo dos procedimentos e mecanismos de controlo interno e de gestão de risco das organizações.

Face ao exposto o nosso trabalho encontra-se organizado em cinco capítulos.

O capítulo I versa sobre o tema Controlo Interno. Inicialmente é feita a revisão da literatura, seguida do enquadramento histórico e dos seus principais aspectos e características. Faz-se também referência a alguns dos modelos existentes de controlo interno, nomeadamente o COSO e a Lei *Sarbanes-Oxley*, considerados, a nível mundial, como um dos mais respeitados e representativos das melhores práticas nesta área.

O capítulo II é dedicado ao Risco e nele são referidas algumas definições existentes na literatura. Dentro deste capítulo é abordado o tema da Gestão de Risco. Este tema contém definições, reflexões e modelos de gestão de risco, designadamente o COSO-ERM e a ISO 31000. É referido, de forma resumida, as características de cada um destes normativos, de forma a revelar que medidas devem ser adoptadas para se implementar um sistema de gestão de risco, e quais são os impactos da sua adopção. São apresentadas as críticas existentes de diversos autores, os pontos fortes e fracos dos dois modelos e referidas as principais diferenças entre estes dois normativos.

O capítulo III descreve a relação entre Controlo Interno e Gestão de Risco e em que medida o controlo interno deve ser parte integrante de um sistema de gestão de risco eficaz e eficiente. O papel da auditoria interna no processo de controlo interno e gestão de risco é também objecto de análise. São apresentadas as opiniões de alguns profissionais da área e também um estudo realizado em 2010 pelo PAIB com o objectivo de identificar os pontos fortes e fracos da gestão de riscos e dos sistemas de controlo interno existentes e praticados a nível mundial, investigar o papel da gestão de riscos e orientações de controlo interno e determinar a necessidade de convergência internacional entre as várias directrizes existentes.

No capítulo IV, no sentido de analisar a aplicação de sistemas de controlo interno e de gestão de risco nas empresas da Área Metropolitana do Porto, efectuamos uma análise empírica. Usando o questionário como metodologia de investigação, tentamos obter evidência empírica sobre a percepção e o nível de implementação de sistemas de controlo interno e de gestão de risco nas empresas, na óptica da gestão e/ou dos auditores internos.

No último capítulo apresentam-se as principais conclusões da revisão da literatura, os resultados obtidos no estudo efectuado e os possíveis e pertinentes temas a estudar dentro desta temática numa futura investigação.

Neste trabalho optou-se por não utilizar o Novo Acordo Ortográfico da Língua Portuguesa.

Capitulo I – Controlo Interno

1.1 Definição

Na língua portuguesa o termo controlar significa examinar, fiscalizar, inspeccionar, conferir, verificar, ter sob controlo, dominar, ter sob seu poder, dominar, orientar, conduzir ou guiar. Controlar significa tomar medidas para que as metas definidas sejam executadas de acordo com o planeado. Assim, podemos entender o controlo como um processo de garantia de que os objectivos delineados são cumpridos.

O controlo interno é um conjunto de regras definidas com vista a garantir que o processo de controlo é eficiente e eficaz e que alcança os objectivos definidos.

Martins & Morais (2007) refere que o AICPA foi o primeiro organismo a definir o controlo interno, através da SAS n.º 1, indicando que "o controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas adoptadas num negócio a fim de garantir a salvaguarda de activos, verificar a adequação e confiabilidade dos dados contabilísticos, promover a eficiência operacional e encorajar a adesão às políticas estabelecidas pela gestão."

O PCAOB na sua AS5 (2010) define controlo interno como um processo desenhado pela gestão da empresa ou sob a sua supervisão para promover uma segurança razoável sobre a fiabilidade do relato financeiro e a preparação de demonstrações financeiras para fins externos, de acordo com os princípios contabilísticos geralmente aceites, e inclui princípios e procedimentos que:

- ✓ Respeitam a inviolabilidade dos registos que, com segurança razoável, reflectem precisa e adequadamente as transacções e utilização dos activos da empresa;
- ✓ Prestam uma razoável segurança de que as transacções são registadas atempadamente para permitir a preparação das demonstrações financeiras, de acordo com os princípios contabilísticos geralmente aceites, e que as receitas e os gastos da empresa são efectuados somente de acordo com a autorização da gestão e da direcção da empresa; e
- ✓ Promovem segurança razoável quanto à prevenção ou detecção tempestiva de aquisições não autorizadas, uso indevido ou retirada dos activos da empresa, que possam ter um efeito material nas demonstrações financeiras.

De acordo com a ISA 315 publicada pelo IFAC [1] (2009) controlo interno é o processo concebido, implementado e mantido pelos responsáveis pela administração, gestão e restante

[1] O IFAC é a organização mundial criada para a profissão de contabilidade e dedicada a servir o interesse público através do fortalecimento da profissão, contribuindo para o desenvolvimento de fortes economias internacionais.

pessoal para providenciar uma segurança razoável acerca do alcance dos objectivos da entidade relacionados com a fiabilidade do relato financeiro, eficácia e eficiência das operações e conformidade com as leis e os regulamentos aplicáveis, consistindo nos seguintes componentes:

- ✓ Ambiente de controlo;
- ✓ Processo de avaliação de riscos da entidade;
- ✓ Sistema de informação, incluindo os processos de negócio relacionados, relevante para a comunicação e relato financeiro;
- ✓ Actividades de controlo; e
- ✓ Monitorização dos controlos.

A DRA n.º 410 (2000) define sistema de controlo interno como sendo todas as políticas e procedimentos (controlos internos) adoptados pela gestão de uma entidade que contribuam para a obtenção dos objectivos da gestão de assegurar, tanto quanto praticável, a condução ordenada e eficiente do seu negócio, incluindo a aderência às políticas da gestão, a salvaguarda de activos, a prevenção e detecção de fraude e erros, o rigor e a plenitude dos registos contabilísticos, o cumprimento das leis e regulamentos e a preparação tempestiva de informação financeira credível.

Segundo esta norma o sistema de controlo interno compreende cinco componentes interligados, a destacar:

- ✓ Ambiente de controlo que se traduz na atitude geral, na consciencialização e nas acções da gestão e do órgão de gestão a respeito do sistema de controlo interno e a sua importância dentro da entidade, influenciando a consciência de controlo dos seus colaboradores. É o ponto de partida para os outros componentes do controlo interno, proporcionando disciplina e estrutura;
- ✓ Avaliação do risco, ou seja, a identificação e análise pela entidade dos riscos relevantes para a realização dos seus objectivos, formando a base para a determinação da forma como os riscos devem ser geridos;
- ✓ Procedimento de controlo, ou seja, as políticas e procedimentos que ajudam a assegurar que as directivas da gestão são executadas;
- ✓ Informação e comunicação é a identificação, recolha e troca de informação de forma a permitir aos empregados levar a cabo as suas responsabilidades;
- ✓ Monitorização, que corresponde ao processo que avalia a qualidade do desempenho do controlo interno ao longo do tempo.

O COSO, por sua vez, define controlo interno como sendo um processo efectuado por pessoas da direcção, da gestão e outros colaboradores, designado para fornecer uma razoável certeza acerca do cumprimento dos objectivos em três categorias, nomeadamente a eficiência e

eficácia das operações, a confiança e fiabilidade das demonstrações financeiras e a conformidade com as leis e regulamentos.

O controlo interno é, desta forma, um instrumento que melhora e aperfeiçoa os processos de gestão e permite à administração atingir os objectivos definidos e tornar a organização mais eficiente através do cumprimento de regras e metas estipuladas e da optimização de recursos.

1.2 O controlo interno antes de 2002

Um certo número de normativos de controlo interno, como o COSO (EUA), *Turnbull* (UK), e CoCo (Canadá), foram desenvolvidos antes dos escândalos financeiros ocorridos em grandes grupos económicos no final do século XX. Estes modelos de controlo interno, descritos como um "processo"[2], foram estabelecidos, operados e monitorizados pelos responsáveis pela administração e gestão de empresas para fornecer garantia razoável quanto à realização dos objectivos definidos. IFAC(2006)

Em 1985 foi formada uma Comissão sobre o Relato Financeiro Fraudulento, conhecida como Comissão *Treadway*[3]. Este grupo de trabalho tinha como objectivo uniformizar o conceito de controlo interno uma vez que existiam várias opiniões e pareceres sobre este tema, não havendo um entendimento comum sobre a definição de controlo interno e qual a sua missão. Dois anos depois foi elaborado um relatório que salientava a necessidade de um ambiente de controlo adequado e de uma função de auditoria interna objectiva, o papel e a importância dos comités de auditoria independentes, que deveriam ser composto por profissionais independentes, competentes e que possuíssem um adequado conhecimento da actividade desenvolvida. Defendia a existência de relatórios públicos que descrevessem a eficiência do controlo interno das organizações e o estabelecimento de critérios de controlo interno que permitissem às empresas melhorar os seus controlos. Pires (2008)

Em 1988, e com base nestas conclusões, a *Securities and Exchange Commission* (SEC) exigiu que todas as empresas por si reguladas tivessem um comité de auditoria, com uma maioria de administradores, não executivos cujo principal objectivo seria o reforço da supervisão do processo de relato financeiro empresarial. Pires (2008)

No seguimento do documento *Treadway Report* foi desenvolvido e publicado pelo COSO, em 1992, um trabalho sobre o controlo interno designado por *Internal Control-Integrated* Framework.

[2] O termo processo é usado em um sentido amplo, que vai além dos procedimentos, incluindo elementos como cultura corporativa e políticas, bem como sistemas e tarefas.

[3] Esta designação deve-se ao facto de a comissão ter sido presidida por James Treadway, um anterior membro da SEC.

Neste trabalho abordaremos apenas como modelos de controlo interno o COSO e a Lei Sarbanes-*Oxley* relativamente às suas principais características e à forma como influenciaram os sistemas de controlo interno das organizações.

1.3 Modelos de controlo interno

1.3.1 COSO

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) é uma organização privada e sem fins lucrativos, com sede nos Estados Unidos da América, composta por cinco organizações profissionais[4],e que, apesar ter estas entidades como patrocinadoras, é um órgão independente e dedicado à melhoria dos relatórios financeiros através da ética, efectividade dos controlos internos e governo das sociedades.

Os resultados do Relatório *Treadway*, atrás referidos, foram determinantes para que o COSO, em 1992, procedesse ao desenvolvimento de um modelo integrado de controlo interno que estabeleceu critérios visando a ética empresarial, a gestão de risco, a avaliação pela gestão do sistema de controlo interno e orientações para o relato público dessa avaliação. Tem sido, desde então, o modelo que mais consenso tem reunido como ferramenta para a avaliação da eficácia do sistema de controlo interno de uma empresa.

O COSO é um dos modelos de controlo interno mais conhecido e utilizado internacionalmente, devido, sobretudo, à facilidade na sua implementação, à adequação a todo o tipo de organização, ao facto de destacar uma visão integrada da empresa, à ênfase nos objectivos definidos pela empresa e nos riscos associados, ao foco nos processos e no facto de o controlo dever ser parte integrante desses processos.

1.3.1.1 COSO Internal Control – Integrated Framework (1992)

Os gestores das organizações têm procurado formas de controlar as suas empresas com o objectivo de manter as metas definidas e de minimizar surpresas a longo prazo. O controlo interno é encarado cada vez mais como uma solução para uma variedade de problemas potenciais.

O modelo COSO deve ser adaptado à realidade e às características da organização para que seja usado como metodologia de avaliação dos controlos internos definidos pela organização.

[4] Estas organizações são o AICPA (American Institute of Certified Public Accountants), a AAA (American Accounting Association), o IAA (The Institute of Internal Auditors), o IMA (Institute of Management Accountants) e o FEI (Financial Executives Institute)

Assim, fornece um critério de avaliação dos componentes do controlo interno com o objectivo de obter um elevado grau de transparência nas demonstrações financeiras.

O controlo interno tem como fim fornecer uma garantia razoável, e não uma certeza, quanto à realização dos objectivos de controlo, designadamente:

- ✓ Eficácia e eficiência das operações, nomeadamente os objectivos de uma organização, incluindo metas de desempenho e rentabilidade e salvaguarda dos activos.
- ✓ Fiabilidade das demonstrações financeiras, abrangendo a preparação de informação financeira fiável; e
- ✓ Cumprimento de leis e regulamentos a que a empresa está sujeita.

É através do controlo interno que uma organização garante as metas definidas, permitindo alcançar os seus objectivos, realizar a sua missão e minimizar os imprevistos. O controlo interno é considerado uma ferramenta que fornece uma visão geral de toda a organização e orientações que auxiliam as diversas áreas ou departamentos da organização, permitindo aos gestores identificar e avaliar as deficiências nas actividades de controlo, permitindo assim a tomada de medidas para fazer face aos desvios encontrados.

A estrutura do COSO identifica cinco componentes de controlo inter-relacionados e que precisam de estar integrados para assegurar o alcance dos objectivos definidos, oferecendo uma estrutura eficaz para descrever e analisar o sistema de controlo interno implementado numa organização. Os cinco componentes são:

- ✓ Ambiente de controlo – é a base para todos os outros componentes do controlo interno proporcionando disciplina e estrutura, incluindo factores como integridade, ética, competência, autoridade e responsabilidade;
- ✓ Avaliação dos riscos – envolve a identificação e análise pela gestão dos riscos relevantes que influenciam a execução dos objectivos definidos pela organização formando uma base para determinar como os riscos devem ser geridos;
- ✓ Actividades de controlo – são as políticas/procedimentos implementados para assegurar que as acções identificadas pela gestão como necessárias para mitigar os riscos são efectivamente realizadas[5];
- ✓ Informação e comunicação – suportam os outros componentes através da captação e comunicação oportuna da informação relevante por toda a organização; e
- ✓ Monitorização ou supervisão – abrange a supervisão dos controlos internos pela gestão ou outras entidades externas ao processo, as actividades da auditoria interna, a avaliação contínua do desempenho do sistema de controlo, os questionários de auto-avaliação e a constante adaptação do sistema à realidade.

[5] Actividades de controlo ocorrem em toda a organização, em todos os níveis e em todas as funções. Elas incluem uma variedade de actividades tão diversas como aprovações, revisões de desempenho operacional, autorizações, verificações, conciliações, a segurança dos activos e segregação de funções.

Figura n.º 1 – Cubo COSO (Internal Control – Integrated Framework)

Fonte: Traduzido COSO (2004)

Existe uma relação directa entre as três categorias de objectivos, que são o que uma entidade pretende alcançar, e as componentes, que consiste nos meios necessários para atingir os objectivos.

Todos os componentes são relevantes para cada categoria de objectivos e devem estar presentes e a funcionar eficazmente, pois só assim o controlo interno pode ser eficaz. O COSO refere que há uma sinergia e articulação entre esses componentes, formando um sistema integrado que reage dinamicamente às mudanças. O controlo interno é mais eficaz[6] quando os controlos são construídos na infra-estrutura da entidade e são uma parte da essência da empresa. Controlos "fabricados" apoiam iniciativas de qualidade de delegação de poder evitando custos desnecessários e facilitando uma resposta rápida às mudanças.

O COSO (1994, p. 79) refere que a probabilidade de atingir os objectivos definidos é afectada por limitações inerentes a todos os SCI, algumas delas independentemente de o controlo interno estar bem concebido e de funcionar eficazmente, tais como desinteresse por parte da administração/gerência, julgamento errado na tomada de decisão, erros humanos, fraude e conluio, ignorar deliberadamente os controlos, relação custo/benefício do controlo, a dimensão da empresa, entre outros.

Assim, no modelo COSO estes componentes interagem para criar uma estrutura de controlo interno forte, através de uma liderança clara, partilha de valores e uma cultura que enfatiza a responsabilidade pelo controlo. Os vários riscos que a empresa enfrenta são identificados e

[6] A avaliação da eficácia pode ser feita para todo o sistema de controlo interno, como pode ser restrita a cada uma das suas categorias de objectivos, mantendo-se, no entanto, a necessidade de satisfazer todos os cinco componentes.

avaliados periodicamente a todos os níveis da organização e dentro de todas as funções. As actividades de controlo são proactivamente desenhadas para mitigar os riscos significativos. A informação crítica para a identificação dos riscos e para alcançar os objectivos do negócio é comunicada através de canais ascendentes, descendentes e ao longo da organização e todo o sistema de controlo interno é monitorizado continuamente e os problemas são tratados atempadamente.

Tanto o COSO como o COSO-ERM[7], que será desenvolvido em capítulo posterior, são aceites como válidos para suportar a avaliação da eficácia do controlo interno sobre o relato financeiro preconizado pela Lei *Sarbanes-Oxley*.

1.3.2 Lei Sarbanes-Oxley

No princípio do século XX, o mercado de acções norte-americano foi afectado de forma significativa por um período de crise de credibilidade no mercado, devido a graves manipulações nas demonstrações financeiras e consequentes fraudes gigantescas de grandes empresas conceituadas do mercado norte-americano, como foi o caso da *Enron*, da *WorldCom*, *Merck*, *Parmalat*, da *Health South*, entre outros, e que abalaram profundamente a confiança dos investidores no relato financeiro das empresas. A reacção no mercado financeiro foi imediata e as bolsas caíram no mundo inteiro contribuindo para o abrandamento da performance do mercado de capitais mundial.

É como consequência de todos estes acontecimentos que surge a Lei *Sarbanes-Oxley*, promulgada em Julho de 2002 nos Estados Unidos, estabelecendo uma das maiores reformas legislativas já ocorridas na regulamentação do mercado de capitais norte-americano na tentativa de restabelecer a confiança dos investidores transformando as boas práticas de governo das sociedades em leis.

Segundo Silva, A. S., Vitorino, A., Alves, C. F., Cunha, J. A., & Monteiro, M. A. (2006, p. 57), a Lei Sox "constitui resposta do poder político norte-americano ao clima de descrença e pessimismo que, no rescaldo daqueles acontecimentos, se havia instalado entre os investidores, já abalados pelo declínio de uma fase de euforia bolsista que pusera em jogo uma parcela importante da poupança privada."

A lei criou um organismo regulador das empresas de auditoria e determinou sansões e responsabilidades dos directores executivos e financeiros, nomeadamente a responsabilização por estabelecer, avaliar e monitorizar a eficiência e eficácia do controlo e procedimentos internos, na ênfase de tentar recuperar o equilíbrio e a confiança no mercado de capitais, e estabeleceu regras mais rígidas e abrangentes para a padronização e aperfeiçoamento dos

[7] Este modelo incorpora o modelo de controlo interno COSO, permitindo que as organizações adoptassem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno progredindo para um processo de gestão de risco.

controlos financeiros das empresas, nacionais ou estrangeiras, e das suas filiais que possuíam capital negociado na Bolsa de Nova Iorque (NYSE).

Essa lei, segundo Schreiner (2004, p. 16), tem como objectivo "obrigar as empresas que têm os seus títulos negociados nesse mercado a cumprirem exigências de avaliação de risco, controlos internos, informação, comunicação e monitorização de maneira muito mais rigorosa do que as regras até então vigentes".

De forma a recuperar a confiança dos investidores nos mercados financeiros e precaver danos decorrentes das fraudes cometidas por empresas já referenciadas neste capítulo a Lei SOX está repleta de reformas com vista a promover um melhor governo das sociedades, nomeadamente quanto à ética nos negócios e à eficácia dos controlos internos, procurando "reparar" a perda da confiança pública nos líderes empresariais e enfatizar uma vez mais a importância dos padrões éticos na preparação das informações financeiras reportadas aos investidores[8].

Borgeth (2007, p.19) relata que o objectivo final da lei é "restabelecer o nível de confiança nas informações geradas pelas empresas e, assim, consolidar a teoria dos mercados eficientes que orienta o funcionamento do mercado de títulos e valores mobiliários".

Com a implementação da Lei SOX a transparência dos relatórios é de fundamental importância para os investidores, garantindo a qualidade e a segurança na informação divulgada nos relatórios financeiros e permitindo aos investidores tomarem melhores decisões sobre o rumo dos seus investimentos.

Para o cumprimento da Lei SOX todo esforço é e/ou foi válido pois a sua implementação fez com que o mercado americano se reerguesse novamente de forma que o mesmo trouxesse vantagens aos investidores e demais intervenientes.

1.3.2.1 Principais aspectos da Lei Sarbanes-Oxley

Com o objectivo de estabilizar e devolver a confiança aos mercados bolsistas, após os escândalos de fraudes já referidos, o Presidente Norte-americano assinou em 30 de Julho de 2002 a Lei de Reforma da Contabilidade Empresarial e da Protecção dos Investidores (*Public Company Accounting Reformand Investor Protection Act*), também conhecida por Lei *Sarbanes-Oxley*.

[8] Para implementar a Lei SOX é necessário que sejam adoptadas boas práticas de governo das sociedades permitindo à empresa conquistar a confiança por parte de todos os envolvidos na organização, principalmente para os investidores, que vêem nas boas práticas um diferencial para tomar decisões de investimento e da sua participação na mesma.

A Lei *Sarbanes-Oxley* centra-se na revisão dos procedimentos de *corporate governance* para empresas cotadas, nacionais ou estrangeiras, especialmente os relacionados com a verificação da adequação e da divulgação da informação financeira relativa a resultados. Também estabelece a responsabilidade pessoal do CEO (*Chief Executive Officer*) e do CFO (*Chief Financial Officer*) na certificação das demonstrações financeiras e das divulgações contidas no relatório periódico relativamente à representação verdadeira, em todos os aspectos materiais, das operações e condições financeiras da empresa, assim como a assunção da responsabilidade pela implementação e eficácia do sistema de controlo interno e conclusões decorrentes da avaliação de realização dos mesmos. Ao nível dos auditores inclui requisitos para a independência do auditor e define que trabalhos de não-auditoria não podem ser realizados pelos auditores, a periodicidade de rotação das empresas que prestam os serviços de auditoria, assim como requer que cada relato financeiro reflicta todos os ajustamentos materiais identificados. Protege também os colaboradores da empresa que forneçam evidência de fraude e torna esta protecção extensível aos auditores e aumenta as penas aplicadas a crimes por fraude.

A Lei *Sarbanes-Oxley* determina que a administração da empresa deve conhecer as informações materiais arquivadas na SEC e distribuídas aos investidores e deve, também, responsabilizar-se pela integridade, profundidade e precisão dessas informações. Esta lei pretende assegurar práticas éticas de negócio através de uma gestão mais responsável, consciente e sustentável com o objectivo de obter uma maior transparência, quer para a direcção e gestão de topo quer para os seus investidores.

Em 2003 o presidente da SEC William Donaldson, testemunhando sobre a implementação da SOX perante uma comissão do senado dos EUA, proferiu a seguinte afirmação:

> "Para muitas empresas as novas regras de relato sobre o controlo interno representarão o único requisito importante associado à Lei *Sarbanes-Oxley*. O estabelecimento e a manutenção dos controlos internos sobre relatórios financeiros sempre foram uma importante responsabilidade da gestão. Um sistema eficaz de controlos internos sobre relatórios financeiros é necessário para produzir demonstrações financeiras fiáveis e outras informações financeiras utilizadas pelos investidores. Ao exigir um relatório declarando a responsabilidade da administração para os controlos internos sobre relatórios financeiros e avaliação da administração sobre a eficácia desse controlo, os investidores serão mais capazes de avaliar as responsabilidades da gestão e da confiança da divulgação de informação de uma empresa. A avaliação anual requerida aos controlos internos sobre os relatórios financeiros, incentivará as empresas a disponibilizar recursos e atenção adequados à manutenção de tal controlo. Além disso, a avaliação deverá ajudar a identificar fraquezas e deficiências potenciais previamente a um colapso do sistema e pode

> ajudar as empresas a detectar mais cedo um relato financeiro fraudulento e, talvez assim, impedir a fraude financeira ou minimizar os seus efeitos adversos"[9].

Uma das críticas feitas à Lei *Sarbanes-Oxley* é o facto de burocratizar procedimentos, ser muito extensa e de difícil compreensão. Uma das maiores desvantagens da aplicação da Sox é o seu elevado custo de implementação, em especial para organizações de pequena dimensão. Tal facto pode ser compensado com os benefícios de eficácia e eficiência das operações e da elaboração de relatórios financeiros fiáveis, devido também à maior responsabilização atribuída aos responsáveis pela sua emissão. Holt (2006 como citado em Silva, Cecília, 2009, p.24)

Segundo McKay, (2007) as vantagens da Sox são o seu impacto positivo no mercado de capitais, uma maior padronização, transparência, formalização dos controlos internos, maior credibilidade dos relatórios financeiros, maior importância dada ao governo das sociedades, ganhos em eficiência e eliminação de más auditorias.

É nas secções 302 e 404, relativas à avaliação pela gestão do sistema de controlo interno existente, nomeadamente quanto ao relato financeiro e subsequente avaliação pela auditoria, que se centram as preocupações da generalidade das empresas que procuram a conformidade com a SOX.

1.3.2.2 Secção 302

A secção 302 designa-se Responsabilidade da Sociedade pelo Relato Financeiro e está toda centrada nas responsabilidades do CEO e CFO quanto ao relato financeiro, sendo que os controlos internos, a sua estrutura, avaliação, divulgação de deficiências/fraquezas e alterações são parte integrante das mesmas. Nessa medida foi determinado que as empresas deveriam adoptar controlos internos mais rígidos com o objectivo de garantir exactidão, fiabilidade e transparência na divulgação de informações financeiras e dos actos praticados pela administração.

Esta secção estabelece que a SEC deve requerer para cada empresa cotada que o seu CEO e o seu CFO certifiquem em cada relato anual ou trimestral que:

- ✓ Procederam à sua revisão;
- ✓ O relatório não contém nenhuma declaração falsa ou omissa que distorça materialmente as demonstrações financeiras, de acordo com o conhecimento que possuem;
- ✓ Baseado na informação que possuem, a informação financeira divulgada no relatório, apresenta de forma verdadeira e apropriada, em todos os aspectos materiais, as

[9]Tradução livre

posições financeiras e os resultados da actividade da entidade emitente até, e para, os períodos apresentados no relato;

- ✓ São responsáveis por estabelecer e manter os controlos internos;
- ✓ Delinearam controlos que asseguram que informação material, relacionada com a entidade emitente e as suas subsidiárias, é-lhes dada a conhecer nomeadamente durante o período de preparação do relato periódico;
- ✓ Avaliaram a eficácia dos controlos internos;
- ✓ Apresentaram no relato as suas conclusões sobre a eficácia dos seus controlos internos baseadas na avaliação efectuada;
- ✓ Foram divulgados ao auditor e à comissão de auditoria todas as deficiências importantes detectadas nos controlos internos que possam adversamente afectar a capacidade do emitente de registar, processar, resumir e relatar informação financeira, fraquezas materiais e qualquer fraude, material ou não, que envolva a administração ou outros colaboradores que tenham um papel significativo nos controlos internos;
- ✓ Divulgaram se houve ou não modificações significativas nos controlos internos ou em outros factores que possam, de forma significativa, afectar os controlos internos em data subsequente à da sua avaliação, incluindo quaisquer acções correctivas relacionadas com deficiências significativas e fraquezas materiais.

Em conclusão, a secção 302 refere de forma explícita que os directores executivos e os directores financeiros devem declarar, pessoalmente, que são responsáveis pela criação, avaliação e monitorização do controlo interno e por divulgar todas e quaisquer relevâncias significativas do controlo, como insuficiências materiais e actos de fraudes. Cada documento trimestral deverá ainda certificar que estes responsáveis avaliaram com eficácia os controlos internos.

1.3.2.3 Secção 404

A secção 404, designada Avaliação dos Controlos Internos pela Administração, determina uma avaliação anual dos controlos e procedimentos internos para a emissão de relatórios financeiros. Tal como é exigido na Secção 302, também os directores executivos e os directores financeiros devem avaliar e atestar periodicamente a eficácia desses controlos.

A Secção 404 obriga as organizações a incluir no seu relatório anual informação sobre controlo interno, emitido pela administração, que:

- ✓ Afirme a responsabilidade da gestão pelo estabelecimento e manutenção de uma estrutura e procedimentos de controlo interno adequados para a emissão do relato financeiro;

- ✓ Contenha uma avaliação e obtenha conclusões, até ao fim do mais recente ano fiscal, da eficácia da estrutura e procedimentos de controlo interno para a emissão de relatórios financeiros;
- ✓ Declare que o auditor independente da organização atestou e reportou a avaliação feita pela administração sobre seus controlos e procedimentos internos para a emissão de relatórios financeiros, de acordo com as normas emitidas ou adoptadas pelo PCAOB, não devendo ser objecto de um compromisso separado.

Segundo a Deloitte (2003) a avaliação fornecida aos auditores independentes deve ser substantiva, bem documentada e abrangente. Para tal essa avaliação deve conter pelo menos:

- ✓ Informações acerca do ambiente de controlos gerais da organização;
- ✓ Descrição do processo adoptado pela administração para identificar, classificar e avaliar riscos que possam impedir que a organização alcance seus objectivos de emissão de relatórios financeiros;
- ✓ Descrição completa dos objectivos de controlo criados pela administração para direccionar os riscos identificados e as respectivas actividades de controlo;
- ✓ Descrição dos sistemas de informática e procedimentos de comunicação adoptados para fornecer suporte ao tópico anterior;
- ✓ Resultados e documentação suporte da avaliação mais recente feita pela administração sobre a eficácia da estrutura e das operações das actividades individuais de controlo;
- ✓ Relação de todas as deficiências encontradas na estrutura e na implementação das actividades de controlo, bem como os procedimentos propostos para sua correcção;
- ✓ Descrição do processo adoptado para comunicar deficiências significativas e insuficiências materiais aos auditores independentes e ao Comité de Auditoria;
- ✓ Descrição dos procedimentos de monitorização executados para assegurar que a estrutura de controlos internos está a ser operada conforme planeado e que os resultados dos procedimentos de monitorização são executados e objecto de revisão;
- ✓ Descrição do processo de criação da divulgação e das actividades de controlo relacionadas.

Nesta secção é referida a importância da ética no relatório anual de informação exigindo que se faça referência à adopção ou não ao código de ética seguido pelos gestores ou pelo responsável pela contabilidade e em caso de alterações ou abandono do código de ética tal deverá ser prontamente divulgado. É também exigido que as informações relativas às operações financeiras sejam actuais, rápidas e frequentes de modo a proteger e a poder informar com a máxima celeridade e eficácia os investidores.

Em jeito de conclusão o *COSO's Internal Control Integrated Framework (1992)* adoptou uma abordagem muito mais ampla de controlo interno que a Lei *Sarbanes-Oxley,* tanto em termos de âmbito, objectivos e abordagem. O COSO adoptou uma abordagem de risco para controlo interno e concentrou-se em todos os controlos a que as organizações estão sujeitas e não apenas nos controlos directamente relacionados com os relatórios financeiros.

Capitulo II – Risco

2.1 Definição

No dicionário de língua portuguesa a palavra risco significa, entre outras coisas, a probabilidade de insucesso, de malogro de determinada coisa em função de um acontecimento eventual e incerto cuja ocorrência não depende exclusivamente da vontade dos interessados.

Não existe um significado universal para este termo sendo que está sempre relacionado com os possíveis efeitos de ocorrência de um evento e, normalmente, tem associado uma conotação negativa. No entanto, o risco também pode ser visto como uma oportunidade, ou seja, pode ter um efeito positivo no sentido de constituir uma oportunidade.

Em termos literários existem também diversas definições de risco.

A norma ISO 31000 (2009) define risco como sendo o efeito da incerteza sobre os objectivos delineados pela organização.

O COSO (2004) define risco como sendo a possibilidade de um evento ocorrer e afectar negativamente a realização dos objectivos definidos. Os eventos podem resultar de fontes internas ou externas à organização e podem causar impactos positivos e ou negativos. Nesse sentido, o COSO refere que os eventos que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os riscos de impacto positivo podem contrabalançar com os de impacto negativo ou podem representar oportunidades que, por sua vez, representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização de objectivos.

Segundo a FERMA (2003) o "risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências".

Para o IIA, o risco é a possibilidade da ocorrência de um evento que possa ter impacto sobre o alcance de objectivos. O risco é medido em termos de impacto e probabilidade de ocorrência (IIA 2009, p. 38).

De acordo com Cruz (2008, como citado em Pires, 2010, p. 5) o risco pode ser definido como uma possibilidade de que algum acontecimento desfavorável venha a ocorrer e que possa

Hussein (2008) o *American Institute of Certified Public Accountants* (AICPA), classificou os riscos em três grupos:

- ✓ Riscos relacionados com o ambiente empresarial, que correspondem a ameaças do ambiente empresarial em que a entidade opera, como riscos decorrentes da actuação

da concorrência, políticos, legais ou decorrentes da acção de órgãos reguladores e fiscalizadores, financeiros e de procura;

- ✓ Riscos relacionados com o processo de negócio e dos seus activos, nomeadamente ameaças ao negócio da organização pelos concorrentes e perdas de activos, sejam físicos ou financeiros; e,
- ✓ Riscos relacionados com informação, designadamente a ocorrência de ameaças decorrentes da má qualidade das informações para o processo de tomada de decisão e fornecimento de informações a terceiros.

Para Beja (2004) o risco significa estar exposto à possibilidade de ocorrência de um resultado negativo.

Cicco e Fantazzini (2003, como citado em Ferreira, 2010, p. 16) consideram que o risco pode significar, por um lado, a incerteza quanto à ocorrência de um determinado evento (acidente) e, por outro, a probabilidade de perda ou perdas que uma empresa pode sofrer em consequência de um ou de vários acidentes.

"Risco é a ameaça de que um evento ou uma acção afecte adversamente a capacidade da organização em maximizar valor para os *stakeholders* e atingir os seus objectivos e estratégias de negócio". Darlington,Grout, &Whitworth (2001).

A DRA 400 (2000) define risco de revisão/auditoria como sendo a susceptibilidade do revisor/auditor dar uma opinião de revisão/auditoria inapropriada quando as demonstrações financeiras estejam distorcidas de forma materialmente relevante.

Numa publicação feita em 1999 o IFAC definiu risco como um acontecimento futuro incerto que possa influenciar o alcance dos objectivos estratégicos, operacionais e financeiros da organização.
Segundo a mesma instituição a noção de risco é normalmente usada em diferentes sentidos, designadamente:

- ✓ Risco como oportunidade na medida que existe uma relação entre risco e rendibilidade uma vez que, em geral, quanto maior o risco maior o potencial lucro ou prejuízo;
- ✓ Risco como perigo ou ameaça, referindo-se aos acontecimentos potencialmente negativos; e
- ✓ Risco como mera incerteza, referindo-se aos efeitos negativos e positivos potenciais.

Em resumo, correr riscos é um facto inerente à própria existência de uma empresa. Face a esta realidade torna-se indispensável às empresas gerir e, na medida do possível, controlar os riscos e a probabilidade da sua ocorrência. Uma das formas de o conseguir é através da implementação de um sistema de gestão de risco de forma a minimizar os riscos e a potenciar

as oportunidades que lhe estão associadas. A performance empresarial depende, assim, de uma boa gestão dos riscos de forma a minimiza-los ou a transformá-los em oportunidades, criando valor para a empresa. A perda de uma oportunidade pode causar o surgimento de um risco e traduzir-se numa redução de valor para a empresa.

Neste capítulo será desenvolvido o tema sobre a gestão de risco, nomeadamente definições existentes na literatura, principais características e modelos de gestão de risco.

2.2 Gestão de risco

2.2.1 Definição

Todas as organizações enfrentam uma variedade de riscos internos e externos, tanto a nível estratégico como a nível operacional. Cada risco tem uma probabilidade de ocorrência e um impacto de maior ou menor intensidade. As organizações devem identificar e avaliar sistematicamente estes riscos tentando gerir os mesmos através da implementação de medidas apropriadas de prevenção e contingência. Assim, o processo de gestão de risco tem como objectivo minimizar o risco de um determinado evento a um nível aceitável em termos da probabilidade de ocorrência e do impacto das suas consequências.

O conceito de gestão de risco como sendo um conjunto de meios utilizados na identificação, avaliação e relato do risco empresarial surgiu nos Estados Unidos da América e foi referido pela primeira vez num artigo publicado no *Harvard Business Review* no ano de 1956. No entanto, só no final do século XX é que a gestão de risco foi considerada como um elemento importante e essencial na gestão empresarial passando a fazer parte das boas práticas de gestão e apoiando a tomada de decisão. Beja (2004)

Diversas são as definições que encontramos na literatura. Algumas dessas definições são apresentadas de seguida.

O COSO ERM (2004) define gestão de risco de uma organização como um processo desenvolvido pelo conselho de administração, órgãos de gestão e outros elementos e que deve abranger toda a organização, aplicada na definição da estratégia a seguir pela organização. O processo de gestão de risco deve ser projectado para identificar eventos potenciais que possam afectar a entidade e que permita gerir o risco dentro do apetite de risco definido, isto é o risco que podem ou querem suportar, de forma a proporcionar uma garantia razoável quanto à obtenção dos objectivos definidos pela entidade, nomeadamente a criação de valor.

Para a FERMA (2003) “a gestão de risco deve ser um processo contínuo e em constante desenvolvimento, aplicado à estratégia da organização e à implementação dessa mesma

estratégia. Deve analisar metodicamente todos os riscos inerentes às actividades passadas, presentes e, em especial, futuras de uma organização".

A gestão de risco, de acordo com o Instituto de Gestão de Risco (IRM) de Londres, conforme citação de Willsher (2007, p. 45), "é o processo que pretende ajudar as organizações a compreender, avaliar e actuar sobre todos os seus riscos, para aumentar a probabilidade de sucesso e reduzir a de fracasso".

Em 2005 Belmiro Azevedo numa intervenção proferida no *Risk Management Forum* 2005 da FERMA, afirmou que a gestão de risco envolve um conjunto muito diversificado de actividades e acções, que vão desde as que se relacionam com os riscos dos negócios até às que dizem respeito aos riscos dos processos operacionais da empresa. Defendeu que esta gestão deve ser integrada e unificadora dado que as decisões tomadas por uma determinada área para reduzir os seus riscos poderão criar ou ser aumentados noutra área.

De acordo com Beja (2004) a gestão de risco significa tomar acções correctivas para mudar a probabilidade de ocorrência dos riscos de forma a aumentar a probabilidade de ocorrência de resultados positivos e diminuir as de resultados negativos. Para a alcançar essa meta a gestão de riscos deve adoptar como estratégias de decisão a prevenção, a criação, a compra ou venda, a diversificação, a concentração e compensação e o impulsionamento dos riscos.

Matyjewicz & D´Arcangelo (2004) refere que a gestão de risco é um processo estruturado, consistente e contínuo ao longo de toda a organização para identificar, avaliar e reportar internamente as oportunidades e ameaças que afectam a realização dos objectivos da organização.

Segundo Banham (2004) a principal diferença entre o processo de gestão de risco e as outras formas tradicionais de gestão de risco é que o processo de gestão de risco adopta uma perspectiva que coordena a gestão de risco ao longo de toda a organização em vez de cada área da organização gerir os seus próprios riscos.

Para Funston (2003) a gestão de risco é um processo de transformação que altera a forma como as organizações gerem o risco, permitindo-lhes avaliar os riscos de forma continuada e identificar as medidas a tomar e os recursos a alocar na mitigação do risco.

De acordo com Fuente & Vega (2003) o conceito de gestão de risco vem representar um avanço na centralização da função de riscos, pois o que se pretende é integrar a gestão especializada dos diversos riscos numa única visão que abarque todas as interdependências, ou seja as correlações dos diferentes riscos com o objectivo de agregar o risco total da organização num único número e construir a partir desse número uma única estratégia de cobertura.

Para Zárate (2001) esta nova abordagem constitui uma ferramenta de gestão moderna, fundamental para a implementação de uma cultura orientada para a criação de valor para o accionista que dinamiza a gestão e proporciona novos elementos para a tomada de decisões.

Diversos são os autores que descreveram o processo de gestão de risco mas, no essencial, todas as definições tem a ideia subjacente de que as organizações que implementem processos de gestão de risco terão uma maior probabilidade de sucesso na identificação e controlo da ocorrência e tratamento dos riscos de impacto potencialmente negativo e de tirar vantagens e oportunidades dos riscos potencialmente positivos, tendo como principal objectivo a criação de valor.

2.2.2 Modelos de gestão de risco

Dada a importância e a necessidade de controlar os riscos que afectam as organizações, cada vez mais complexos, abrangentes e universais, há iniciativas mundiais no sentido de tentar padronizar orientações/directrizes sobre gestão de risco de forma a garantir a uniformização de conceitos, processos para implementação de gestão de riscos, estrutura organizacional e objectivos da gestão de risco.

Actualmente existem várias metodologias de gestão de risco, entre as quais se destaca:

- ✓ Norma de Gestão de Riscos da FERMA: Risk Management Standard emitida em 2002 pela Federation of European Risk Management Associations;
- ✓ Norma de Gestão de Riscos Australiana AS/NZS 4360 (2004) - Risk Management Guidelines;
- ✓ Gestão de Risco Empresarial: ERM – Enterprise Risk Management Framework, emitido pelo COSO em 2004;e
- ✓ ISO 31000 da International Organization for Standardization emitida em 2009.

Contudo, vamo-nos focar em alguns dos modelos que consideramos mais relevantes e actuais, nomeadamente o COSO ERM (2004) e a ISO 31000 (2009).

2.2.2.1 COSO Enterprise Risk Management - Integrated Framework

2.2.2.1.1 Referências históricas

Em 2004, para satisfazer as necessidades decorrentes de uma preocupação e focalização crescentes na gestão de riscos, o COSO emitiu um modelo integrado de gestão de risco (ERM – Enterprise Risk Management), desenvolvido pela PWC, sob a sua supervisão, e que incorpora dentro de si o modelo de controlo interno COSO de 1992, permitindo que as

organizações adoptassem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno progredindo para um processo de gestão de risco.

O modelo de gestão de risco proposto pelo COSO ERM é apresentado como um modelo de referência, não só a nível internacional como também a nível nacional. Esta metodologia caracteriza-se por ser abrangente e completa, por ser a metodologia mais divulgada e reconhecida internacionalmente e a mais utilizada pelos profissionais de auditoria.

2.2.2.1.2 Definição e principais características

O modelo COSO ERM define gestão de riscos como parte integrante do controlo interno e preconiza a agregação dos riscos e uma visão global dos mesmos a partir do topo, ao contrário de muitas organizações que procedem à gestão do risco ao nível da subdivisão. O risco, interno e/ou externo à organização, deve ser parte relevante para a determinação da estratégia da entidade para alcançar os seus objectivos. O controlo interno é também parte desse processo em que as estruturas de controlo e os procedimentos internos são essenciais para garantir que estes objectivos sejam alcançados.

Segundo Castanheira e Rodrigues (2006) a visão tradicional do risco tem vindo a sofrer alterações e a ganhar novas formas começando a dar cada vez maior importância ao conceito de gestão de risco. Assim, a abordagem tradicional do risco que assentava numa gestão informal e descentralizada onde cada área da organização gere os seus próprios riscos torna-se cada vez menos frequente.

Este modelo é gerado a partir da ideia de risco em vez da de controlo interno. Neste sentido, desenvolve de forma sistemática todos os aspectos relevantes para uma gestão de risco Pereira (2007).

O COSO ERM é uma estrutura que pretende ajudar as organizações a perceber o que é o risco, de que modo é que ele está presente na empresa e de que forma ele pode afectar adversamente os objectivos estratégicos da organização e a criação de valor. É pois um guia prático de fácil aplicação e é desenhado de modo a identificar determinados acontecimentos que possam afectar a organização. Destina-se a identificar, avaliar e gerir o risco de modo a fornecer uma segurança razoável quanto à realização dos objectivos da organização (COSO, 2004).

O COSO ERM acredita que esta abordagem deve ser incorporada na gestão estratégica e nos processos de gestão da empresa e deve englobar aspectos mais amplos do controlo interno e não apenas aqueles que directamente estão relacionados com o relato financeiro.

O ponto-chave deste modelo refere que os responsáveis pela gestão devem adoptar uma abordagem baseada no risco para avaliação do controlo interno relativamente à sua eficácia. O

modelo deverá ser avaliado e implementado em toda a organização, partindo de um nível mais elevado (entidade) até chegar ao nível mais básico (actividades). Face às incertezas e diversidade de riscos que as organizações enfrentam os desafios colocados à gestão são o de determinar qual é o nível de incerteza que a empresa está preparada para aceitar e quais os riscos que enfrentam de modo a identificá-los, mensurá-los e prioritizá-los. Com base neste estudo a gestão irá definir uma estratégia que permita controlar, partilhar ou transferir e/ou diversificar ou evitar os riscos conforme a possibilidade de reacção e de estratégia da empresa.

Dada a relação entre risco e controlo interno o objectivo principal do controlo interno é auxiliar a gerir e a controlar o risco a que as organizações estão expostas e não de o eliminar, assumindo, por isso, um papel importante no auxílio à gestão e controlo do risco, na medida que pode transformar os riscos em oportunidades. Um bom sistema de controlo interno dependerá, então, de uma avaliação cuidada e regular da natureza e da dimensão dos riscos a que a empresa está exposta.

2.2.2.1.3 Modelo COSO ERM

Segundo o COSO (2004) toda a estrutura de gestão de risco é definida com o fim de alcançar os objectivos de uma organização que são classificados em quatro categorias, nomeadamente os objectivos estratégicos, operacionais, relato e conformidade.

O COSO ERM acrescenta relativamente ao COSO de 1992 mais uma categoria de objectivos, designada de objectivos estratégicos que operam a um nível superior em relação aos outros objectivos e que resultam da missão ou visão da organização com as quais deveriam estar alinhados os objectivos operacionais, de informação e de conformidade e inclui também o conceito de apetite ao risco e tolerância ao risco. Este conceito define o nível de apetite ao risco tolerado pela empresa no sentido de lhe incrementar valor, ou seja a empresa deverá quantificar o risco que está disposta a aceitar para assim perseguir um determinado objectivo

De modo a proporcionar uma segurança razoável de que os objectivos são alcançados o COSO ERM identifica oito componentes relacionados entre si, designadamente ambiente interno, fixação de objectivos, identificação de eventos, avaliação do risco, mitigação dos riscos, actividades de controlo, informação e comunicação e acompanhamento, e que permitem um efectivo processo de gestão de risco. A associação destes componentes complementam o modo como a gestão conduz a empresa e permitem compreender se a gestão do risco é eficaz.

Segundo Castanheira (2007, p.20) o processo de gestão de risco empresarial " inicia-se com a identificação e priorização numa base consistente de todos os riscos enfrentados pela organização. Numa segunda fase, segue-se a avaliação e mitigação dos principais riscos, sendo que os mesmos devem ser priorizados atendendo à sua probabilidade, ao valor actual do seu impacto e à qualidade dos controlos já implementados. Por último, o passo final no

processo de ERM é a monitorização contínua dos riscos, quer sejam novos ou quer sejam os já previamente identificados nas fases do processo de ERM".

Este modelo acrescenta três novos componentes em relação ao modelo de 1992, nomeadamente a definição de objectivos, a identificação dos eventos e a resposta aos riscos.

Existe uma relação directa entre objectivos, que são as metas a alcançar pelas organizações, e componentes de gestão de risco, que são os meios necessários para atingir esses objectivos. Esta relação é representada através de uma matriz tridimensional, conforme é exemplificado na figura a seguir:

Figura n.º 2 – Cubo COSO - ERM

Fonte: Adaptado COSO (2004)

A definição de objectivos aplica-se quando a gestão possui uma estratégia de gestão de risco na determinação dos objectivos a alcançar pela empresa. Para isso deverá determinar o seu apetite pelo risco, isto é, uma visão de alto nível sobre qual o nível de risco que a gestão e a administração estão dispostas a aceitar para criar valor. A tolerância ao risco será o nível aceitável de variação em volta dos objectivos alinhados com o apetite pelo risco.

A identificação de eventos distingue riscos e oportunidades e identifica os factores internos e externos com capacidade de influenciar a estratégia e os seus objectivos. Os factores externos compreendem a conjuntura económica/financeira, factores sociais, políticos, tecnológicos e de natureza ambiental. Os factores internos estão ligados às infra-estruturas, aos activos humanos, aos processos de trabalho e à tecnologia aplicada. Os eventos que possam ter impacto negativo representam riscos. Os eventos que possam ter um impacto positivo representam oportunidades, que a gestão deve ter em conta na definição da estratégia.

Funston (2003) refere que o processo de gestão de risco inicia-se com a avaliação do ambiente em que a organização opera, a sua estratégia para alcançar os objectivos, a cultura da organização e o apetite de risco. Nessa medida, conhecer o ambiente externo em que opera a organização, conhecer os objectivos e a estratégia do negócio é um passo essencial para conhecer as condições do negócio e a natureza dos riscos que a organização está sujeita.

O processo de gestão de risco inicia-se com a identificação e priorização, numa base consistente, de todos os riscos enfrentados pela organização. De seguida, segue-se a avaliação e mitigação dos principais riscos a que a organização está sujeita, sendo que os mesmos devem ser priorizados atendendo à sua probabilidade, ao valor actual do seu impacto e à qualidade dos controlos já implementados. A resposta ao risco é o processo de desenvolver e determinar acções para mitigar os riscos, reduzindo as ameaças que podem afectar os objectivos da organização. A administração avalia a probabilidade e o impacto da ocorrência do risco, os custos e benefícios das medidas tomadas para minimizar o risco potencial, a prioridade das acções a implementar e selecciona a resposta que melhor se adequa aos limites de tolerância do risco aceite. Na resposta aos riscos, depois de identificados e avaliados, a gestão deve preparar respostas que permitam evitar o risco, reduzir o risco, partilhar o risco ou aceitar o risco. A fase final do processo de gestão de risco é a monitorização contínua dos riscos, quer sejam novos ou já previamente identificados.

Na opinião de Mandel (2003) para que o processo de gestão de risco seja verdadeiramente efectivo deve focalizar-se nos assuntos internos e externos e nos processos, minimizar a complexidade, desenvolver um modelo que indique claramente quem é responsável pela gestão de risco e quem controla o processo de implementação e, finalmente, visualizar o processo em sistemas horizontais e verticais.

A gestão de riscos permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas a que as entidades estão sujeitas na sua actividade, focando-se nos riscos cujo impacto seja maior, quer sejam positivos ou negativos, com o objectivo de criar valor para os accionistas.

Muitas empresas começam a reconhecer a necessidade de implementar processos de gestão de risco, na medida que verificam que a introdução de uma forte cultura de gestão de risco na organização pode melhorar a eficácia da gestão de risco. No entanto, verifica-se nem todos os sectores de actividade apresentam o mesmo nível de maturidade de gestão de risco sendo as empresas financeiras e seguradoras, face à natureza dos riscos e à regulação a que estão sujeitas, aquelas que apresentam níveis de maturidade de gestão de risco mais avançados. Para Zárate (2001) a gestão de riscos só tem um nível aceitável de desenvolvimento nas áreas financeiras e seguradoras. Nos restantes sectores, a gestão de riscos reduz-se, basicamente, a uma cobertura daqueles riscos relacionados com a responsabilidade ou com a integridade dos activos.

2.2.2.1.4 Críticas ao normativo COSO ERM

Diversos têm sido os apoios e as críticas que o normativo COSO ERM tem recebido ao longo dos últimos anos. Nesse período foram apontadas várias deficiências técnicas à norma. Alguns dos aspectos positivos e negativos a apontar são os seguintes:

A aplicação do modelo COSO ERM nas organizações permitirá obter aos seguintes benefícios:

- ✓ A harmonização internacional dos processos de gestão de riscos, proporcionando os princípios e orientações genéricas sobre a sua aplicação;
- ✓ A identificação dos riscos das organizações;
- ✓ A responsabilização dos riscos;
- ✓ A visualização integral dos riscos da organização;
- ✓ A eficiência através da adopção de medidas de acções correctivas.

Quanto às limitações inerentes à aplicação deste modelo podemos enumerar:

- ✓ A subjectividade inerente ao processo de tomada de decisões pode enviesar as respostas aos riscos;
- ✓ Uma efectiva gestão de riscos apenas proporcionará uma segurança razoável à administração e ao conselho de administração quanto ao cumprimento dos objectivos da organização;
- ✓ Deve-se avaliar a relação custo/benefício relativa à implementação de controlos ou de acções correctivas;
- ✓ O risco de acontecimentos negativos poder ocorrer causados por erros ou omissões humanos que, quando agregados, podem tornar-se significativos;
- ✓ O risco dos processos de controlo interno poderem ser contornados pelo conluio;
- ✓ O risco da gestão ter a possibilidade e a capacidade de ignorar as decisões da organização em termos de gestão de risco.

Segundo o IIA (2004) o COSO ERM pode contribuir e ajudar a organização a gerir os riscos de modo a atingir os objectivos. Os seus benefícios incluem:

- ✓ Maior probabilidade de atingir esses objectivos;
- ✓ Relatórios consolidados sobre os diferentes riscos;
- ✓ Melhor compreensão dos principais riscos e das suas implicações;
- ✓ Identificação e partilha de riscos do negócio;
- ✓ Maior foco da gestão em questões que realmente importam;
- ✓ Menos surpresas ou crises;
- ✓ Maior foco e concentração em fazer as coisas certas da maneira mais correcta;
- ✓ Aumenta a probabilidade de as novas iniciativas serem alcançadas;
- ✓ Capacidade de assumir um maior risco para obter uma maior recompensa; e
- ✓ Maior informação sobre os riscos e a tomada de decisão.

Grant Purdy presidiu ao comité que desenvolveu a Norma de Gestão de Riscos Australiana AS/NZS 4360 (2004) - *Risk Management Guidelines* e em um inquérito feito num congresso sobre Risco, realizada em Agosto de 2010 pelo IIA, falou sobre os méritos (na maior parte das falhas) do *Management Framework COSO Enterprise Risk*. Purdy acredita que este modelo

tem uma série de pontos positivos mas no geral é um modelo complexo e difícil de implementar. Segundo Purdy algumas das falhas encontradas e que transformam o processo em algo deficiente e ineficaz são:

- ✓ O modelo centra-se principalmente no ambiente interno. Os factores externos são referidos mas o normativo não reflecte a influência que o ambiente de negócios, as condições regulamentares e as partes interessadas externas têm sobre os riscos que a organização enfrenta, sua cultura organizacional, e como influenciam o apetite pelo risco e a priorização do tratamento do risco;
- ✓ As partes interessadas, especialmente as externas, não são mencionadas no normativo e os seus objectivos e influência nas decisões sobre a definição de níveis e tipos de risco são omissos;
- ✓ Os riscos são descritos como eventos e estes são definidos como ocorrências súbitas. Não há apreciação das circunstâncias em se verifica as mudanças lentas e que poderão dar origem a alguns dos riscos mais críticos;
- ✓ A norma mede o risco em termos de probabilidade de um evento ocorrer e apenas no que diz respeito às suas consequências típicas. No entanto, nem sempre as consequências são as esperadas. Cada consequência poderá ter uma probabilidade diferente de ocorrer;
- ✓ Ao longo da norma o termo "probabilidade de risco" é usado, mas o risco não tem uma probabilidade. Os riscos não acontecem quando os eventos ocorrem mas quando estabelecemos objectivos. Se não houver objectivos então não existem riscos;
- ✓ Os riscos estão principalmente associados a perdas e os tratamentos sugeridos no modelo apenas incluem a redução da probabilidade e gravidade das perdas. O documento não é maduro o suficiente para apreciar e explicar que o risco é apenas o efeito da incerteza e que os resultados podem ser benéficos, prejudiciais ou ambos;
- ✓ A forma como é descrita a respostas aos riscos, actividades de controlo e monitorização é confusa e desconcertante;
- ✓ O apetite pelo risco ou tolerância ao risco é tratado de uma forma mecanicista e ingénua. A ideia transmitida de que antes de se fazer uma avaliação do risco é possível determinar qual o nível de risco aceitável é idealizado, irreal, sendo o custo/benefício a única maneira de fazer essa avaliação;
- ✓ O modelo confunde e mistura a estrutura (as estruturas organizacionais, políticas e mecanismos criados para promover, integrar e melhorar a gestão de risco) com o processo utilizado para a gestão de risco, nomeadamente quanto à avaliação de risco, tratamento de riscos e monitorização e revisão.

Nesse mesmo congresso também Arnold Schanfield, membro do Conselho Consultivo do IIA, apontou algumas críticas à norma, nomeadamente:

- ✓ Não há a mínima atenção às partes interessadas externas e às suas necessidades e/ou expectativas. O COSO ERM parece estar voltado principalmente para o público interno, mas as partes interessadas externas são fundamentais;
- ✓ O COSO ERM confunde processo de gestão de risco com estrutura de gestão de risco, facto que explica a difícil compreensão e aplicação da norma;
- ✓ A norma refere os riscos cuja evolução é rápida e discrimina os riscos considerados mais lentos em evolução, como por exemplo as mudanças demográficas da população;
- ✓ O risco é associado a um aspecto negativo cuja ocorrência trará desvantagens não sendo dada grande relevância aos riscos que poderão ser positivos, nomeadamente em oportunidades de negócios inexplorados ou ascendentes.

2.2.2.2 ISO 31000 Risk Management - Principles and Guidelines on Implementation

2.2.2.2.1 Referência histórica

A ISO 31000, publicada em 2009, é a mais recente norma internacional sobre gestão de riscos e foi elaborada pela *International Organization for Standardization*[10]. Esta norma teve como base a norma AS/NZS 4360 (2004) e foi desenvolvida por uma comissão composta por delegações de 35 países que se uniram para criar um grupo de trabalho multidisciplinar designado *ISO Technical Management Board on Risk Management* e que abrangeu especialistas em gestão de risco de diversas áreas, como a financeira, segurança, qualidade, meio ambiente, tecnologia, saúde, defesa, seguros, entre outros. O trabalho obtido não representa apenas as conclusões desta comissão mas as opiniões e experiências de centenas de profissionais envolvidos em gestão de risco.

A necessidade de se criar uma norma internacional específica para a gestão de riscos resultou do facto de a ISO ter constatado que existiam diversos grupos de trabalho que desenvolviam normas e procedimentos sobre gestão de risco e que utilizavam conceitos, terminologias, processos e pressupostos diferentes, criando muitas inconsistências e ambiguidades entre os diferentes normativos. Com base nessa informação foi criada a ISO 31000 com o objectivo de integrar e padronizar todos esses conceitos, terminologias, regulamentação e *frameworks* anteriormente publicados, através de um processo consistente e uma estrutura abrangente, e de estabelecer os princípios e orientações genéricas sobre a estrutura e a implementação de

[10] Foi também publicado a ISO Guia 73 (2009) com vocabulário e conceitos sobre gestão de risco, que complementa a ISO 31000. Trata-se de uma norma cujo objectivo foi a padronização de terminologias da área de gestão de riscos, através da criação de uma linguagem comum, definindo vocabulário, terminologia e conceitos genéricos que se aplicam a todas as áreas e todos os sectores.
Em Dezembro de 2009 foi publicada a nova norma internacional ISO/IEC 31010 (2009) - Gestão de Riscos - Técnicas de Avaliação de Riscos e que é uma norma de apoio à ISO 31000 (2009), fornecendo orientação detalhada sobre a selecção e aplicação de técnicas sistemáticas de avaliação de riscos.

um sistema de gestão de risco de forma a ajudar as organizações a gerir o risco de forma eficaz, eficiente e coerentemente.

2.2.2.2.2 Principais características

A norma ISO 31000 recomenda as organizações a desenvolver, implementar e melhorar continuamente um sistema de gestão de risco como uma componente integral do seu sistema de gestão. Nesse sentido, a norma pode ser adoptada por todo o tipo de organizações e dimensões, qualquer que seja o sector de actividade em que está inserida, e pode ser aplicada a toda a organização e para uma ampla gama de actividades, processos, funções, projectos, produtos, serviços, activos, operações e decisões. Trata-se, portanto, de uma norma abrangente e que tem como principal objectivo ajudar os responsáveis no desenvolvimento de políticas de gestão de riscos das organizações a assegurar que os riscos são eficazmente geridos. A norma vem assim ajudar as organizações a desenvolver, programar e melhorar continuamente uma estrutura com a finalidade de integrar o processo de gestão de riscos no governo, na estratégia, na gestão, nos processos e na cultura de toda a organização.

A utilização de princípios e normas comuns entre as diversas áreas ou departamentos das empresas nos processos de gestão de riscos traz ganhos significativos para a empresa. Nesse sentido, a ISO 31000 foi desenvolvida para auxiliar as organizações a:

- ✓ Aumentar a probabilidade de atingir os objectivos;
- ✓ Incentivar a gestão pró-ativa;
- ✓ Consciencializar da necessidade de identificar e tratar o risco em toda a organização;
- ✓ Melhorar a identificação de oportunidades e ameaças;
- ✓ Cumprir os requisitos legais e regulamentares e as normas internacionais;
- ✓ Melhorar o reporte da informação financeira;
- ✓ Melhorar a governação;
- ✓ Melhorar a confiança dos *stakeholders*;
- ✓ Estabelecer uma base confiável para a tomada de decisão e planeamento;
- ✓ Melhorar os controlos;
- ✓ Utilizar eficazmente recursos para tratamento de riscos;
- ✓ Melhorar a eficácia e a eficiência operacional;
- ✓ Melhorar o desempenho em segurança e protecção ambiental;
- ✓ Melhorar a prevenção de perdas e a gestão de incidentes;
- ✓ Minimizar as perdas;
- ✓ Melhorar a aprendizagem organizacional;
- ✓ Melhorar a capacidade de superar as adversidades organizacionais.

A implementação de um processo de gestão de risco bem sucedida, baseado na ISO 31000, permitirá ajudar as organizações a cumprir normativos e requisitos legais, a estabelecer uma maior confiança no planeamento e na tomada de decisões assim como no uso adequado dos recursos, no aumento da consciencialização sobre a necessidade de identificar e tratar os riscos a que a organização está sujeita e melhorar a identificação de oportunidades e ameaças, os controlos, a eficácia operacional e a eficiência.

A ISO 31000 recomenda a adopção de processos consistentes dentro de uma estrutura própria para análise e gestão integrada dos riscos de uma organização, exigindo-se que as empresas procurem internamente harmonizar seus padrões, políticas e directrizes relacionadas com a gestão de riscos, criando uma única concepção holística na gestão dos mesmos. Isto permite a optimização de tempo e de recursos e a criação de valor para a organização.

A inovação desta norma é a inclusão de princípios de gestão e da ênfase que é dada ao risco. O risco é definido como o efeito da incerteza sobre os objectivos e não apenas como um evento. Cada organização tem objectivos estratégicos, tácticos e operacionais para alcançar e para isso vai ter de saber gerir o efeito da incerteza sobre os objectivos.

2.2.2.2.3 Críticas à norma ISO 31000

Apesar de todos os esforços feitos para que a norma fosse completa e clara e abrangesse todo o tipo de riscos e organizações há sempre oportunidades para a melhoria e aperfeiçoamento. A necessidade mais premente, no entanto, é o de desenvolver algumas orientações práticas sobre a aplicação da norma ISO.

Foi estabelecido que dois anos após a publicação da ISO 31000 se iria proceder a uma revisão da norma de forma a corrigir eventuais incongruências e falhas entretanto detectadas. Essa revisão está a ser precedida por uma pesquisa internacional aos diversos grupos de gestão de risco mundiais, que se efectuou entre Outubro e Novembro de 2011, de forma a conhecer-se a opinião e as preocupações dessas comunidades relativamente à ISO 31000. O objectivo do estudo, a publicar em 2013, é avaliar como a ISO 31000 é vista pelos profissionais de gestão risco e dar um contributo para a elaboração da futura ISO 31004.

Segundo Purdy (2010) os temas que necessitam de revisão são:

- ✓ Os conceitos de apetite ao risco e tolerância ao risco são confusos e ambíguos, não havendo uma clara definição dos dois termos nem a evidência da diferença entre eles;
- ✓ Ficou por responder a questão sobre até que ponto o tratamento do risco deve continuar quando se atinge algum critério de risco definido ou quando a relação custo/benefício é benéfica mesmo para os riscos com menor probabilidade de ocorrência e se deve haver lugar a um tratamento de risco adicional;

- ✓ Embora a descrição da gestão do risco, existente na cláusula 4 da norma, ser bastante sucinta há alguns elementos que poderiam ser simplificados para que a estrutura e a sua implementação se tornasse mais compreensível, mais simples e menos onerosa para as organizações mais pequenas.

Leitch (2010) fez uma análise às fraquezas e pontos fortes constantes da norma ISO 31000. Segundo ao autor a norma tem como fraquezas:

- ✓ Não ser clara, na medida que usa terminologia e definições complexas, ambíguas, pouco claras e compreensíveis;
- ✓ O risco é também definido como podendo ser uma potencial surpresa agradável, no entanto a norma é descrita como se apenas potenciais surpresas desagradáveis fossem aí compreendidas e só sugere tratamentos para os riscos negativos;
- ✓ Algumas das orientações levam a decisões ilógicas;
- ✓ A norma inclui alguns requisitos idealistas que, seguidos literalmente, são impossíveis de cumprir;
- ✓ As orientações não têm uma base matemática, nomeadamente quanto a probabilidades, tratamentos de dados ou modelos.

Relativamente aos aspectos positivos da norma o autor identifica os seguintes:

- ✓ A norma salienta, repetidamente, a importância de a gestão de risco fazer parte integrante do processo de gestão, a todos os níveis da organização, embora não forneça orientações específicas sobre a forma como se processa essa integração;
- ✓ A norma destaca a importância de se considerar a interdependência dos diferentes riscos e das suas origens;
- ✓ A norma afirma que a análise de risco pode ser tomada para diferentes níveis de detalhe, dependendo do risco;
- ✓ A organização deve considerar e divulgar a confiança nas avaliações de risco efectuadas.

Embora a norma não seja perfeita, a publicação da ISO 31000 e da Guia 73 representa um avanço muito significativo na harmonização de políticas de gestão de risco, principalmente no que se refere a uma maior coerência nas definições e processos com vista a uma maior confiança nas decisões tomadas e à condução de melhores decisões.

2.2.2.3 Diferenças entre o COSO ERM e a ISO 31000

A ISO 31000 e o COSO ERM não são normativos totalmente autónomos. A ISO 31000 é um normativo compatível com o COSO ERM dado que é considerada uma actualização da segunda norma e que reflecte o pensamento actual da gestão de risco internacional. A

diferença principal entre ISO 31000 e COSO ERM está no destaque que é dado à avaliação e gestão de risco. A ISO 31000 está focada nas consequências de um determinado evento ocorrer. Tal é demonstrado através da definição de risco como sendo o "efeito da incerteza sobre os objectivos" definidos pela organização, reconhecendo as oportunidades positivas e as consequências negativas associadas. O COSO ERM centra-se mais nos acontecimentos do que nas suas consequências dado que a definição de risco refere-se a este termo como sendo "a possibilidade de que um evento irá ocorrer e afectar adversamente a realização dos objectivos".

Uma vez que a ISO 31000 é uma norma genérica a sua adopção e implementação poderá ser dispendiosa e lenta, dado que as organizações terão ter de fazer um esforço maior para definir sua própria estrutura. Como resultado elas podem encontrar no COSO ERM uma alternativa melhor, embora seja mais normativa e restrita.

Para Preis (2011) as principais diferenças entre COSO ERM e ISO 31000 são:

- ✓ Na ISO o risco é definido como a incerteza sobre os objectivos definidos pela organização enquanto no COSO ERM o risco é definido como o efeito adverso no cumprimento dos objectivos. Isso significa que para o COSO ERM o risco é apenas um desvio negativo enquanto a ISO reconhece que o risco também pode ser algo positivo e gerador de oportunidades para a organização;
- ✓ A ISO define explicitamente o ambiente externo, tornando o seu âmbito mais abrangente e útil em ambientes distintos e abrange uma variedade de *stakeholders,* enquanto o COSO ERM centra-se no contexto interno da organização;
- ✓ De acordo com a revista Risk Management num artigo de 2011 intitulado "*The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework*" a ISO 31000 dá forte ênfase à articulação de riscos e processos de gestão de risco no que concerne aos objectivos estratégicos da organização, políticas de gestão de risco defendendo e exigindo comunicação inter-organizacional e expande a responsabilidade de gestão de risco a toda a organização;
- ✓ A ISO 31000 pode ser usada por qualquer comunidade, organização, grupo, empresa ou individual, já que não há restrições definidas no quadro previsto, enquanto o COSO ERM é mais restrito.

Gjerdrum (2011) identificou algumas diferenças entre o normativo COSO ERM e a ISO 31000. Segundo a autora:

- ✓ O COSO ERM é um normativo complexo e com várias etapas sendo difícil a sua implementação em muitas organizações enquanto a ISO 31000 fornece uma abordagem mais simplificada;

- ✓ A base do modelo COSO ERM é o controlo e a conformidade, o que poderá representar dificuldade na sua adopção e implementação por parte dos gestores de risco tradicionais. A ISO 31000 baseia-se em um processo de gestão, que adaptado ao processo de cada organização, integra-se na gestão e na estratégia da organização;
- ✓ Uma diferença significativa em relação ao tradicional processo COSO ERM é que o modelo ISO inclui os factores de estabelecimento do contexto e institui a contínua comunicação e consulta;
- ✓ Se o normativo COSO ERM for implementado por uma equipa de auditoria interna da organização poderá acontecer que o mesmo seja auditado pelas mesmas pessoas que o desenvolveram e aprovaram. ISO permite uma auditoria independente nas fases de monitorização e revisão;
- ✓ O COSO ERM foi elaborado por auditores, contabilistas e especialistas financeiros enquanto a ISO 31000 foi criada por profissionais de gestão de risco e peritos em normas internacionais.

Em termos de terminologia foram descritas algumas das principais diferenças existentes entre os dois normativos, nomeadamente:

Quadro n.º 1 – Diferenças entre a ISO 31000 e o COSO ERM

Palavras-chave	**ISO 31000**	**COSO ERM *Framework***
Âmbito	A norma fornece princípios e directrizes genéricas sobre gestão de risco. Pode ser usada por qualquer entidade pública, privada ou comunitária, associação, grupo ou individual. Por conseguinte, esta norma não é específica para qualquer actividade ou sector.	A definição é propositadamente ampla. Ela contém os principais conceitos fundamentais para as empresas e outras organizações a gerirem o risco. Centra-se diretamente na realização dos objectivos fixados por uma entidade e proporciona uma base para a definição de gestão de riscos empresariais.
Definição de gestão de risco	Actividades coordenadas para dirigir e controlar uma organização no que respeita ao risco.	É um processo, realizada pela administração de uma organização, gestão e outro pessoal, aplicado na definição da estratégia e a toda a empresa, destinado a identificar potenciais eventos que possam afectar a entidade e gerir o risco dentro de seu apetite pelo risco, de modo a fornecer uma garantia razoável quanto à realização dos objetivos da entidade.
Definição de risco	Efeito da incerteza sobre objectivos.	Possibilidade de um evento ocorrer e afectar adversamente a realização dos objectivos.
Definição de apetite pelo risco	Quantidade e tipo de riscos que uma organização está disposta a prosseguir ou reter.	Quantidade ampla de riscos que uma entidade está disposta a aceitar na prossecução da sua missão ou visão.
Definição de avaliação de risco	Processo global de identificação, análise e avaliação do risco.	Os riscos são analisados em função da sua probabilidade e impacto, como base para determinar a forma como devem ser geridos. Os riscos são avaliados como sendo inerentes ou residuais.

Fonte: Adaptado – Gjerdrum, Dorothy e Peter, Mary, The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework (2011)

Apesar das diferenças apontadas muitos autores consideram existir mais semelhanças do que diferenças entre os dois normativos. Para as organizações com processos de gestão de risco baseados no COSO ERM o conselho dado é compensar as fragilidades que o modelo apresenta com a normativa ISO 31000, nomeadamente quanto à melhoria do desempenho da organização através de uma melhor integração da gestão de risco, da estratégia, do controlo e da governação com vista ao crescimento e rentabilidade da organização.

Capitulo III – Controlo Interno vs Gestão de Risco

3.1 O controlo interno como parte integrante da gestão de risco

Uma das melhores estratégias para se conseguir um bom desempenho empresarial é ter um SCI adequado, forte e eficaz que permita criar e preservar valor e mitigar os riscos a que a organização está sujeita. Nesse sentido, o controlo interno deve ser parte integrante de um sistema de gestão de risco pois só assim é possível conseguir um processo de gestão de risco eficaz e eficiente, tal como refere o normativo COSO ERM.

A implementação de um SCI contribui para uma melhor identificação dos riscos decorrentes de falhas operacionais. As actividades de controlo são constituídas por políticas, procedimentos e práticas desenvolvidas para direccionar especificamente cada controlo a fim de atenuar os riscos previamente identificados e que afectam, de alguma forma, o cumprimento dos objectivos definidos pela organização. Um bom SCI permite a identificação dessas mesmas deficiências minimizando-as ou, se possível, eliminando-as contribuindo para uma melhoria dos procedimentos que consequentemente terão reflexo nos resultados da empresa. Nesse sentido, é cada vez mais crítico que as organizações possuam adequados sistemas de gestão do risco e controlo interno, alinhados entre si e integrados na sua cadeia de valor e nos seus processos de negócio. Assim, um SCI deverá fazer parte da cultura e da gestão da própria empresa permitindo responder com rapidez aos riscos relacionados com o negócio. Um controlo interno eficaz permite criar vantagens competitivas para a organização permitindo-lhe assumir riscos adicionais com vista à criação e preservação de valor.

Nos últimos anos deu-se um maior destaque ao controlo interno como parte integrante da gestão de risco em detrimento de um controlo interno como questão separada e distinta. Por exemplo, os *frameworks* que têm sido publicados sobre estes temas têm colocado mais ênfase na gestão de risco do que sobre o controlo interno. O controlo interno pode ser mais eficaz quando está integrado com a gestão de risco e incorporado em todos os processos de uma organização. A gestão de riscos e controlo interno devem, portanto, ser vistos como duas faces da mesma moeda em que o risco de identificação diz respeito à gestão de ameaças e oportunidades enquanto o sistema de controlo interno é projectado para gerir eficazmente essas ameaças e oportunidades. Existem, no entanto, diversas barreiras à integração destes dois conceitos.

Num projecto publicado pelo IFAC em Dezembro de 2011 intitulado de Orientação Internacional de Boas Práticas - Avaliar e Melhorar o Controlo Interno nas Organizações foi sugerido um novo conceito de controlo interno tendo em conta algumas das sugestões retiradas da Pesquisa Internacional do IFAC sobre Gestão de Riscos e Controlo Interno (2011). Este conceito designa controlo interno como parte integrante da gestão de uma organização e

do sistema de gestão de risco efectuado, compreendido e acompanhado activamente pela administração da organização, gestão e outro pessoal, para explorar as oportunidades e gerir os riscos para atingir os objectivos da organização através de:

- ✓ Eficazes e eficientes processos estratégicos e operacionais;
- ✓ Fornecimento de informações confiáveis para utilizadores internos e externos para a tomada de decisão oportuna e eficaz;
- ✓ Assegurar a conformidade com leis e regulamentos aplicáveis, bem como com as políticas da própria organização, procedimentos e directrizes;
- ✓ Salvaguarda de recursos da organização contra a perda, a fraude, o mau uso e danos; e
- ✓ Salvaguarda da disponibilidade, confidencialidade e integridade dos sistemas de informação da organização.

Em 2007 o IFAC publicou um trabalho realizado por Robert Bruce, jornalista especialista na área financeira. Este trabalho consistiu na realização de entrevistas a dez dos principais profissionais da área da contabilidade a nível mundial acerca das suas experiências e visões sobre controlo interno e gestão de risco. Algumas das opiniões retiradas dessa publicação estão explanadas de seguida.

Para Rob Whiteman, chefe executivo da London Borough of Barking e Dagenham “a gestão de riscos e o controlo interno são parte integrante para o uso eficaz dos recursos e de desempenho”.

John Fraser vice-presidente, auditor interno e director de gestão de risco da empresa Hydro One Inc., a maior empresa de distribuição de electricidade em Ontário, Canadá, refere que o " controlo interno é apenas um meio de obter uma gestão de risco empresarial. O controlo interno é um subconjunto do governo e da gestão de riscos empresariais e (…) é a chave de uma boa gestão”.

James Riley,director financeiro da Jardine Matheson Group, uma das maiores e mais antigas empresas asiáticas de comércio baseada em conglomerados, indica que "o controlo interno é apenas uma das ferramentas disponíveis para gerir o risco e tem um papel central na forma como a organização gere o risco. (…) Em essência, um forte sistema de controlo interno é a chave e faz parte integrante da execução e gestão de um negócio disciplinado e controlado. "

A nível interno o Banco de Portugal, em 2008, decidiu rever os requisitos aplicáveis em matéria de controlo interno às instituições sujeitas à sua supervisão aproximando as orientações existentes sobre controlo interno e gestão de risco. O artigo 3.º do Aviso n.º 5/2008 determina que o sistema de controlo interno deve ter por base um sólido sistema de gestão de riscos, destinado a identificar, avaliar, acompanhar e controlar todos os riscos que possam influenciar

a estratégia e os objectivos definidos pela instituição, que assegure o seu cumprimento e que são tomadas as acções necessárias para responder adequadamente a desvios não desejados.

Apesar da interligação entre controlo interno e gestão de risco as orientações ou directrizes existente actualmente ainda permanecem regulamentadas separadamente. O primeiro passo para o fortalecimento nesta área é combinar essas orientações específicas em um conjunto integrado no sentido de ajudar a aumentar a compreensão geral de que a gestão de risco e o controlo interno são partes integrantes de um sistema de gestão eficaz. Esta foi uma das conclusões a que se chegou do inquérito realizado pelo IFAC sobre gestão de riscos e controlo interno. Este inquérito, cujos resultados foram publicados em Fevereiro de 2011 pelo PAIB, organismo pertencente ao IFAC, e realizado em colaboração com o COSO, teve como objectivo:

- ✓ Identificar os pontos fortes e fracos da gestão de riscos e dos sistemas de controlo interno existentes e praticados a nível mundial;
- ✓ Investigar o papel da gestão de risco e directrizes e/ou orientações de controlo interno; e
- ✓ Determinar a necessidade de convergência internacional entre as várias directrizes e/ou orientações nacionais existentes.

O inquérito *on-line* realizado a nível internacional foi efectuado entre Junho e Agosto de 2010. Obteve-se 604 respostas das quais 586 foram usadas para análise. As respostas recebidas vieram de mais de 80 países, sinal de que a gestão de risco e o controlo interno são temas actuais e bastante importantes dentro das organizações.

Nesse documento podemos observar os resultados obtidos, as análises efectuadas e recomendações propostas. Os resultados obtidos indicam que existe a consciência dos benefícios da implementação de um sistema de gestão de risco, que devem ser criados sistemas de controlo interno e que a gestão de risco e os sistemas de controlo interno devem ser melhor integrados nas organizações.

Segundo os entrevistados as ferramentas e orientação para desenvolver e implementar uma verdadeira integração de gestão de risco e de sistemas de controlo interno não existe realmente. Actualmente, as directrizes de gestão de risco estão muitas vezes separadas das directrizes de controlo interno. O primeiro passo para o fortalecimento de orientações nesta área, de acordo com os inquiridos, é combinar essas orientações num conjunto integrado permitindo aumentar a compreensão geral de que a gestão de risco e o controlo interno são partes integrantes de um sistema de governação eficaz. Além disso, a grande maioria dos entrevistados acredita que as exigências e orientações sobre gestão de riscos e controlo interno devem estar internacionalmente mais harmonizados. Como muitas organizações têm actividades a nível internacional um alinhamento internacional beneficiaria as suas operações

e processos de conformidade, permitindo a comparação destes sistemas, aumentando a confiança dos investidores e reduzindo custos.

Há um claro apelo para a colaboração entre os órgãos reguladores nacionais e internacionais e associações profissionais para chegarem a um acordo sobre um conjunto integrado de directrizes comuns, princípios básicos, e regulamentos alinhados. Segundo os inquiridos, as limitações identificadas nas orientações/directrizes existentes não são adequadamente discutidas, a nível nacional ou internacional, nem há uma discussão real sobre o alinhamento internacional de gestão de riscos e directrizes de controlo interno.

As principais conclusões obtidas foram os seguintes:

- ✓ A maioria das organizações tem uma gestão de risco e sistemas de controlo interno formais, a maior parte das vezes por exigência de órgãos reguladores e/ou supervisores;
- ✓ A gestão de risco e o sistema de controlo interno estão geralmente separados, apesar de a grande maioria dos entrevistados acreditar que eles deveriam estar mais integradas;
- ✓ A importância dada pelas organizações à gestão de risco e ao controlo interno tem aumentado, em comparação com os resultados obtidos em estudos anteriores, assim como a preocupação de integrar gestão de risco e controlo interno;
- ✓ Existe uma clara diferença dos responsáveis pela gestão de risco e pelo controlo interno. O responsável pela gestão de risco é, na maioria das vezes, um especialista em gestão de risco ou alguém da administração enquanto o responsável pelo controlo interno pode ser o auditor interno ou o responsável financeiro e/ou contabilístico;
- ✓ Deve ser dada uma maior ênfase aos benefícios obtidos da implementação de uma gestão de riscos e de sistemas de controlo interno, sendo que estes sistemas devem ser melhor integrados na governação estratégia e operacional da organização, abrangendo todos os principais processos organizacionais;
- ✓ Devido à crise financeira global verifica-se uma maior atenção à integração da gestão de risco com o controlo interno, comparando com dados de há dois anos atrás;
- ✓ Em média, os entrevistados estão bastante satisfeitos com o actual grau de alinhamento das suas directrizes nacionais sobre gestão de riscos e controlo interno com as directrizes internacionais.
- ✓ A grande maioria dos inquiridos acredita que um maior alinhamento internacional entre directrizes de gestão de risco e de controlo interno seria benéfico, pois uma gestão de risco e de controlo interno mais consistente a nível global permitiria um tratamento mais equitativo e uma maior facilidade em criar negócios em diferentes países;
- ✓ A grande maioria dos inquiridos acredita que se verificou um aumento do interesse dos *stakeholders* internacionais e/ou o processo de normalização internacional melhorou

devido a um maior alinhamento internacional entre as várias orientações sobre gestão de risco e/ou controlo interno existentes.

Relativamente às recomendações propostas, e segundo os inquiridos, os organismos de normalização nacionais e internacionais, as associações profissionais e as entidades reguladoras devem colaborar de forma a:

- ✓ Identificar as principais semelhanças e diferenças entre os vários normativos e/ou orientações;
- ✓ Compilar normativos e/ou orientações sobre gestão de riscos e de controlo interno; e
- ✓ Considerar os benefícios de uma maior integração e normalização internacional de regulamentos e orientações na área de governo das sociedades, gestão de riscos e controlo interno.

É também referido que estes organismos deveriam pedir a colaboração dos diferentes *stakeholders* de modo a compreenderem melhor os procedimentos de gestão de risco, os processos de controlo interno e as perspectivas quanto ao impacto da sua implementação nas organizações.

Os inquiridos gostariam que se criasse um organismo internacional de forma a reunir os princípios gerais ou comuns existentes quanto à gestão de risco e controlo interno de modo a avançar com o alinhamento e consequente normalização internacional. Como resultado da normalização as directrizes nacionais já existentes poderiam ser melhoradas ou modificadas em função circunstâncias específicas nacionais mas atendendo aos princípios de um quadro internacional.

A conclusão principal do inquérito realizado é que a normalização internacional traz benefícios potenciais mas ainda é um objectivo ambicioso e desafiador. Todos os responsáveis pelo desenvolvimento, implementação, utilização e aplicação dos requisitos e orientações sobre gestão de risco e controlo interno devem trabalhar em conjunto para promover um reconhecimento internacional.

3.2 O papel da auditoria interna no processo de controlo interno e de gestão de risco

Tradicionalmente, a auditoria interna foi concebida para ajudar as organizações a garantir a confiabilidade e integridade das informações financeiras e operacionais, a salvaguardar dos seus activos, a eficiência e eficácia das operações e o cumprimento das leis, regulamentos, políticas, procedimentos e contratos. Mais recentemente, a auditoria interna evoluiu para englobar auditoria operacional, controlo interno, avaliação de risco, garantia de serviços de tecnologias de informação, entre outros. Este crescente papel tem aumentado a importância da

auditoria interna nas organizações, nomeadamente no controlo de gestão (Widener e Selto, 1999) ou na gestão de riscos (Spira e Page, 2003), como citado em Speklé (2007).

Face à crescente importância atribuída ao papel da auditoria interna no processo de gestão de risco, o IIA veio clarificar a sua posição acerca do papel da auditoria interna nas organizações com processos de gestão de risco. De acordo com o IIA (2004) "o principal papel da auditoria interna no processo de gestão de risco é fornecer segurança objectiva acerca da eficácia das actividades de gestão de risco das organizações, contribuir para assegurar que os principais riscos do negócio estão a ser geridos de forma apropriada e que os sistemas de controlo interno estão a funcionar eficazmente."

Num projecto publicado pelo COSO em Dezembro de 2011 e denominado de *Internal Control – Integrated Framework* é referido que o âmbito de aplicação da auditoria interna inclui a supervisão, a gestão de riscos e o controlo interno, auxiliando as organizações em manter o controlo eficaz, avaliar a sua eficácia e eficiência e promover a melhoria contínua das suas operações.

Conforme referido pela FERMA (2003) a função de Auditoria Interna pode incluir alguns ou todos os seguintes aspectos:

- ✓ Focar o seu trabalho nos principais riscos do negócio, identificados pela gestão da organização e efectuar auditorias aos processos de gestão de riscos implementados;
- ✓ Garantir que a gestão de riscos é eficaz e apoiar no processo de gestão de riscos da organização;
- ✓ Possibilitar a identificação/avaliação de riscos e promover formação sobre gestão de riscos e controlo interno aos colaboradores;
- ✓ Gerir a comunicação de riscos que é efectuada ao Conselho de Administração, ao Comité de Auditoria, entre outros órgãos.

Merkley e Miccolis (2002) referem um estudo que concluiu que os responsáveis por liderar o processo de gestão de risco são, regra geral, provenientes da área de auditoria interna. O mesmo estudo revela que em cerca de 32% das respostas obtidas a auditoria interna estava envolvida nas equipas de trabalho responsáveis pela gestão de risco.

Também Walker *et al*. (2003) aponta um estudo realizado acerca do papel da auditoria interna no processo de gestão de risco em cinco organizações de topo (FirstEnergy Corp., General Motors Corp., WalMart Stores Inc., Unocal Corp. e Canadá Post Corp.) que implementaram com sucesso processos de gestão de risco concluíram que a função de auditoria interna estava extremamente envolvida no processo de gestão de risco.

É cada vez mais crítico que as organizações possuam adequados sistemas de gestão do risco e controlo interno, alinhados entre si e integrados na sua cadeia de valor e nos seus processos

de negócio. A auditoria interna assume aqui um importante papel no sentido de avaliar a adequação e eficácia dos controlos, promovendo a melhoria contínua dos processos e auxiliando a organização a criar valor para os seus accionistas. Assim, a auditoria interna passou a ter uma atitude mais pró-activa e menos preocupada com factos passados e assumiu uma maior responsabilidade na análise, avaliação e controlo dos riscos e do controlo interno das organizações. Pode, por isso, dar um apoio importante à gestão na medida em que garante uma correcta identificação e avaliação dos riscos na organização, garante que os processos de gestão de risco e de controlo interno são adequados e funcionam de forma eficaz, garante a eficácia dos controlos e identifica a necessidades de melhoria ou de alteração dos controlos.

Capitulo IV – Estudo Empírico

Este trabalho de investigação pretende analisar em que medida as empresas portuguesas, nomeadamente as empresas sedeadas na Área Metropolitana do Porto, tem implementado SCI e de gestão de risco nas suas organizações. Para se efectuar esta análise realizou-se um questionário baseado nos princípios preconizados no COSO ERM e distribuiu-se por uma amostra considerada diversificada.

4.1 Metodologia

Segundo o dicionário de língua portuguesa metodologia é um conjunto de regras ou princípios empregados no ensino de uma ciência ou arte, parte da lógica que estuda os métodos das diversas ciências ou arte de dirigir o espírito na investigação da verdade.

É através da metodologia que se estuda, descreve e explica os procedimentos adoptados nas diversas etapas de um trabalho de pesquisa.

É comum encontrar-se autores que não diferenciam os termos "metodologia", métodos" e "técnicas". Todos eles são termos usados para designar os diversos meios que auxiliam e orientam o investigador na sua pesquisa.

Kaplan,1998, como citado por Coutinho, 2011, p. 22 afirma:

> "A metodologia preocupa-se com as técnicas e princípios que designarei por métodos. Os métodos são técnicas suficientemente gerais para serem comuns às diferentes ciências ou uma parte significativa delas (…) Incluem procedimentos como formar conceitos e hipóteses, fazer observações e medidas, descrever protocolos experimentais, construir modelos e teorias (…) A metodologia, por seu lado, procura descrever e analisar os métodos, alertar para os seus limites e recursos, clarificar os pressupostos e consequências, relatar as suas potencialidades nas zonas obscuras das fronteiras do conhecimento (…) Convida (a metodologia) a uma especulação sobre a ciência e o sentido prático da filosofia. Em suma, o objectivo da metodologia é ajudar-nos a compreender, no sentido mais amplo do termo, não os resultados do método científico mas o próprio processo em si."

4.1.1 Metodologia de Investigação

Segundo Ryan et al., (2002 como citado por Ferreira, 2009, p. 13) a selecção da metodologia de investigação depende do fenómeno a investigar. Isto significa que para que a metodologia de investigação escolhida seja adequada ao estudo a realizar esta deve responder aos objectivos da investigação.

A metodologia de investigação pode ser classificada segundo uma perspectiva qualitativa ou quantitativa.

Na investigação qualitativa o investigador tem como objectivo estudar e explicar a forma como os fenómenos sociais são concebidos, constituídos, interpretados e compreendidos.

Na investigação quantitativa a pesquisa centra-se na análise de factos e fenómenos observáveis e na medição/avaliação de variáveis comportamentais e/ou sócio-afectivas passíveis de serem medidas, comparadas e/ou relacionadas no decurso do processo da investigação empírica (Coutinho, 2011). Na investigação quantitativa a informação recolhida para posterior análise deverá ser exacta, fiável, válida e completa.

Do ponto de vista metodológico a investigação qualitativa baseia-se no método indutivo enquanto a investigação quantitativa constrói-se a partir de um modelo hipotético-dedutivo.

Enquanto a investigação qualitativa estuda fenómenos sociais a investigação quantitativa estuda fenómenos naturais.

Os investigadores que conduzem investigação qualitativa partilham a ideia de que estes métodos podem proporcionar uma compreensão mais profunda dos fenómenos sociais do que aquela obtida pelos métodos usualmente adoptados na investigação quantitativa. A investigação qualitativa adopta uma orientação holística, permitindo compreender, interpretar e explicar em profundidade as práticas sociais. (…)Toda a investigação quantitativa e qualitativa é baseada em pressupostos acerca do que constitui investigação válida e que métodos de investigação são apropriados(Ferreira, 2009).

A utilização de mais do que um método é possível e muitas vezes usual numa investigação. A conjugação de métodos pode ser muito relevante, dado que possibilita a triangulação da informação, permitindo identificar, explorar e compreender as diferentes dimensões do estudo, reforçando os resultados obtidos na investigação e enriquecendo as suas interpretações, mas nem sempre se apresenta oportuno ou mesmo exequível o seu uso.

A investigação qualitativa fornece ao investigador informação mais rica, detalhada e contextualizada que normalmente a investigação quantitativa é incapaz de fornecer. (…) Para um investigador qualitativo o processo de análise dos elementos recolhidos não se baseia no domínio de técnicas estatísticas[11], mas sim na sua capacidade em analisar a evidência seguindo procedimentos mais ou menos estabelecidos e em articulá-los com a teoria adoptada no estudo (Ferreira, 2009).

[11] Na investigação quantitativa o domínio de técnicas estatísticas é suficiente para conferir ordem e sentido à evidência recolhida

4.1.2 Fontes de Informação

Quando se faz a revisão da literatura relativamente a um tema que será objecto de estudo há que procurar fontes de informação para se situar o estudo no contexto e, com isso, estabelecer um vínculo entre o conhecimento existente sobre o tema e o problema que se pretende investigar.

As fontes de informação podem classificar-se como fontes primárias e fontes secundárias.

As fontes primárias são artigos originais e relatórios de investigação em que o autor comunica directamente ao leitor o que foi o seu estudo, que metodologia e/ou métodos utilizou, que resultados chegou (Coutinho, 2011). Estas fontes podem ser qualitativas, quantitativas e mistas e normalmente constam de bases de dados.

As fontes secundárias são aquelas que constam de publicações levadas a cabo por outros autores/investigadores. Estas publicações podem ter a forma de monografias, enciclopédias, manuais, artigos, revisões bibliográficas, livros, entre outras. Numa fase inicial de revisão de literatura é importante a consulta de fontes secundárias dado que permitem formar uma visão geral sobre o tema a estudar. No entanto, há que ter cuidado com a informação que se recolhe através destas fontes uma vez que esta pode estar desactualizada e/ou incompleta.

4.2 Recolha de dados

O estudo envolve a aplicação de um inquérito por questionário, destinado aos auditores internos das empresas ou, na sua falta, aos membros da gestão, junto de empresas sedeadas na Área Metropolitana do Porto cujo volume de negócios em 2011 ascenda a 10.000.000 de euros e com um número médio de trabalhadores superior a 200, tendo como objectivo analisar e avaliar os procedimentos e mecanismos de controlo interno e de gestão de risco nestas organizações. As duas variáveis usadas para determinar a amostra vão de encontro a dois dos três parâmetros de medida enunciados pelo artigo 262º do Código das Sociedades Comerciais Português, nomeadamente o volume de negócios e o número médio de trabalhadores.

Para determinar a população solicitamos a colaboração da empresa Informa D&B Serviços de Gestão de Empresas, Sociedade Unipessoal, Lda. que nos forneceu uma listagem das entidades que se enquadravam no âmbito da nossa análise, totalizando 142 empresas. Destas 142 empresas 19,7% são empresas sedeadas no concelho do Porto, 16,2% são empresas sedeadas nos concelhos da Maia e de Matosinhos e 18,3% no concelho de Vila Nova de Gaia. Estes quatro concelhos representam mais de 70% da nossa população. Relativamente às actividades económicas desenvolvidas por estas empresas verificou-se uma diversidade bastante grande, sendo que 47,68% são empresas industriais, 33,10% são empresas prestadoras de serviços e 19,01% são empresas ligadas ao comércio. Das 142 empresas 9

tem como actividade a fabricação de componentes e acessórios para veículos automóveis, 7 de comércio de veículos automóveis ligeiros e de actividades de prática médica de clínica especializada em ambulatório, 5 de comércio a retalho de vestuário para adultos e de transporte rodoviário de mercadorias, 4 de restauração sem serviço de mesa e com 3 empresas cada temos as actividades de engenharia e técnicas afins, de construção de edifícios e de fabricação de chapas, folhas, tubos e perfis plásticos. Estas 9 actividades representam 32,17% da população. Outras 20 actividades representam 27,97% da nossa população com actividades tão diversificadas que vão desde o transporte interurbano em autocarros, a edição de jornais, actividades de limpeza, produção de vinhos comuns e licorosos, hotéis com restaurante, entre outras. As restantes 56 actividades representam 39,86% da população.

No total o questionário foi enviado às 142 empresas que constituem a população tendo sido obtidos 30 questionários válidos. Numa primeira fase, os questionários foram enviados por correio tendo sido dirigidos para o órgão de gestão ou para o departamento de auditoria interna das empresas. De forma a se conseguir um elevado índice de respostas, os questionários faziam-se acompanhar de uma carta de apresentação do estudo, assinada pela autora e que sensibilizava os inquiridos para a importância da colaboração dos mesmos no preenchimento do questionário. Um mês e meio após o envio do questionário, e dada a reduzida quantidade de respostas, optou-se por enviar o inquérito por correio electrónico e contactar telefonicamente as empresas cujos questionários remetidos ainda não tínhamos recebido, sensibilizando-as para a importância da colaboração das mesmas. A maioria das empresas justificou a ausência de respostas por falta de tempo. Após esta 2.ª tentativa, e ao fim de mais três meses, o número de respostas aumentaram para 30. Obteve-se, assim, uma amostra constituída por 30 empresas o que representa uma percentagem de respostas válidas de 21,13%.

4.3 Hipóteses de investigação

Através da literatura revista pareceu-nos haver evidência, nomeadamente através de Zárate (2001), de que o sector financeiro e segurador apresenta uma maior maturidade na gestão de risco em relação aos outros sectores de actividade, principalmente devido às exigências impostas por órgãos reguladores. A nossa investigação vai no sentido de analisar quais os sectores de actividade que evidenciam terem implementado processos de gestão de risco e de controlo interno. Também iremos analisar se há uma maior propensão para as empresas do sector industrial terem implementado ou estarem a implementar sistemas de gestão de risco e de controlo interno em relação às empresas prestadoras de serviços e de comércio.

Estudos revelam que os responsáveis por liderar os processos de gestão de risco são, em regra, provenientes da área de auditoria interna (Merkley & Miccolis, 2002) e que, normalmente, a auditoria interna está extremamente envolvida na implementação e

acompanhamento dos processos de gestão de risco (Walker *et al*., 2003). Neste sentido pretendemos analisar se as empresas objecto de estudo possuem um departamento de auditoria interna e se, por conseguinte, têm implementado sistemas de controlo interno e de gestão de risco.

Para o COSO (2004) a gestão de risco é da responsabilidade da administração ou gestão de uma organização e não da auditoria interna. Segundo o IIA (2004) o principal papel da auditoria interna no processo de gestão de risco é fornecer segurança objectiva acerca da eficácia das actividades de gestão de risco das organizações, contribuir para assegurar que os principais riscos do negócio estão a ser geridos de forma apropriada e que os sistemas de controlo interno estão a funcionar eficazmente. Nesse sentido iremos analisar se, na opinião dos inquiridos, o órgão responsável por estruturar e implementar um processo de gestão de risco e de controlo interno será a administração ou a auditoria interna.

De acordo com Beja (2004) a gestão de risco significa tomar acções correctivas para mudar a probabilidade de ocorrência dos riscos de forma a aumentar a probabilidade de ocorrência de resultados positivos e diminuir a de resultados negativos. Já Funston (2003) refere que a gestão de risco é um processo de transformação que altera a forma como as organizações gerem o risco, permitindo-lhes avaliar os riscos de forma continuada e identificar as medidas a tomar e os recursos a alocar na mitigação do risco.

Do exposto formulamos as seguintes hipóteses de investigação:

H1 – A proporção de empresas com processos de gestão de risco implementados difere de sector de actividade (Zárate, 2001).

H2 – As empresas que possuem auditoria interna têm probabilidade de terem sistemas de controlo interno e de gestão de riscos implementados (Merkley & Miccolis, 2002) e (Walker *et al*., 2003).

H3 – A auditoria interna poderá ser o órgão responsável por estruturar e implementar um processo de gestão de risco e de controlo interno (COSO, 2004) e (IIA, 2004).

H4 – A auditoria interna poderá ter apenas um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno (COSO, 2004) e (IIA, 2004).

H5 – Os riscos a que a organização está exposta são analisados e reavaliados continuamente e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos (Beja, 2004) e (Funston, 2003).

Face às hipóteses formuladas foi elaborado um questionário[12] (apêndice 1). O questionário foi estruturado em quatro secções com perguntas, na sua maioria, fechadas. Esta opção de recolha de informação impossibilita o inquirido de emitir opinião sobre as perguntas, apenas sendo-lhe permitido seleccionar a sua escolha dentro das opções dadas. Em algumas questões foi dada ao inquirido a possibilidade de emitir opiniões e sugestões com o objectivo de que a informação recolhida melhor caracterizasse essa organização.

As questões formuladas inserem-se em quatro secções distintas. A primeira pretende fazer uma caracterização da amostra, nomeadamente quanto à actividade económica, capital social detido por empresas internacionais, volume de negócios e existência de auditoria interna dentro da organização. A segunda secção tem como objectivo analisar a mostra relativamente ao sistema de controlo interno. Nesse sentido pretende-se verificar se as empresas elaboraram um manual de controlo interno, se têm implementados meios de controlo interno e qual a sua percepção e conhecimento sobre este tema. Na terceira secção do questionário insere-se questões que têm por objectivo saber se as empresas que compõem a amostra conhecem os riscos que enfrentam, se tem um processo de gestão de risco implementado, e quais as vantagens daí resultantes, e qual o papel da auditoria interna na avaliação e supervisão de um processo de gestão de risco. Nas duas secções anteriores é dada a possibilidade do inquirido caracterizar melhor a sua organização, tendo-lhe sido permitido acrescentar informação complementar às opções dadas pelo inquiridor sobre os meios de controlo interno e de gestão de risco existentes na organização e expressar a sua opinião sobre estes dois temas. A quarta secção analisa a percepção do inquirido sobre a relação entre controlo interno e gestão de risco.

Para responder às hipóteses formuladas foram inquiridas as seguintes perguntas:

Hipóteses Formuladas		**Perguntas Inquiridas**
1) A proporção de empresas com processos de gestão de risco implementados difere de sector de actividade.	⟹	Qual é a actividade económica da sua empresa? Que meios de controlo interno existem na sua organização? A empresa tem implementado um processo formal de gestão de risco?

[12] Um questionário é um conjunto variável de perguntas consistentes, devidamente estruturadas e direccionadas para os objectivos da investigação para serem respondidos pelos indivíduos de uma amostra ou população.
A opção por se realizar um questionário para recolha de informação tem como vantagens a sua natureza impessoal, a sua apresentação uniformizada, a ordem idêntica de questões e as mesmas directrizes para todos os inquiridos, o que permite a análise de dados através da utilização de métodos estatísticos, uma maior facilidade na leitura dos resultados, a codificação das respostas, a comparação das respostas obtidas e uma menor probabilidade de se efectuar uma interpretação ambígua e subjectiva da informação recolhida.

2) As empresas que possuem auditoria interna têm probabilidade de terem sistemas de controlo interno e de gestão de riscos implementados.	⇨	A empresa possui um departamento de auditoria interna? Que meios de controlo interno existem na sua organização? A empresa tem implementado um processo formal de gestão de risco?
3) A auditoria interna poderá ser o órgão responsável por estruturar e implementar um processo de gestão de risco e de controlo interno. 4) A auditoria interna poderá ter apenas um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno.	⇨	A auditoria interna poderá ser o órgão responsável por estruturar e implementar um processo de gestão de risco e de controlo interno? A auditoria interna poderá ter um papel estratégico na avaliação e supervisão de um processo de gestão de risco de uma organização? A auditoria interna poderá ter apenas um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno? O órgão de gestão deverá ser o responsável pelo planeamento, implementação e supervisão do sistema de controlo interno? Os processos de gestão de risco são acompanhados pela gestão de modo a garantir que as respostas e as acções desenvolvidas para controlar ou eliminar os riscos são eficazes e estão em linha com os objectivos da organização?
5) Os riscos a que a organização está exposta são analisados e reavaliados continuamente e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos.	⇨	A empresa tem compreensão exacta e abrangente dos riscos que actualmente enfrenta? Periodicamente são analisados e reavaliados os riscos a que a organização está exposta e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos? A avaliação da eficácia dos controlos e o seu ajustamento deverão ser feitos periodicamente?

4.4 Análise dos resultados obtidos

4.4.1 Introdução

Neste capítulo pretendemos apresentar os resultados obtidos no estudo realizado. Assim, após a formulação das hipóteses e a recolha dos dados, procedemos à análise estatística, de forma a validar as hipóteses que servem de suporte para as conclusões finais.

4.4.1.1 Caracterização da amostra

Para começar a análise do estudo efectuado iremos caracterizar as empresas que compõe a amostra segundo o CAE rev.3 (3 dígitos)[13], conforme apresentado o quadro n.º 2.

Quadro n.º 2 – Caracterização da amostra consoante o CAE

CAE	Descrição	N.ª de empresas	%
0'12	Culturas permanentes (Viticultura)	1	3,33%
110	Indústria de bebidas	3	10,00%
152	Indústria de calçado	2	6,67%
162	Fabricação de artigos de madeira, de cortiça, de espartaria e de cestaria, excepto mobiliário	2	6,67%
222	Fabricação de artigos de matérias plásticas	2	6,67%
233	Fabricação de produtos cerâmicos para a construção	1	3,33%
251	Fabricação de elementos de construção em metal	1	3,33%
289	Fabricação de outras máquinas e equipamento para uso específico	1	3,33%
293	Fabricação de componentes e acessórios para veículos automóveis	3	10,00%
360	Captação, tratamento e distribuição de água	1	3,33%
464	Comércio por grosso de bens de consumo, excepto alimentares, bebidas e tabaco	2	6,67%
467	Comércio por grosso de combustíveis, metais, materiais de construção, ferragens e outros produtos n. e	1	3,33%
477	Comércio a retalho de outros produtos, em estabelecimentos especializados	1	3,33%
494	Transportes rodoviários de mercadorias e actividades de mudanças	2	6,67%
611	Telecomunicações	1	3,33%
619	Outras actividades de telecomunicações	1	3,33%
620	Consultoria e programação informática e actividades relacionadas	1	3,33%
711	Actividades de arquitectura, de engenharia e técnicas afins	1	3,33%
861	Actividades dos estabelecimentos de saúde com internamento	3	10,00%
	Total	30	100,00%

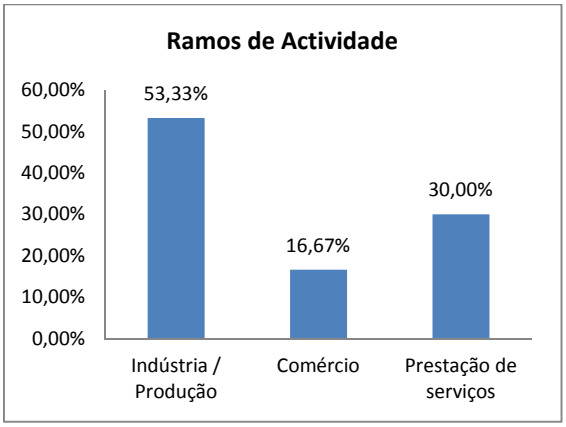
Fonte: Elaboração própria

[13] No apêndice 2 é apresentado de forma mais detalhada os sectores de actividade das empresas representativas da amostra

Analisando o quadro que caracteriza as empresas que integram a amostra verificamos que 30% das empresas tem como actividade económica a indústria de bebidas, a fabricação de componentes e acessórios para veículos automóveis e a prestação de cuidados de saúde. A indústria de calçado, a fabricação de artigos de madeira, a fabricação de materiais plásticos, o comércio por grosso de bens de consumo e o transporte rodoviário de mercadorias representa 33,33% da amostra. Os restantes 46,67% da amostra representam uma diversidade de actividades que engloba a viticultura, a fabricação de produtos cerâmicos de construção, actividades de telecomunicações, actividades de arquitectura e engenharia, entre outros.

Segundo o ramo de actividade a amostra é composta por 53,33% de empresas industriais ou ligadas ao sector produtivo, 30% são empresas prestadoras de serviços e 16,67% são empresa de comércio, conforme se pode visualizar no gráfico n.º 1, complementado com o apêndice 3.

Gráfico n.º 1 – Caracterização da amostra segundo o ramo de actividade



Fonte: Elaboração própria

As empresas cujo volume de negócios obtido em 2011 atingiu um valor inferior ou igual a 50 milhões representam 56,67% da amostra e as que tem um volume de negócios maior que 50 milhões e inferior ou igual a 100 milhões representam 16,67%. A mesma percentagem é obtida nas empresas com um volume de negócios superior a 100 milhões e inferior ou igual a 500 milhões. Por fim, a amostra é composta por 10% de empresas com um volume de negócios superior a 500 milhões. Estas conclusões poderão ser analisadas no quadro n.º 3.

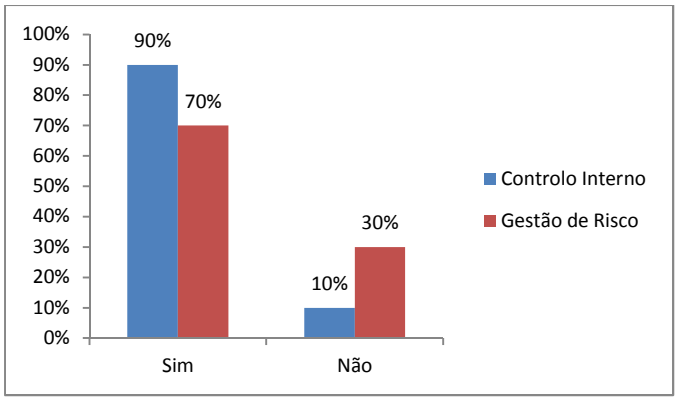
Quadro n.º 3 – Volume de negócios obtido em 2011

Volume de negócios (milhões de euros)	Frequência Absoluta	Frequência Relativa
≤ 50	17	56,67%
>50 e ≤ 100	5	16,67%
>100 e ≤ 500	5	16,67%
>500	3	10,00%
Total	**30**	**100,00%**

Fonte: Elaboração própria

Quanto à existência de um sistema de controlo interno 90% da amostra demonstra ter procedimentos de controlo interno implementados nas suas organizações. Relativamente à existência de processos de gestão de risco apenas 70% das organizações tem implementado processos de gestão de risco. As empresas que não tem um processo de gestão de risco implementado, e que representam 30% da amostra, também não estão a implementar um processo de gestão de risco na sua organização. Estas conclusões podem ser analisadas no gráfico seguinte, complementadas no apêndice 3.

Gráfico n.º 2 – Percentagem de empresas com sistemas de controlo interno e processos de gestão de risco implementados



Fonte: Elaboração própria

4.4.1.2 Análise dos resultados

No ponto 4.3 deste trabalho foram apresentadas as hipóteses subjacentes a este estudo. Após a recolha, tratamento e estudo das hipóteses formuladas iremos concluir acerca da veracidade dessas mesmas hipóteses.

4.4.1.2.1 Variável sector de actividade

No quadro seguinte podemos analisar a existência de sistemas de controlo interno e de gestão de risco por sectores de actividade nas empresas representativas da nossa amostra.

Quadro n.º 4 – Existência de sistemas de controlo interno e de gestão de risco por sectores de actividade

		Sistema de Controlo Interno		Processo de Gestão de Risco	
Sectores de Actividade	**N.º Empresas (%)**	**Sim**	**Não**	**Sim**	**Não**
Agricultura	3%	100%	0%	100%	0%
Indústrias transformadoras	50%	87%	13%	67%	33%
Captação, tratamento e distribuição de água; saneamento, gestão de resíduos e despoluição	3%	100%	0%	100%	0%
Comércio por grosso e a retalho	13%	100%	0%	50%	50%
Transportes e armazenagem	7%	100%	0%	100%	0%
Actividades de informação e de comunicação	10%	67%	33%	67%	33%
Actividades de consultoria, científicas, técnicas e similares	3%	100%	0%	100%	0%
Actividades de saúde humana	10%	100%	0%	67%	33%
Total	100%				

Fonte: Elaboração Própria

Analisando apenas os sectores de actividade com maior expressão na amostra, e que representam 83% do total dos sectores de actividade, verifica-se que nas empresas transformadoras 87% das organizações demonstram ter procedimentos e mecanismos de controlo interno e 67% delas têm processos de gestão de risco implementados. Já no comércio por grosso e a retalho 100% das empresas têm procedimentos de controlo interno mas apenas 50% dessas empresas têm gestão de risco. Relativamente às actividades de informação e comunicação os resultados obtidos indicam que 67% das empresas têm um sistema de controlo interno e a mesma percentagem é obtida quando questionadas sobre a existência de processos de gestão de risco nas suas organizações. Nas empresas cuja actividade é a prestação de cuidados de saúde 100% delas têm procedimentos de controlo interno implementados e 67% têm processos de gestão de risco.

Face aos resultados obtidos, e analisando apenas os sectores com maior expressão na amostra, verifica-se que as indústrias transformadoras, as actividades de informação e comunicação e as empresas prestadoras de cuidados de saúde são as actividades que apresentam uma maior implementação de processos de gestão de risco. Relativamente às empresas que demonstram usar procedimentos e mecanismos de controlo interno como ferramenta de gestão, para além das actividades já referidas, também as empresas de comércio por grosso e a retalho evidenciam possuir procedimentos de controlo interno.

Para analisarmos a existência de sistemas de controlo interno e de gestão de risco por ramos de actividade elaborou-se o seguinte quadro:

Quadro n.º 5 – Existência de sistemas de controlo interno e de gestão de risco por ramos de actividade

Ramo de actividade	N.ª de empresas	Sistema de Controlo Interno		Processo de Gestão de Risco	
		Sim	Não	Sim	Não
Indústria / Produção	16	88%	13%	69%	31%
Comércio	5	100%	0%	60%	40%
Prestação de serviços	9	89%	11%	78%	22%

Fonte: Elaboração Própria

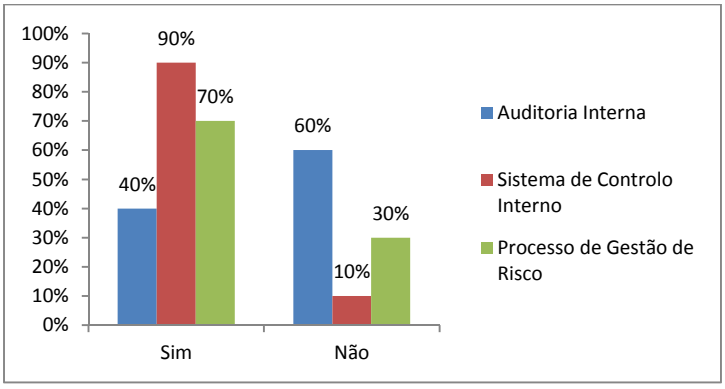
A análise dos dados obtidos mostra que são as empresas prestadoras de serviços que demonstram ter maior implementação de sistemas de controlo interno e de gestão de risco nas suas organizações. Neste ramo de actividade 89% das empresas evidenciam ter implementado um sistema de controlo interno e 78% dessas empresas tem gestão de risco. Em 88% das empresas industriais existe sistemas de controlo interno e apenas 69% dessas empresas tem processos de gestão de risco. Já nas empresas ligadas ao comércio 100% das empresas da amostra evidenciam ter um sistema de controlo interno e apenas 60% dessas empresas tem processos de gestão de risco.

Em conclusão, são as empresas prestadoras de serviços que revelam ter uma maior implementação de processos de gestão de risco nas suas organizações.

4.4.1.2.2 Variável auditoria interna

No gráfico seguinte está representada a relação entre a auditoria interna e existência de processos de gestão de risco e de controlo interno.

Gráfico n.º 3 – Relação entre a existência de auditoria interna e sistema de controlo interno e de gestão de risco

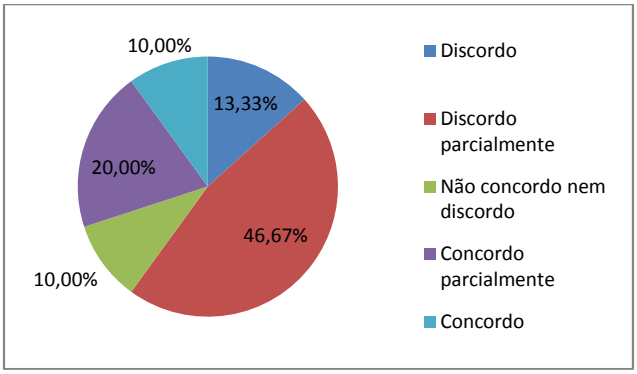


Fonte: Elaboração Própria

Da análise aos resultados obtidos não se evidencia existir uma relação positiva entre a existência de auditoria interna nas empresas e a existência de um sistema de controlo interno e de gestão de risco como ferramenta de gestão. Da amostra obtida 60% das empresas não tinham auditoria interna mas 90% das empresas evidenciavam ter procedimentos de controlo interno e 70% indicaram ter processos de gestão de risco implementados. Verifica-se assim não haver uma relação positiva entre a existência de auditoria interna nas empresas e a existência de processos de controlo interno e de gestão de risco.

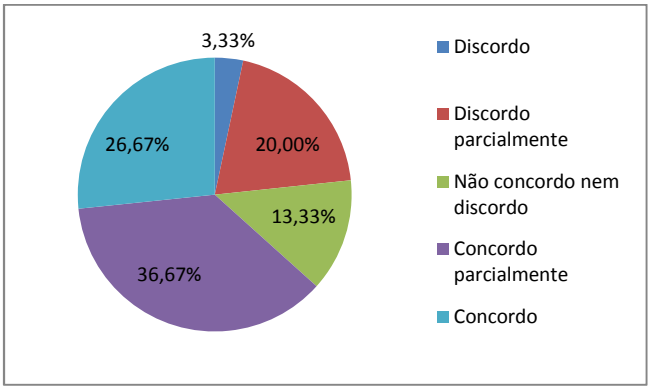
Foram também questionados e analisados itens acerca do órgão responsável pela estruturação e implementação de um processo de gestão de risco e do papel da auditoria interna na supervisão e avaliação de um processo de gestão de risco e de controlo interno. Os resultados são os apresentados nos gráficos n.º 4, 5 e quadro n.º 6.

Gráfico n.º 4 - Auditoria interna como responsável pela estruturação e implementação do processo de gestão de risco



Fonte: Elaboração Própria

Gráfico n.º 5 - Papel da auditoria interna na avaliação e supervisão de um sistema de controlo interno e de gestão de risco



Fonte: Elaboração Própria

Quadro n.º 6 – Papel da auditoria interna na avaliação e supervisão do processo de gestão de risco

Auditoria interna tem um papel estratégico de avaliação e supervisão na gestão de risco	Frequência Absoluta	Frequência Relativa
Sim	28	93,33%
Não	2	6,67%
Total	**30**	**100,00%**

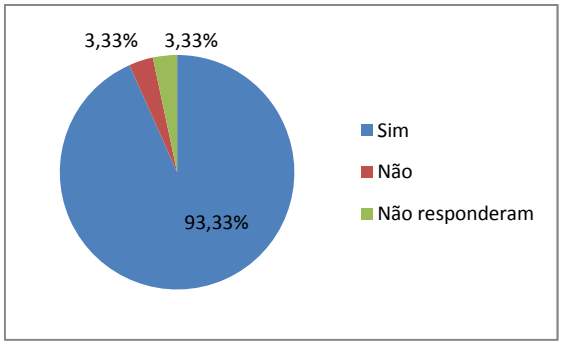
Fonte: Elaboração própria

Dos resultados obtidos verifica-se que 13,33% e 46,67% dos inquiridos discordam ou discordam parcialmente, respectivamente, que a auditoria interna seja o órgão responsável pela estruturação e implementação de um processo de gestão de risco. Apenas 20% concorda parcialmente e só 10% concorda em absoluto com esta afirmação. Os inquiridos que não expressaram opinião constituem 10% das respostas. Em resumo, 60% dos inquiridos não atribuem à auditoria interna a responsabilidade pela estruturação e implementação de um processo de gestão de risco.

Relativamente ao questionado sobre o papel da auditoria interna verificou-se que 36,67% dos inquiridos concordam parcialmente que a auditoria interna deverá ter um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno e que apenas 26,67% concordam com esta asserção. As empresas que discordam ou discordam parcialmente desta questão constituem 23,33% dos resultados. Aqueles que não têm opinião formada representam 13,33% da amostra. Apesar de 63,34% das respostam afirmarem que a auditoria interna deverá ter um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno a existência de auditoria interna nas organizações é pouco significativa dado que apenas 40% dos inquiridos revelaram ter auditoria interna. Quando questionados apenas acerca do papel da auditoria interna no processo de gestão de risco 93,33% os inquiridos revelaram que esta pode ter um papel estratégico na avaliação e supervisão de um processo de gestão de risco de uma organização.

Foi também inquirido se os processos de gestão de risco são acompanhados pela gestão, de modo a garantir que as respostas e as acções desenvolvidas para controlar ou eliminar os riscos são eficazes e estão em linha com os objectivos da organização. Das respostas obtidas 93,33% afirmaram que é a gestão o órgão que acompanha o processo de gestão de risco existente na sua organização, sendo que apenas 3,33% discordaram desta afirmação e outros 3,33% não responderam, conforme representado no gráfico seguinte.

Gráfico n.º 6 – Gestão como responsável por acompanhar processos de gestão de risco



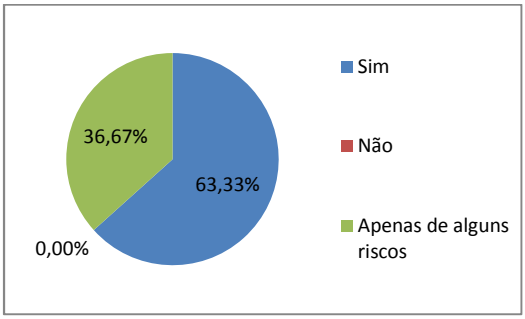
Fonte: Elaboração Própria

Em resumo, 63,34% dos inquiridos concordam que a auditoria interna deverá apenas supervisionar e avaliar o processo de gestão de risco e de controlo interno e 60% discordam que a auditoria interna seja o órgão responsável pela estruturação e implementação de um processo de gestão de risco. Dos resultados obtidos concluiu-se que 93,33% dos inquiridos indicam que é a gestão o órgão que acompanha o processo de gestão de risco existente na sua organização.

4.4.1.2.3 Variável risco

Pretendemos saber se as empresas tinham uma percepção exacta e abrangente dos riscos que actualmente enfrentam e obteve-se os resultados constantes no seguinte gráfico.

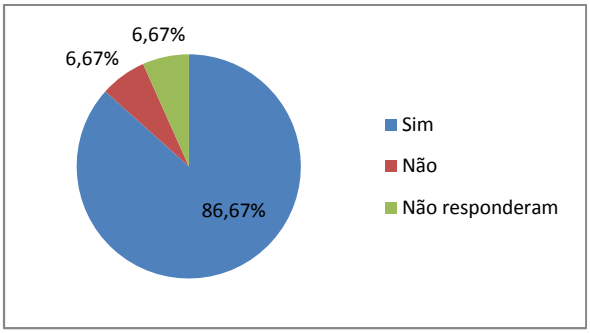
Gráfico n.º 7 – Consciencialização dos riscos que actualmente enfrentam



Fonte: Elaboração Própria

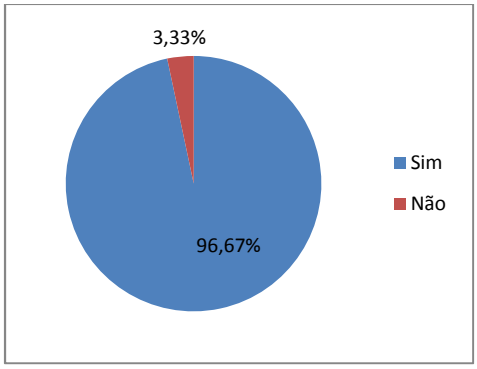
Também pretendíamos analisar se as empresas avaliam periodicamente os riscos a que estão sujeitas e se avaliam a eficácia dos controlos e procediam a ajustamentos, obtendo-se os resultados constantes dos gráficos n.º 8 e 9.

Gráfico n.º 8 – Avaliação periódica dos riscos



Fonte: Elaboração Própria

Gráfico n.º 9 - Avaliação periódica da eficácia dos controlos e seu ajustamento



Fonte: Elaboração Própria

Da análise dos dados obtidos verificamos que apenas 63,33% das empresas afirmam saber os riscos que actualmente estão sujeitas. Desses 63,33% a grande maioria das empresas refere a concorrência, a situação económica e os riscos financeiros do país, a retracção do consumo e a evolução tecnológica como os principais riscos que enfrentam actualmente[14].

A maioria dos inquiridos, cerca de 86,67%, afirmou que periodicamente são analisados e reavaliados os riscos a que a organização está exposta. Os resultados obtidos indicaram também que 96,67% dos inquiridos avaliavam periodicamente a eficácia dos controlos implementados nas suas organizações e procediam a ajustamentos que considerassem relevantes.

Em conclusão, a maioria das empresas conhece os riscos a que estão sujeita e periodicamente faz uma avaliação da eficácia dos controlos assim como analisa e reavalia os riscos a que a organização está exposta e estabelecem medidas que reduzem a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos.

[14] A totalidade das respostas recebidas relativamente a esta questão estão no apêndice 4 pergunta n.º 11

Capitulo V – Conclusão

5.1 Conclusões da revisão da literatura

As inúmeras falências ocorridas nas duas últimas décadas, muitas delas fraudulentas, reforçaram a ideia de que as organizações deveriam implementar sistemas de controlo interno e de gestão de risco. Desde então, foram publicados diversos normativos e linhas de orientação. Enquanto para algumas organizações a adopção destas directrizes são meras opções de gestão para outras existe a obrigatoriedade de implementação e cumprimento de normativos sobre sistemas de controlo interno, nomeadamente empresas, nacionais e estrangeiras, com capitais negociados na Bolsa de Nova Iorque. Estes normativos foram criados para impor regras mais rígidas e abrangentes para a padronização e aperfeiçoamento dos controlos financeiros das empresas.

As organizações que implementaram sistemas de controlo interno e de gestão de risco, mesmo que por imposição legal, reconhecem as vantagens da sua implementação mas também os elevados custos que lhe estão associados. São, no entanto, poucas as organizações que adoptam esta estratégia de gestão por iniciativa própria.

É cada vez mais crítico que as organizações possuam adequados sistemas de gestão do risco e controlo interno, alinhados entre si e integrados na sua cadeia de valor e nos seus processos de negócio. A auditoria interna assume aqui um importante papel no sentido de avaliar a adequação e eficácia dos controlos, promovendo a melhoria contínua dos processos e auxiliando as organizações a criar valor para os seus accionistas.

Os normativos e/ou orientações existentes sobre controlo interno e gestão de risco são diversificados mas, em geral, semelhantes e todos tem como objectivo melhorar a conduta ética nos negócios, a transparência, a credibilidade, a responsabilidade e a integridade das demonstrações financeiras e do relato financeiro perante os *stakeholders*.

Estudos recentemente realizados indicam que ainda há muito trabalho a fazer no sentido de se harmonizar e integrar, a nível mundial, directrizes sobre controlo interno e gestão de risco. Há um claro apelo para a colaboração entre os órgãos reguladores, nacionais e internacionais, e associações profissionais para chegarem a um acordo sobre um conjunto integrado de directrizes, comuns, princípios básicos, e regulamentos. Esta harmonização internacional traria grandes benefícios às organizações. Dado que muitas organizações têm relações e transacções a nível mundial, um alinhamento internacional beneficiaria as suas operações e processos de conformidade, permitindo a comparação destes sistemas, aumentando a confiança dos investidores e reduzindo custos. Prevê-se, portanto, muito trabalho e discussões no sentido da harmonização de normativos internacionais sobre controlo interno e gestão de risco.

Há um longo caminho a percorrer pelas organizações no sentido da sensibilização das empresas para as vantagens da implementação sistemas de controlo interno e de gestão de risco e deste modo fomentar a cultura controlo e de gestão de risco e sensibilizar para a sua importância no seio da gestão.

5.2 Conclusões do estudo

No estudo realizado pretendemos analisar e avaliar em que medida as empresas sedeadas na Área Metropolitana no Porto aplicam procedimentos e mecanismos de controlo interno e de gestão de risco como ferramenta de gestão. Para determinarmos a população foram definidos dois critérios com referência ao ano de 2011, nomeadamente um volume de negócios superior a 10 milhões de euros e um número médio de trabalhadores superior a 200.

Após a definição da amostra verificamos que a sua maioria é constituída por empresas industriais ou ligadas ao sector produtivo, representando 53,33% da amostra, 30% são empresas prestadoras de serviços e 16,67% são empresa de comércio. Uma análise mais detalhada permite verificar que 30% das empresas tem como actividade económica a indústria de bebidas, a fabricação de máquinas e equipamentos e a prestação de cuidados de saúde. A indústria de calçado, a fabricação de artigos de madeira, a fabricação de materiais plásticos, o comércio por grosso de bens de consumo e o transporte rodoviário de mercadorias representa 33,33% da amostra. Os restantes 46,67% da amostra representam uma diversidade de actividades que engloba a viticultura, a fabricação de produtos cerâmicos de construção, actividades de telecomunicações, actividades de arquitectura e engenharia, entre outros.

A amostra é composta por 56,67% de empresas com um volume de negócios inferior ou igual a 50 milhões de euros, 33,34% de empresas com um volume de negócios superior a 50 milhões de euros e inferior ou igual a 500 milhões de euros e 10% de empresas com um volume de negócios superior a 500 milhões de euros.

Quanto à existência de um sistema de controlo interno 90% da amostra demonstra ter procedimentos e mecanismos de controlo interno implementados nas suas organizações mas apenas 70% das organizações têm implementado processos de gestão de risco.

A primeira hipótese colocada pretendeu verificar se a empresas com processos de gestão de risco implementados difere de sector de actividade. Da análise às respostas obtidas nada se pode concluir uma vez que as empresas que representam a amostra têm uma grande diversidade de actividades e do seu enquadramento por sector de actividade obtém-se resultados pouco significativos e que não permitem confirmar esta hipótese.

O estudo efectuado revelou que são as empresas prestadoras de serviços que demonstram ter maior implementação de sistemas de controlo interno e de gestão de risco nas suas organizações. Neste ramo de actividade 89% das empresas evidenciam ter implementado um

sistema de controlo interno e 78% dessas empresas tem gestão de risco. Em 88% das empresas industriais existe sistemas de controlo interno e apenas 69% dessas empresas tem processos de gestão de risco. Já nas empresas ligadas ao comércio 100% das empresas da amostra evidenciam ter um sistema de controlo interno e apenas 60% dessas empresas tem processos de gestão de risco.

Tendo a auditoria interna um papel cada vez mais importante na avaliação e supervisão dos processos de gestão de risco e de controlo interno que as organizações implementam os resultados obtidos no estudo efectuado demonstram não haver uma relação positiva entre a existência de auditoria interna nas empresas e a existência de um sistema de controlo interno e de gestão de risco como ferramentas de gestão. Da amostra obtida 60% das empresas não tinham auditoria interna mas 90% das empresas evidenciavam ter procedimentos de controlo interno e 70% indicaram ter processos de gestão de risco implementados. Face aos resultados obtidos, a hipótese colocada que pretendia averiguar se as empresas que têm auditoria interna têm probabilidade de terem sistemas de controlo interno e de gestão de riscos implementados não se confirmou.

Quando questionadas sobre o papel que a auditoria interna deverá desempenhar 63,34% da amostra é da opinião que a auditoria interna deverá ter um papel de supervisão e avaliação no processo de gestão de risco e de controlo interno. Relativamente ao papel da auditoria interna no processo de gestão de risco 93,33% dos inquiridos revelaram que esta pode ter um papel estratégico na avaliação e supervisão de um processo de gestão de risco de uma organização. Apesar destes resultados existência de auditoria interna nas organizações é pouco significativa dado que apenas 40% das inquiridas revelaram ter auditoria interna.

Um dos pontos essenciais para um eficaz sistema de controlo interno e de gestão de risco é que o órgão de gestão seja o grande impulsionador e responsável pela estruturação e implementação destas duas ferramentas de gestão. Na amostra 60% das empresas concorda que a gestão deverá ser o órgão responsável pela estruturação e implementação de um processo de gestão de risco. Nas empresas que revelaram ter processos de gestão de risco implementados 93,33% afirmaram que é a gestão o órgão que acompanha o processo de gestão de risco existente na sua organização.

Assim, e face às hipóteses colocadas que pretendiam averiguar se a auditoria interna seria o órgão responsável por estruturar e implementar um processo de gestão de risco e de controlo interno ou se teria um papel de supervisão e avaliação, o estudo confirmou que à auditoria interna é atribuído o papel de supervisão e avaliação dos sistemas de controlo interno e de gestão de risco, cabendo à gestão a responsabilidade pela sua estruturação e implementação.

Para que uma organização construa e implemente um processo de gestão de risco eficaz é necessário ter uma percepção exacta e abrangente dos riscos que enfrentam, avaliar periodicamente os riscos a que estão sujeitas, avaliar a eficácia dos controlos implementados e

proceder com regularidade a ajustamentos. Da análise dos dados obtidos verificamos que apenas 63,33% das empresas afirmam saber quais os riscos que actualmente estão sujeitas. Desses 63,33% a grande maioria das empresas refere a concorrência, a situação económica e os riscos financeiros do país, a retracção do consumo e a evolução tecnológica como os principais riscos que enfrentam actualmente. Cerca de 86,67% dos inquiridos afirmaram que periodicamente são analisados e reavaliados os riscos a que a organização está exposta. Os resultados obtidos indicaram também que 96,67% dos inquiridos avaliavam periodicamente a eficácia dos controlos implementados nas suas organizações e procediam a ajustamentos que considerassem relevantes.

Na última hipótese pretendia-se testar a possibilidade das empresas analisarem e reavaliarem continuamente os riscos a que estão expostas e tomarem medidas que reduzam a ocorrência de perdas futuras e/ou potenciem ganhos. A análise efectuada confirmou que as empresas têm consciência da importância da adopção deste tipo de procedimentos e que periodicamente analisam e reavaliam os riscos a que estão expostas e a eficácia dos controlos implementados e, em resultado destas acções, fazem ajustamentos de modo a assegurar uma gestão de risco mais eficaz.

Como conclusão final, o estudo efectuado revela que a maioria das empresas evidenciam ter procedimentos e mecanismos de controlo interno e de gestão de risco, no entanto há ainda um longo caminho a percorrer e diversos pontos a melhorar para que as empresas possam usufruir em pleno dos benefícios desta ferramenta de gestão.

O estudo realizado tem algumas limitações pelo facto de se ter tido pouca receptividade das empresas em responder ao inquérito realizado, apesar dos esforços feitos junto dessas entidades no sentido de evidenciar a importância da sua contribuição na investigação do tema objecto de estudo. Grande parte das empresas revelaram a falta de tempo e a confidencialidade da informação pedida como motivos principais para não colaborarem neste estudo.

5.3 Orientações para investigações futuras

Como sugestão para trabalhos futuros poderíamos propor uma análise focalizada nos sistemas de controlo interno e de gestão de risco para um menor número de sectores de actividade, podendo ter como variáveis a dimensão da empresa e/ou a localização territorial.

Poder-se-ia também propor um estudo mais pormenorizado acerca dos procedimentos de controlo interno e de gestão de risco nas empresas cotadas no Mercado de Valores Mobiliários Português.

Referências Bibliográficas

Alexandre, Túlio (2011). A Integração da Gestão dos Riscos Corporativos. Revista Gestão de Riscos, Edição 63, pp. 34-38

Alves, Ana (2009). A Evolução da Auditoria Interna após a Lei SOX - Impactos indirectos no caso português, pp. 14-43

Auditing Standard nº 5 (2007). An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements, Public Company Accounting Oversight Board

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

Banham, R. (2004). Enterprising views of risk management, Journal of Accountancy, Jun, pp. 65-71

Beasley, Mark S., Clune, Richard e Hermanson, Dana R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Acedido em 2012-09-15 em http://www.sciencedirect.com/science/article/pii/S0278425405000566

Beja, Rui (2004). Risk Management – Gestão, Relato e Auditoria dos Riscos do Negócio; Áreas Editora, S.A.

Benaroch, M (2002). Managing Information Technology Investment Risks: A Real Options Perspective. Journal of Management Information Systems 19 (2), pp.43-84

Borgerth, Vânia Maria da Costa (2007). SOX: entendendo a Lei Sarbanes-Oxley: um caminho para a informação transparente. 1º Ed. São Paulo, Ed. Thomson Learning

Camazano, Magali (2007). Estudo da Influência do "Sarbanes-Oxley Act of 2002" sobre o Gerenciamento do Risco Operacional em Instituições Financeiras Brasileiras

Castanheira, N. (2007). Auditoria Interna Baseada no Risco - Estudo do caso Português

Castanheira, N. e L. L. Rodrigues (2006). Gestão de risco - Da abordagem tradicional à gestão de risco empresarial (ERM). Revista Revisores e Empresas n º 34 de Julho/Setembro de 2006. Lisboa, Revista dos Revisores Oficiais de Contas

Castanheira, N. e L. L. Rodrigues (2009). Factores Associados à Adopção de Abordagens Baseadas no Risco no Processo de Auditoria Interna

Cicco, Francesco e Fantazzini, Mario (2003).Tecnologias consagradas de gestão de riscos, Série Risk Management. Risk Tecnologia Editora Ltda; 2ª Edição Maio

COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control - Integrated Framework - Executive Summary. Acedido em 2012-01-09 em http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf

COSO Gerenciamento de Riscos Corporativos - Estrutura Integrada. Acedido em 2012-01-09 em http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf

Coutinho, Clara Pereira (2011). Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática pp. 21-65

Darlington, A., Grout, S., e Whitworth, J. (2001). How safe is sage enough? An introduction to risk management, presented at: the staple inn actuarial society, p. 3. Acedido em 2012-04-30, em http://www.sias.org.uk/siaspapers/listofpapers/view_paper?id=RiskManagement

Deloitte (2003). Lei Sarbanes-Oxley, Guia para Melhorar a Governança Corporativa Através de Eficazes Controles Internos

Directriz de Revisão/Auditoria n.º 400 (2000). Avaliação do Risco de Revisão/Auditoria, Ordem dos Revisores Oficiais de Contas

Directriz de Revisão/Auditoria n.º 410 (2000). Controlo Interno, Ordem dos Revisores Oficiais de Contas

Doyle, Jeffrey, Ge, Weili, McVay, Sarah (2007). Determinants of Weaknesses in Internal Control Over Financial Reporting. Journal of Accounting and Economics 44. pp. 193–223

Donaldson, William (2003). Testimony Concerning Implementation of the Sarbanes-Oxley Act of 2002 before the Senate Committee on Banking, Housing and Urban Affairs. Acedido em 2012-01-09, em http://www.sec.gov/news/testimony/090903tswhd.htm

Ereira, Sabrina Mota (2007). O relato do risco: Uma Análise no Contexto das Empresas Cotadas na EuronextLisbon

Ferma (2003). Norma de Gestão de Riscos, Federation of European Risk Management Associations

Fernandez, Mariana (2009). O Advento das ISOS da Gestão de Riscos. *Revista Gestão de Riscos, Edição 49/50*, pp. 38-47

Ferreira, Aldónio *et al.*(2009). Contabilidade e Controlo de Gestão – Teoria, Metodologia e Prática, pp. 131-135 e 167-207; Escolar Editora

Ferreira, Albertina (2010). A Gestão de Risco Aplicada à Auditoria Interna. Universidade de Aveiro

Funston, R. (2003). Creating a risk-intelligent organization, The Internal Auditor, April, pp. 59-63

Fuente, L. & Vega, G (2003). "La gestión de riesgos en empresas no financieras", Partida Doble, Diciembre, pp. 54-60

Gjerdrum, Dorothy & Peter, Mary (2011). The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework, pp. 8-12

Gomes, Emília R. (sem data). A Importância do Controlo Interno. Acedido em 2012-01-18, em http://www.jmmsroc.pt/downloads/10anos/11.pdf

Hussein, Haji (2008). E- Commerce e Ressource Centre; Article; *Risk Assessement; Using COBIT® as a Guide Risk Assessement Assurande Services*. Acedido em 2011-12-18 em http://fata86.webs.com/riskassesment.html

IFAC (1999). Enhancing Shareholder Wealth by Better Managing Business Reporting. Acedido em 2012-06-07 em http://devbiz.narod.ru/home/kozloff/PWC/risk_mngmnt99.pdf

IFAC (2006). Internal Controls — A Review of Current Developments Professional Accountants in Business Committee, International Federation of Accountants. Acedido em 2011-12-18, em http://www.ifac.org/sites/default/files/publications/files/internal-controls-a-revie.pdf

IFAC (2007). Internal Control from a Risk-Based Perspective. Acedido em 2011-12-18, em http://www.ifac.org/sites/default/files/publications/files/internal-control-from-a-ris.pdf

IFAC (2011). Evaluating and Improving Internal Control in Organizations. Acedido em 2012-06-07, em https://www.ifac.org/publications-resources/evaluating-and-improving-internal-control-organizations

IIA (2004).The Role of Internal Auditing in Enterprise-wide Risk Management

IIA (2009). Enquadramento Internacional de Práticas Profissionais de Auditoria Interna - Tradução do IPAI Agosto 2009. I. T. I. o. I. Auditors. Lisboa.

IIA ERM Risk Summit (2010).Acedido em 2012-04-30 em http://www.theiia.org/guidance/iia-erm-risk-summit-august-22-2010/

International Standard on Auditing n.º 240 (2009). The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements

International Standard on Auditing n.º 315 (2009). Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment

International Organization for Standardization n.º 31000 (2008). Risk management — Principles and guidelines on implementation

Leitch, Matthew (2010). ISO 31000 (2009) - The New International Standard on Risk Management. Risk Analysis, Vol. 30, No. 6. Acedido em 2012-04-14 em http://web.ebscohost.com/ehost/pdf viewer/pdfviewer?sid=42a785d0-47b0-4db6-9eee-8f0ad4ffd0a5%40 sessionmgr13&vid=2&hid=19

Martins, I., & Morais, G. (2007). Auditoria Interna - Função e Processo. Áreas Editora.

Martins, Paulo, Azevedo, Graça e Inácio, Helena (2010). Análise de Risco da Aplicação da NCRF 12 – Imparidade de Activos e o Papel da Auditoria Interna. Acedido em 2012-03-24 em http://www.aeca.es/xivencuentroaeca/cd/71a.pdf

Mandel, C. E. (2003). COSO gives a good start to implement ERM, Business Insurance, December: p.12

McKay, M. (2007).Sarbanes- Oxley Act - Impact of Law. Acedido em 2012-01-09 em http://www.docstoc.com/docs/4980663/impact-from-sarbanes-oxley-act

Matyjewicz, G. & D´Arcangelo, J.R. (2004), "ERM-based auditing", The Internal Auditor, Nov/Dec, pp 4-18

Merkley, B. W. & Miccolis, J. A. (2002), "Getting left behind", Risk Management, Apr, pp: 28-50

New ISO Standard for Effective Management of Risk. Acedido em 2012-04-09 em http://www.iso.org/iso/pressrelease.htm?refid=Ref1266

QuivY, Raymond e Campenhoudt, LucVan (2005). Manual de Investigação em Ciências Sociais

Pereira, N. (2007). Crescente Relevância dos Sistemas de Controlo Interno e de Governo nas Sociedades Comerciais, Revista de Auditoria Interna, n.º28, Outubro/Dezembro

Pires, Ana Isabel Marinho (2008). Impacto da Lei Sabarnes-Oxley no Sistema de Controlo Interno das Empresas Cotadas nos EUA – O Caso Português

Pires, José Pedro (2010). Contributo da Auditoria Interna na Detecção e Mitigação de Riscos Empresariais

Preis, Armin (2011). ISO Risk Management Process: Information System Design. Acedido em 2012-04-14 em http://www.arminpreis.at/files/2012/ISO-31000-Risk-Management.pdf

Professional Accountants in Business Committee (2011), Global Survey on Risk Management and Internal Control - Results, Analysis, and Proposed Next Steps

Purdy, Grant (2010).ISO 31000:2009—Setting a New Standard for Risk Management. Risk Analysis, Vol. 30, No. 6, 2010. Acedido a 2012-05-01 em http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=61e535c0-2b5a-4a19-bbfd-025411509649%40sessionmgr4&vid=2&hid=19

Quintas, Tiza, T.,Czesnat, Aline O. e Fernandes, Francisco C., Panorama de Boas Práticas em Governança Corporativa: Uma Abordagem sobre a Metodologia de Gerenciamento de Riscos Adotada pelas Empresa Listadas na BOVESPA. Acedido em 2012-01-09 em http://www.ead.fea.usp.br/semead/11semead/resultado/trabalhosPDF/750.pdf

Schreiner, Sérgio Ricardo Silva (2004). Controles internos e governança corporativa: Por que e como uma empresa brasileira deve atender à legislação Sarbanes-Oxley: Estudo de Caso da Perdigão S/A. 2004. 210f. Dissertação (Mestrado em Controladoria e Contabilidade Estratégica) – Centro Universitário Álvares Penteado – UniFecap

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

Silva, A. S., Vitorino, A., Alves, C. F., Cunha, J. A., & Monteiro, M. A. (2006). Livro Branco Sobre o *Corporate Governance* em Portugal. Acedido em 2012-01-09 em http://br.librosintinta.in/biblioteca/ ver-pdf/www.ecgi.org/codes/documents/libro_bianco_cgov_pt.pdf.htx

Silva, Alex S, Satim, Luciana A., Souza, Maria E. A., Silva Roseli F e Henrique, Marcelo R., A (2007). Lei Sarbanes Oxley e seus Efeitos nas Transparências para os Investidores Brasileiros em Empresas S/A. Acedido em 2012-01-09 em http://www.praticacontabil.com/contadorperito/Lei_Sarbanes_Oxley_e_seus_efeitos.pdf

Silva, Cecília (2009). A Importância atribuída pelos Empresários da Grande Lisboa ao Controlo Interno, pp 10-73

Speklé ,Roland F., EltenHilco J. Van, Kruis,Anne-Marie (2007). Sourcing of internal auditing: An empirical study

Walker, P. L., Shenkir, W. G. & Barton, T. L. (2003), “ERM in practice”, The Internal Auditor, Aug, pp. 51-55.

Willsher, Richard (2007), Um negócio arriscado; Revista Exame World Business; Agosto/Setembro/Outubro, pp..42- 47

Zárate, F. C. O (2001). La gestión de riesgos: un enfoque práctico, Partida Doble, Julio-Agosto: 64-76

Apêndices

Apêndice 1 – Questionário

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

O presente questionário realiza-se no âmbito de uma dissertação do Mestrado em Auditoria do Instituto Superior de Contabilidade e Administração do Porto (ISCAP) tendo como propósito analisar qual a percepção e o nível de implementação de Sistemas de Controlo Interno e de Gestão de Risco nas empresas.

O questionário é dirigido aos membros da gestão ou ao departamento de auditoria interna da empresa.

É garantida a confidencialidade da informação fornecida, que irá ser utilizada exclusivamente para a investigação académica que se pretende realizar no âmbito da referida dissertação. A sua colaboração é fundamental para a realização do estudo que se pretende desenvolver, na certeza de que os resultados a obter poderão contribuir para a melhoria da prática de auditoria.

1 – CARACTERIZAÇÃO DA EMPRESA

1. **A que sector de actividade a sua empresa pertence?**

   _____

2. **Qual a percentagem de capital social da sua organização detido por empresas estrangeiras?**

   ☐ 0% ☐ ≤ 20% ☐ > 20% e ≤ 50% ☐ > 50% e ≤ 70% ☐ > 70%

3. **Qual o volume de negócios obtido em 2011 (em milhões de euros)?**

   ☐ ≤ 50 ☐ > 50 e ≤ 100 ☐ > 100 e ≤ 500 ☐ > 500

4. **Em 2011, qual é a percentagem de volume de negócios que a empresa transaccionou para fora do mercado nacional?**

   ☐ ≤ 20% ☐ > 20% e ≤ 50% ☐ > 50% e ≤ 70% ☐ > 70%

5. **A empresa possui um departamento de auditoria interna?**

   ☐ Sim ☐ Não

2 – CONTROLO INTERNO

6. Existe algum manual de Controlo Interno na empresa?

☐ Sim ☐ Não

7. Como descreveria um Sistema de Controlo Interno? (assinale as suas opções)

☐ É um sistema que conduz à eficiência e eficácia das operações

☐ Contribui para a confiança e fiabilidade das demonstrações financeiras

☐ Assegura a conformidade com as leis e regulamentos

☐ Meio de prevenção de erros e/ou procedimentos ilegais ou fraudulentos

☐ Auxilia o processo de gestão

☐ Permite proteger os activos da empresa

☐ A sua implementação gera mais custos que benefícios

☐ A sua implementação não gera vantagens competitivas à empresa

☐ Não é um requisito importante na criação de valor para os seus accionistas

☐ Outras características

_____

(por favor indique quais)

8. Que meios de Controlo Interno existem na sua empresa?

☐ Existência de organigrama contendo responsabilidades definidas, segregação de deveres e funções

☐ Verificação e conferência de registos e realização de conciliações

☐ Definição de autoridade e delegação de responsabilidades

☐ Pessoal qualificado, competente e responsável

☐ Manual de procedimentos, formulários e documentos

☐ Rotatividade e fluxo de entrada e saída de elementos chave à organização

☐ Rotinas de validação

☐ Confronto das contagens de caixa, títulos, activos e existências com os registos contabilísticos

☐ Restrição do acesso físico directo aos activos e registos

☐ Aprovação e controlo de documentos

☐ Comparação de informação com fontes externas de informação

☐ Comparação dos elementos obtidos com os orçamentados

☐ Controlo de contas e balancetes de verificação

☐ Outros

_____

(por favor indique quais)

9. Na sua opinião:	Sim	Não
9.1 Considera o Controlo Interno como uma ferramenta de gestão?	☐	☐
9.2 O órgão de gestão deverá ser o responsável pelo planeamento, instalação e supervisão do Sistema de Controlo Interno?	☐	☐
9.3 A existência de um código de conduta é desnecessária, já que todos os colaboradores sabem quais são as suas tarefas e responsabilidades?	☐	☐
9.4 Um Controlo Interno eficaz pode ajudar os gestores a avaliar e gerir o risco de negócio?	☐	☐
9.5 Um Sistema de Controlo Interno bem construído e operativo significa, por si só, que a empresa esteja imune a situações como a ocorrência de erros, fraudes e irregularidades?	☐	☐
9.6 O Controlo Interno deverá ser extensível e focalizado apenas aos níveis hierárquicos intermédios e baixos da organização?	☐	☐
9.7 A avaliação da eficácia dos controlos e o seu ajustamento deverão ser feitos periodicamente?	☐	☐
9.8 Existem alguns mecanismos de Controlo Interno que gostaria de ver implementados na sua empresa?	☐	☐

Se sim indique quais:_____

3 – GESTÃO DE RISCO

10. A vossa empresa tem implementado um processo formal de Gestão de Risco?

☐ Sim ☐ Não ☐ Está a decorrer o processo de implementação

11. A empresa tem uma compreensão exacta e abrangente dos riscos que actualmente enfrenta?

☐ Sim ☐ Não ☐ Apenas de alguns riscos

Em caso afirmativo, indique 5 dos principais riscos a que a empresa está sujeita:

_____

12. Considera que a auditoria interna pode ter um papel estratégico na avaliação e supervisão de um processo de Gestão de Riscos de uma organização?

☐ **Sim** ☐ **Não**

13. Na sua organização:	Sim	Não
13.1 Assumir riscos é considerado uma estratégia de gestão?	☐	☐
13.2Estão definidos e correctamente implementados controlos que mitiguem eficazmente os riscos identificados na sua empresa, de modo a não colocar em causa a concretização dos objectivos definidos pela gestão?	☐	☐
13.3 Existem meios ou técnicas para identificar potenciais eventos que poderão originar prováveis riscos ou oportunidades?	☐	☐
13.4 Os processos de gestão de risco são acompanhados pela gestão de modo a garantir que as respostas e as acções desenvolvidas para controlar ou eliminar os riscos são eficazes e estão em linha com os objectivos da organização.	☐	☐
13.5 Periodicamente são analisados e reavaliados os riscos a que a organização está exposta e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos.	☐	☐

14. Na sua opinião, quais são as 5 principais vantagens resultantes da implementação de um Processo de Gestão de Risco:

☐ Criação de procedimentos homogéneos de governação

☐ Habilitar a administração a correr riscos apropriados na criação de valor

☐ Maior monitorização da performance

☐ Melhoria da capacidade de relato para organismos reguladores

☐ Melhoria da comunicação com os accionistas e *stakeholders*

☐ Aumento da reputação

☐ Maior clareza no processo de decisão e da cadeia de comando a todos os níveis da organização

☐ Habilitar a administração a pensar de modo empreendedor e inovador

☐ Maior capacidade de atingir objectivos estratégicos

☐ Maior rentabilidade

☐ Outras

_____

(por favor indique quais)

4 – RELAÇÃO ENTRE CONTROLO INTERNO E GESTÃO DE RISCO

Utilizando a seguinte escala, exprima a sua opinião sobre cada um dos aspectos abaixo indicados.

1	2	3	4	5
Discordo	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo

	1	2	3	4	5
1. Um processo de gestão de risco empresarial deverá ser implementado independentemente da existência de um sistema de controlo interno.	○	○	○	○	○
2. Cada departamento de uma organização deverá ter um responsável pelo controlo interno, não cabendo apenas à gestão de topo essa responsabilidade.	○	○	○	○	○
3. A auditoria interna deverá ser o órgão responsável por estruturar e implementar um processo de gestão de risco numa organização.	○	○	○	○	○
4. A auditoria interna deverá ter apenas o papel de supervisão e avaliação num processo de gestão de risco e de controlo interno.	○	○	○	○	○
5. A gestão de riscos relaciona-se com a gestão de ameaças e oportunidades enquanto o sistema de controlo interno é projectado para gerir eficazmente essas ameaças e oportunidades.	○	○	○	○	○
6. O objectivo do controlo interno é o de auxiliar a gerir e a controlar o risco de forma adequada e não de o eliminar.	○	○	○	○	○
7. Um controlo interno eficaz permite criar vantagens competitivas para a organização permitindo-lhe assumir riscos adicionais com vista à criação e preservação de valor para os seus accionistas.	○	○	○	○	○
8. A gestão de risco e o controlo interno não garantem que os objectivos de uma organização sejam todos atingidos, apenas dão uma segurança razoável de que tais objectivos possam ser alcançados.	○	○	○	○	○
9. A existência de fluxos de informação e retorno entre os órgãos de gestão e as unidades operacionais são fundamentais para que a informação chegue, de forma tempestiva e exacta, a todos os colaboradores da empresa.	○	○	○	○	○
10. Um bom sistema de controlo interno é essencial a uma gestão de risco eficiente.	○	○	○	○	○

Apêndice 2 – Caracterização da amostra segundo o CAE

CAE	Descrição	N.º de empresas	%
0'12	Culturas permanentes (Viticultura)	1	3,33%
110	Indústria de bebidas	3	10,00%
152	Indústria de calçado	2	6,67%
162	Fabricação de artigos de madeira, de cortiça, de espartaria e de cestaria, excepto mobiliário	2	6,67%
222	Fabricação de artigos de matérias plásticas	2	6,67%
233	Fabricação de produtos cerâmicos para a construção	1	3,33%
251	Fabricação de elementos de construção em metal	1	3,33%
289	Fabricação de outras máquinas e equipamento para uso específico	1	3,33%
293	Fabricação de componentes e acessórios para veículos automóveis	3	10,00%
360	Captação, tratamento e distribuição de água	1	3,33%
464	Comércio por grosso de bens de consumo, excepto alimentares, bebidas e tabaco	2	6,67%
467	Comércio por grosso de combustíveis, metais, materiais de construção, ferragens e outros produtos n. e	1	3,33%
477	Comércio a retalho de outros produtos, em estabelecimentos especializados	1	3,33%
494	Transportes rodoviários de mercadorias e actividades de mudanças	2	6,67%
611	Telecomunicações	1	3,33%
619	Outras actividades de telecomunicações	1	3,33%
620	Consultoria e programação informática e actividades relacionadas	1	3,33%
711	Actividades de arquitectura, de engenharia e técnicas afins	1	3,33%
861	Actividades dos estabelecimentos de saúde com internamento	3	10,00%
	Total	30	100,00%

Apêndice 3 – Caracterização da amostra segundo o ramo de actividade

Ramo de actividade	Frequência Absoluta	Frequência Relativa
Indústria / Produção	16	53,33%
Comércio	5	16,67%
Prestação de serviços	9	30,00%
Total	30	100,00%

Apêndice 4 – Caracterização da amostra segundo o CAE e a existência de sistemas de controlo interno e de gestão de risco

CAE	Descrição	Sistema de Controlo Interno		Processo de Gestão de Risco	
		Sim	Não	Sim	Não
0'12	Culturas permanentes (Viticultura)	1		1	
110	Indústria de bebidas	3		3	
152	Indústria de calçado	1	1		2
162	Fabricação de artigos de madeira, de cortiça, de espartaria e de cestaria, excepto mobiliário	2		2	
222	Fabricação de artigos de matérias plásticas	2		2	
233	Fabricação de produtos cerâmicos para a construção	1			1
251	Fabricação de elementos de construção em metal	1			1
289	Fabricação de outras máquinas e equipamento para uso específico	1		1	
293	Fabricação de componentes e acessórios para veículos automóveis	2	1	2	1
360	Captação, tratamento e distribuição de água	1		1	
464	Comércio por grosso de bens de consumo, excepto alimentares, bebidas e tabaco	2		1	1
467	Comércio por grosso de combustíveis, metais, materiais de construção, ferragens e outros produtos n. e	1		1	
477	Comércio a retalho de outros produtos, em estabelecimentos especializados	1			1
494	Transportes rodoviários de mercadorias e actividades de mudanças	2		2	
611	Telecomunicações	1		1	
619	Outras actividades de telecomunicações	1		1	
620	Consultoria e programação informática e actividades relacionadas		1		1
711	Actividades de arquitectura, de engenharia e técnicas afins	1		1	
861	Actividades dos estabelecimentos de saúde com internamento	3		2	1
	Total	**27**	**3**	**21**	**9**
		90%	**10%**	**70%**	**30%**

Apêndice 5 – Análise dos resultados obtidos no inquérito

1 – CARACTERIZAÇÃO DA EMPRESA

1. Qual é a actividade económica da sua empresa?

CAE	Descrição	N.º Empresas
1210	Produção e comercércio de vinho	1
11021	Produção de vinhos	2
11050	Fabricação de cerveja	1
15201	Indústria calçado	1
15202	Fabricante de componentes para calçado	1
16230	Fabricação obras de carpintaria para contrução	2
22210	Indústria de plásticos	1
22292	Indústria de artigos plásticos	1
23312	Indústria de cerâmica de construção	1
25110	Fabricação de estruturas de construções metálicas	1
28940	Fabricação de máquinas para indústria têxtil, vestuário e couro	1
29320	Fabricação de componentes e acessórios para veículos automóveis	3
36002	Abastecimento de água, drenagem águas residuais, recolha de resíduos sólidos urbanos	1
46460	Comércio p/ grosso produtos farmacêuticos	2
46732	Comércio p/ grosso de mat. construção	1
47711	Comércio a retalho de vestuário	1
49410	Transporte rodoviário de mercadorias	2
61100	Telecomunicações e multimédia	1
61900	Outras actividades de telecomunicações	1
62090	Tecnologias informação	1
71120	Actividades de Engenharia	1
86100	Prestação cuidados saúde	3
	Total	**30**

2. Qual a percentagem de capital social da sua organização detido por empresas estrangeiras?

Percentagem de capital social detido por empresas estrangeiras	Frequência Absoluta	Frequência Relativa
0%	21	70,00%
≤ 20%	2	6,67%
> 20% e ≤ 50%	2	6,67%
> 50% e ≤ 70%	0	0,00%
> 70%	5	16,67%
Total	**30**	**100,00%**

3. Qual o volume de negocios obtido em 2011 (em milhões de euros)?

Volume de negócios (milhoes de euros)	Frequência Absoluta	Frequência Relativa
≤ 50	17	56,67%
>50 e ≤ 100	5	16,67%
>100 e ≤ 500	5	16,67%
>500	3	10,00%
Total	**30**	**100,00%**

4. Em 2011, qual é a percentagem de volume de negócios que a empresa transaccionou para fora do mercado nacional?

Percentagem de volume de negócios transacionados para o exterior	Frequência Absoluta	Frequência Relativa
≤ 20%	13	43,33%
> 20% e ≤ 50%	7	23,33%
> 50% e ≤ 70%	5	16,67%
> 70%	5	16,67%
Total	**30**	**100,00%**

5. A empresa possui um departamento de auditoria interna?

Auditoria Interna	Frequência Absoluta	Frequência Relativa
Sim	12	40,00%
Não	18	60,00%
Total	**30**	**100,00%**

2 – CONTROLO INTERNO

6. Existe algum manual de Controlo Interno na empresa?

Manual de controlo interno	Frequência Absoluta	Frequência Relativa
Sim	18	60,00%
Não	12	40,00%
Total	**30**	**100,00%**

7. Como descreveria um Sistema de Controlo Interno? (assinale as suas opções)

Descrição de um sistema de controlo interno	Frequência Absoluta	Frequência Relativa
É um sistema que conduz à eficiência e eficácia das operações	26	18,71%
Contribui para a confiança e fiabilidade das demonstrações financeiras	25	17,99%
Assegura a conformidade com as leis e regulamentos	25	17,99%
Meio de prevenção de erros e/ou procedimentos ilegais ou fraudulentos	25	17,99%
Auxilia o processo de gestão	27	19,42%
Permite proteger os activos da empresa	11	7,91%
A sua implementação gera mais custos que benefícios	0	0,00%
A sua implementação não gera vantagens competitivas à empresa	0	0,00%
Não é um requisito importante na criação de valor para os seus accionistas	0	0,00%
Outras características	0	0,00%

8. Que meios de Controlo Interno existem na empresa?

Meios de controlo existentes na empresa	Frequência Absoluta	Frequência Relativa
Existência de organigrama contendo responsabilidades definidas, segregação de deveres e funções	28	9,56%
Verificação e conferência de registos e realização de conciliações	27	9,22%
Definição de autoridade e delegação de responsabilidades	27	9,22%
Pessoal qualificado, competente e responsável	25	8,53%
Manual de procedimentos, formulários e documentos	24	8,19%
Rotatividade e fluxo de entrada e saída de elementos chave à organização	6	2,05%
Rotinas de validação	13	4,44%
Confronto das contagens de caixa, títulos, activos e existências com os registos contabilísticos	26	8,87%
Restrição do acesso físico directo aos activos e registos	17	5,80%
Aprovação e controlo de documentos	29	9,90%
Comparação de informação com fontes externas de informação	20	6,83%
Comparação dos elementos obtidos com os orçamentados	26	8,87%
Controlo de contas e balancetes de verificação	23	7,85%
Outros (indique quais)	2	0,68%

Outros (indique quais):

Funções / áreas de planeamento e controlo de gestão, *revenue assurance*, fraude, gestão de risco (ERM), continuidade de negócio, segurança, qualidade e sistemas de controlo de qualidade de funções críticas, ambiente, auditoria interna, orgãos de governo independente (Conselho Fiscal e Comissão de Auditoria e Finanças)

9. Na sua opinião:

	Sim	Não
Considera o Controlo Interno como uma ferramenta de gestão?	100,00%	0,00%
O órgão de gestão deverá ser o responsável pelo planeamento, instalação e supervisão do Sistema de Controlo Interno?	76,67%	23,33%
A existência de um código de conduta é desnecessária, já que todos os colaboradores sabem quais são as suas tarefas e responsabilidades?	16,67%	83,33%
Um Controlo Interno eficaz pode ajudar os gestores a avaliar e gerir o risco de negócio?	100,00%	0,00%
Um Sistema de Controlo Interno bem construído e operativo significa, por si só, que a empresa esteja imune a situações como a ocorrência de erros, fraudes e irregularidades?	10,00%	90,00%
O Controlo Interno deverá ser extensível e focalizado apenas aos níveis hierárquicos intermédios e baixos da organização?	3,33%	96,67%
A avaliação da eficácia dos controlos e o seu ajustamento deverão ser feitos periodicamente?	96,67%	3,33%
Existem alguns mecanismos de Controlo Interno que gostaria de ver implementados na sua empresa? Se sim indique quais	60,00%	40,00%

Existem alguns mecanismos de controlo interno que gostaria de ver implementados na sua empresa? Se sim indique quais:

Manual de procedimentos claramente determinados que considerem as funções de todas as secções da empresa; mecanismos de controlo ligados aos activos fixos tangíveis; maior cruzamento de dados e verificações físicas externas.

3 – GESTÃO DE RISCO

10. A empresa tem implementado um processo formal de Gestão de Risco?

Processo de gestão de risco	Frequência Absoluta	Frequência Relativa
Sim	21	70,00%
Não	9	30,00%
Está a decorrer o processo de implementação	0	0,00%
Total	**30**	**100,00%**

11.A empresa tem uma compreensão exacta e abrangente dos riscos que actualmente enfrenta?

Compreensão exacta dos riscos	Frequência Absoluta	Frequência Relativa
Sim	19	63,33%
Não	0	0,00%
Apenas de alguns riscos	11	36,67%
Total	**30**	**100,00%**

Em caso afirmativo, indique 5 dos principais riscos a que a empresa está sujeita:

Derrapagem orçamental, controlo de infecção, erro terapeutico, acidentes cirúrgicos, queda de doentes, identificação de doentes; influências macroeconómicas, regulatório, concorrência,inovação tecnológica; desvio de dinheiro, segregação de funções; riscos financeiros e de qualidade; risco de crédito, redução do volume de negócios/redução de preços; riscos económicos, concorrência, imagem, satisfação do cliente, perdas financeiras; risco de incêndio, risco de afunilamento da produção em algumas áreas típicas, risco de não ter capacidade instalada suficiente para um aumento anormal de encomendas, risco de substâncias perigosas para o meio ambiente; obtenção de crédito, situação económica do país, envolvente macro-económica; retracção do consumo, falta de poder de compra.

12.Considera que a auditoria interna pode ter um papel estratégico na avaliação e supervisão de um processo de Gestão de Riscos de uma organização?

Auditoria interna tem um papel estratégico de avaliação e supervisão na gestão de risco	Frequência Absoluta	Frequência Relativa
Sim	28	93,33%
Não	2	6,67%
Total	**30**	**100,00%**

13.Na sua organização:

	Sim	Não	Não responderam
13.1 A gestão está disposta a assumir riscos para alcançar os objectivos estratégicos definidos pela organização?	93,33%	6,67%	0,00%
13.2 Estão definidos e correctamente implementados controlos que mitiguem eficazmente os riscos identificados na sua empresa, de modo a não colocar em causa a concretização dos objectivos definidos pela gestão?	80,00%	20,00%	0,00%
13.3 Existem meios ou técnicas para identificar potenciais eventos que poderão originar prováveis riscos ou oportunidades?	90,00%	10,00%	0,00%
13.4 Os processos de gestão de risco são acompanhados pela gestão de modo a garantir que as respostas e as acções desenvolvidas para controlar ou eliminar os riscos são eficazes e estão em linha com os objectivos da organização.	93,33%	3,33%	3,33%
13.5 Periodicamente são analisados e reavaliados os riscos a que a organização está exposta e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos.	86,67%	6,67%	6,67%

14.Na sua opinião, quais são as 5 principais vantagens resultantes da implementação de um Processo de Gestão de Risco:

Vantagens da implementação de um processo de gestão de risco	**Frequência Relativa**
Criação de procedimentos homogéneos de governação	6,71%
Habilitar a administração a correr riscos apropriados na criação de valor	16,11%
Maior monitorização da performance	18,12%
Melhoria da capacidade de relato para organismos reguladores	5,37%
Melhoria da comunicação com os accionistas e *stakeholders*	3,36%
Aumento da reputação	4,03%
Maior clareza no processo de decisão e da cadeia de comando a todos os níveis da organização	17,45%
Habilitar a administração a pensar de modo empreendedor e inovador	6,71%
Maior capacidade de atingir objectivos estratégicos	10,74%
Maior rentabilidade	10,07%
Outras, por favor indique quais:	1,34%

Outras, por favor indique quais:

Aumentar a segurança de doentes e colaboradores; envolvimento e responsabilização dos serviços; antecipar a ocorrência dos vários riscos de forma a evitar essa mesma ocorrência e a ter implementado uma acção de reacção para minorar ou eliminar as consequências desse acontecimento

4 – RELAÇÃO ENTRE CONTROLO INTERNO E GESTÃO DE RISCO

	Discordo	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo
Um processo de gestão de risco empresarial deverá ser implementado independentemente da existência de um sistema de controlo interno.	20,00%	16,67%	0,00%	36,67%	26,67%
Cada departamento de uma organização deverá ter um responsável pelo controlo interno, não cabendo apenas à gestão de topo essa responsabilidade.	0,00%	6,67%	10,00%	36,67%	46,67%
A auditoria interna deverá ser o órgão responsável por estruturar e implementar um processo de gestão de risco numa organização.	13,33%	46,67%	10,00%	20,00%	10,00%
A auditoria interna deverá ter apenas o papel de supervisão e avaliação num processo de gestão de risco e de controlo interno.	3,33%	20,00%	13,33%	36,67%	26,67%
A gestão de riscos relaciona-se com a gestão de ameaças e oportunidades enquanto o sistema de controlo interno é projectado para gerir eficazmente essas ameaças e oportunidades.	3,33%	6,67%	13,33%	26,67%	50,00%
O objectivo do controlo interno é o de auxiliar a gerir e a controlar o risco de forma adequada e não de o eliminar.	0,00%	3,33%	3,33%	43,33%	50,00%
Um controlo interno eficaz permite criar vantagens competitivas para a organização permitindo-lhe assumir riscos adicionais com vista à criação e preservação de valor para os seus accionistas.	3,33%	0,00%	6,67%	26,67%	63,33%
A gestão de risco e o controlo interno não garantem que os objectivos de uma organização sejam todos atingidos, apenas dão uma segurança razoável de que tais objectivos possam ser alcançados.	0,00%	0,00%	3,33%	23,33%	73,33%
A existência de fluxos de informação e relato entre os órgãos de gestão e as unidades operacionais são fundamentais para que a informação chegue, de forma tempestiva e exacta, a todos os colaboradores da empresa.	0,00%	0,00%	3,33%	26,67%	70,00%
Um bom sistema de controlo interno é essencial a uma gestão de risco eficiente.	0,00%	0,00%	0,00%	20,00%	80,00%