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

ISCAL

Contributo da Auditoria Interna na Detecção e Mitigação de Riscos Empresariais

José Pedro Fernandes Andrade da Silva Pires

DEFINITIVO

Lisboa, Junho de 2010

“O Planeamento de longo prazo não lida com decisões futuras, mas com o futuro de decisões presentes”

Peter Ferdinand Drucker

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

Contributo da Auditoria Interna na Detecção e Mitigação de Riscos Empresariais

José Pedro Fernandes Andrade da Silva Pires

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria realizada sob a orientação científica do Prof. Doutor Manuel Mendes da Cruz, doutorado em Gestão.

Constituição do Júri:

Presidente _____ [Carlos Baptista da Costa]

Vogal_____ [Manuel Mendes da Cruz]

Vogal_____ [António da Trindade Nunes]

Lisboa, Junho de 2010

Agradecimentos

Concluída esta dissertação de mestrado resta-me registar os mais sinceros agradecimentos às individualidades que de várias formas contribuíram para que esta se tornasse numa realidade.

Gostaria antes de mais de agradecer ao Professor Doutor Manuel Mendes da Cruz, orientador desta dissertação, pelo apoio, estímulo, disponibilidade e cordialidade demonstrada em todas as fases que levaram à concretização deste trabalho.

A todos os professores que leccionaram na parte curricular do mestrado o meu muito obrigado pela partilha constante dos seus conhecimentos e experiencias, que muito me enriqueceram.

Ao Dr. Pedro Terruta, dos Serviços de Informação e Documentação (SID) do ISCAL na incansável colaboração prestada em todas as fases de pesquisa bibliográfica.

Aos meus colegas de mestrado em especial a Sofia Magalhães por todo o auxílio na revisão do trabalho, em particular em algumas questões técnicas, assim como todo o apoio e incentivo que sempre me deu ao longo da execução do mesmo.

Agradeço também aos meus amigos pelo entusiasmo constante, e pela compreensão demonstrada em algumas ocasiões importantes em que me privei da sua companhia.

Sou também muito grato a todos os meus familiares nomeadamente aos meus pais e irmã pelo estímulo e carinho que deles recebi ao longo deste complicado período de elaboração do trabalho, em que não tive possibilidade de privar com eles da forma que todos desejaríamos.

Um agradecimento muito especial e particular ao meu pai pela inesgotável e imprescindível colaboração na derradeira revisão de todo o trabalho.

A todos, o meu mais profundo e sincero agradecimento.

ABSTRACT

The scandals on financial markets around the world led to the production of documents that define how internal controls should be understood and implemented in order to cope with situations that could lead to similar disasters. All this conducted to what we call "the changing of paradigm" in internal auditing.

The role of internal auditor is nowadays more valued and it is expected that its work contributes decisively to the detection and mitigation of risks to which the companies are exposed.

We find it therefore particularly relevant to answer questions like: How can an internal auditor contribute to the risk management process? In which phase of its work should it be more aware for the issue of enterprise risks?

The aim of this work is to add value to the internal auditing profession by answering the above questions.

This will be achieved through investigation on literature, which will allow us to develop the theme in order for its study to become more consistent.

Key words: Internal Auditing, Enterprise Risk, Internal Control, Enterprise Risk Management; Internal Control System

RESUMO

Os escândalos que assolaram os mercados financeiros um pouco por todo o mundo, como são o caso da ENRON e PARMALAT contribuíram para a elaboração de documentos que definem como deve ser entendido e implementado um SCI (Sistema de Controlo Interno), de forma a fazer face a novas situações de risco que pudessem conduzir a desastres semelhantes ou piores aos já verificados. Tudo isto potenciou aquilo a que hoje chamamos de "mudança de paradigma" na função de auditoria interna. O papel do auditor interno passou a ser valorizado de uma outra forma esperando-se que o seu trabalho, contribua de forma decisiva, para a detecção e mitigação dos riscos a que as empresas estão sujeitas.

Considerou-se de particular interesse responder a questões como: De que forma contribui o trabalho do auditor interno no processo de gestão dos riscos empresariais? Em que fase do trabalho o auditor deve estar mais desperto para a questão dos riscos empresariais?

O objectivo do presente estudo é precisamente responder assim às questões acima enunciadas e, desta forma, contribuir para o incremento de valor na profissão de auditor interno.

Este tema vai ser estudado através da revisão de literatura, que permitirá efectuar um adequado enquadramento do mesmo no sentido de tornar o seu estudo mais consistente para a aprendizagem e evoluir da profissão.

Palavras-Chave: Auditoria Interna, Riscos Empresariais, Controlo Interno, Gestão de Risco; Sistema de Controlo Interno;

Índice Geral

Índice de Figuras

Índice de Quadros

LISTA DE ABREVIATURAS

AAA – American Accounting Association

AECA- The American European Community Association

AI – Auditoria Interna

AICPA - American Institute of Certified Public Accountants

CEO – Chief Executive Officer

CFO – Chief Financial Officer

CI – Controlo Interno

COBIT – Control Objectives for IT

COSO - Committee of Sponsoring Organizations of the Treadway Commission

DAI – Departamento de Auditoria Interna

DRA – Directriz de Revisão e Auditoria

FEI –Financial Executives International

IIA – Institute of Internal Auditors

IMA- Institute of Management Accountants

ISACA - Information Systems Audit and Control Association

NC – Nível de Consequência

ND – Nível de Deficiência

NE – Nível de Exposição

NP – Nível de Probabilidade

NR – Nível de Risco

PCAOB - Public Company Accounting Oversight Board

SBI – Sistema Bancário Internacional

SCI – Sistema de Controlo Interno

SOX – Sarbanes-Oxley

SWOT - Strengths, Weaknesses, Opportunities and Threats

I - INTRODUÇÃO

Os escândalos financeiros que assolaram os EUA e também deixaram um rasto de "destruição" na Europa, como foram o caso da ENRON em 2001, WORLDCOM em 2002 e PARMALAT em 2003,entre outros, estiveram na base da elaboração de alguns documentos que auxiliaram a definir como deveria ser entendido e implementado um SCI (Sistema de Controlo Interno), para fazer face a novas e potenciais situações como as já ocorridas.

As diversas situações que degeneraram nas falências que se conheceram, tiveram na sua origem, entre outras situações, riscos corridos por algumas entidades, riscos esses cujo foco se centrava em situações de fraude e que em alguns casos ainda mais impacto tiveram pela falta de ética que se verificou. Ao serem implementados mecanismos de controlo que permitissem a mitigação desses mesmos riscos, seria provável que muitas destas situações tivessem sido evitadas. Daqui se infere a importância que poderão ter todos os mecanismos de controlo interno (CI) na gestão de riscos das empresas. Contudo, será sempre necessário alertar para a importancia da relação custo-benifício no processo de gestão de risco, pois a eficiente alocação de recursos neste processo será sem dúvida um factor auxiliar na mitigação de risco.

Por outro lado, tendo em conta a conjuntura económico-social a que hoje se assiste, é cada vez mais notória a importância dada à avaliação e análise dos tipos de risco que estão associados a determinado sector de actividade.

Desta feita, e dada a sua crescente importância, todas as organizações com aspirações a conseguirem ou a manterem um posicionamento firme no sector onde

"habitam", tendem a dar cada vez mais destaque aos riscos associados ao seu *core business.*

Uma das formas encontradas para praticar uma eficiente mitigação dos riscos, passa pela implementação de controlos que poderão auxiliar, de sobremaneira, na detecção dos mesmos, assim como possibilitar que estes tenham um impacto menos significativo numa organização. Um importante coadjuvante na implementação desses mesmos mecanismos de controlo é a auditoria interna (AI).

Esta é, sem dúvida, uma época de mudança de paradigma, sendo que a função de AI se tem revelado cada vez mais um importante instrumento e meio de auxílio para um melhor desempenho empresarial, facto que outrora não se vislumbrava. Anteriormente a função de AI limitava-se a efectuar uma mera avaliação do cumprimento dos procedimentos e princípios pelos quais se regia o CI de uma dada entidade, comedindo-se, após isso e apenas, a relatar factos, assumindo assim uma postura muito pouco proactiva, contrariamente ao que hoje acontece.

Actualmente são também muitas mais as empresas a adoptarem e a implementarem procedimentos e sistemas de controlo interno (SCI), pois cada vez mais tem sido notório o forte contributo que um sistema destes poderá oferecer às organizações que o possuem.

O estudo aqui vertido pretende dar uma visão das verdadeiras mais-valias que a AI poderá dar na prevenção e consequente mitigação dos riscos empresariais.

Pretende-se, com este trabalho, analisar a relação existente entre os riscos a que as empresas estão expostas e o contributo que a AI lhes poderá dar na detecção e mitigação dos mesmos. Ambiciona-se também percepcionar quais as efectivas mais

valias do trabalho de AI no seio de uma organização, sendo esta uma questão que interessa aos profissionais da área assim como aos demais estudiosos.

Tudo o que foi aqui explanado será suportado numa substancial revisão de literatura, que permitirá efectuar um adequado enquadramento do tema no sentido de incrementar valor, o que permitirá torná-lo mais consistente do ponto de vista teórico.

A escolha deste assunto decore de uma revisão bibliográfica que permitiu concluir que se trata de uma temática ainda pouco abordada em Portugal como toda aquela que abarca AI e Riscos Empresariais.

Outro aspecto que pesou para a escolha deste tema, prendeu-se com o facto de riscos empresariais, como é sabido, se tratar de uma matéria muito em voga nos dias que correm, pois uma entidade para poder vingar num mercado tão competitivo e globalizado como o que se conhece, está constantemente exposta a riscos, daí o desígnio de estudar esses riscos e perceber a forma como a AI poderá auxiliar na sua mitigação.

Será dado um grande enfoque à temática dos riscos empresariais dissecando a sua importância num contexto actual, pois a redução de risco está muito associada ao aumento do controlo, afirmando-se cada vez mais como uma prática indispensável.

Será também muito importante compreender o funcionamento do departamento de AI de uma entidade a fim de melhor percepcionar qual o alcance do trabalho que é desenvolvido por este.

Desta forma, para alcançar este objectivo, optou-se por fazer uma análise aos riscos empresariais, partindo da sua definição e classificação até chegar ao processo de gestão dos mesmos.

No capítulo em que se explana a gestão dos riscos empresariais optou-se por fazer uma abordagem não só ao processo de gestão do risco e possíveis estratégias a seguir, mas também aos marcos históricos (Relatório Turnbull e Basileia I e II) que alteraram a forma como é encarado este processo tão importante dentro de uma organização.

Passa-se então à área de CI, onde se começa por uma incursão histórica acerca da evolução do conceito e perspectiva dos SCI, abordando os vários modelos propostos por diferentes organismos, para chegar ao COSO – ERM, modelo mais relacionado com a gestão de riscos empresariais, constituindo este o cerne do estudo em apreço.

Do CI chegou-se então à função de AI, onde se demonstra como esta tem vindo a evoluir e dá-se também algum destaque à mudança de paradigma ocorrida nos anos 90. Neste capítulo mostra-se ainda como funciona um departamento de AI de forma a perceber como embutir o contributo esperado deste nos seus métodos e fases de trabalho.

No capítulo final, a conclusão, analisa-se o que pode ser absorvido deste trabalho alertando para possíveis e pertinentes assuntos a estudar dentro desta temática, num futuro próximo.

II - DESENVOLVIMENTO

CAPÍTULO 1 - RISCOS EMPRESARIAIS

1.1 - Definição de risco

Tal como referido na Introdução, o ambiente empresarial tem a si associado diversos riscos pois "toda a actividade empresarial consubstancia a assunção de riscos, de incerteza da ocorrência de perdas económicas" [CRUZ:2005].

Como se pôde verificar aquando da revisão de literatura efectuada para a elaboração do presente estudo, existem diversas definições de riscos empresariais difundidas por diferentes autores, sendo que se optou por destacar as seguintes:

"O risco pode ser definido como uma possibilidade de que algum acontecimento desfavorável venha a ocorrer e que possa afectar um grande número de activos da empresa." [*CRUZ*: 2008].

Segundo *BARALDI* (2005) "Os riscos empresariais são todos os eventos que impedem a empresa e as pessoas de ganharem dinheiro e respeito. São elementos incertos e as expectativas que agem constantemente sobre os meios estratégicos e o ambiente e que provocam os desastres financeiros."

De uma forma muito genérica, o risco do negócio pode surgir das mais variadas formas, podendo estar ligado a factores como decisões de investimentos estratégicos, lançamento de novos produtos, pode ainda estar associado a estratégias de marketing, competição de mercado e incertezas quanto ao

comportamento das vendas entre outras condições, sendo esta a perspectiva apresentada pelos autores *LINSMEIER & PEARSON*, (1996).

Do que acima se leu pode-se retirar que correr riscos é um facto inerente à própria existência de uma empresa, pressupondo, contudo, que esta tenha uma capacidade e vontade de inovar e gerar riqueza, aproveitando assim as oportunidades que lhe vão surgindo de todo o meio envolvente. Essa capacidade fará com que a empresa possa tirar proveito de uma situação de risco, tranformando um risco numa oportunidade de acordo com a lógica da análise SWOT – ferramenta utilizada para fazer análises de cenários, nomeadamente na gestão e planeamento estratégico. **SWOT** é um termo inglês, acrónimo de Forças (**S**trengths), Fraquezas (**W**eaknesses), Oportunidades (**O**pportunities) e Ameaças (**T**hreats).

1.2 - Distinção entre Risco e Incerteza

Ainda no âmbito da definição de risco há que caracterizar dois conceitos distintos mas bastante relacionados – Risco e Incerteza.

Esta é uma perspectiva proposta por *CRUZ* (2008), tendo sido feita por este autor uma interessante distinção entre estes dois conceitos:

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

De notar que o conceito de incerteza é de acrescida importância no âmbito deste trabalho, pois um dos objectivos da A.I. passa também por reduzir a incerteza associada ao negócio, o que permitirá, pela ligação entre incerteza e risco, contribuir para a mitigação de alguns dos riscos empresariais. Sendo esse o âmbito

de estudo do presente trabalho, passar-se-á agora a aprofundar um pouco mais o conceito de incerteza e qual a sua ligação com a gestão de riscos.

1.2.1 - Ligação entre Incerteza e Gestão de Riscos - o papel da Auditoria Interna

No círculo da gestão de riscos, a incerteza é um factor que deverá ser mantido sob controlo, pois num ambiente empresarial há que tomar decisões, muitas das vezes, tão repentinas e sem as informações mais detalhadas quanto seria desejável, o que fará com que essas situações se revistam de uma enorme incerteza, situação esta que não permitirá controlar as consequências da decisão tomada, podendo estas ser danosas para a organização. [*MURTEIRA*; 1996].

Considera-se esta uma situação pouco favorável à empresa dado que "todo o processo de tomada de decisões poderá influenciar o futuro da empresa pois as decisões tomadas hoje trarão consequências ainda mais tarde" [AECA, 2002].

Contudo, as decisões têm que ser tomadas e muitas delas não se podem fazer esperar, dada a constante e "impiedosa" concorrência que se constata no mundo empresarial actual, logo, não se pode esperar que a incerteza desapareça do sector empresarial. Tudo o que se mostrar um poderoso auxiliar na tomada de decisões num determinado ambiente, será, sem dúvida, um valioso elemento. Daqui se constata a importância que poderá ter o departamento de auditoria interna (DAI) na produção de informação para o auxílio na tomada de decisões. O trabalho desenvolvido por este departamento será certamente uma mais-valia para a organizaçao, pois através da análise dos elementos resultamtes do seu trabalho permitirá, de algum modo uma minimização da incerteza na altura da decisão.

1.3 - Classificação dos riscos empresariais

Como referido anteriormente os riscos aos quais as empresas estão expostas, não são todos iguais, nem tão pouco têm as mesmas consequências, daí ser importante fazer uma adequada classificação dos mesmos. Há a salientar o facto de existirem diversas classificações de riscos consoante o entendimento dos diversos autores analisados. Contudo encontra-se um ponto comum em todos os autores, trata-se da importância dada à realizadação de uma adequada análise para posteriormente se proceder à devida alocação de recursos na monitorização dos riscos aos quais estão expostas as empresas.

Segundo a perspectiva de *CRUZ* (2008) os riscos empresariais podem classificar-se da seguinte forma:

Riscos associados à estratégia – São os riscos relacionados com a forma como a empresa é gerida e orientada, são aqui focados factores competitivos, estrutura organizacional, desenvolvimento de novos produtos, considerando-se também a estratégia de formação de preços;

Riscos Financeiros – Estes são os riscos associados à posição financeira da empresa, neste contexto a gestão deste tipo de risco relaciona-se com instrumentos de tesouraria e fluxos financeiros;

Risco de Mercado – Trata-se do risco associado à própria actividade normal da empresa, ou seja, um risco externo que a empresa não pode controlar, está associado à conjuntura onde esta se insere, sempre sujeita a mudanças, podem ser disso exemplo factores como a inflação, mudanças cambiais entre outras. Este tipo de risco pode assumir um cariz "económico e financeiro,

representando a possibilidade de perda que a empresa possa sofrer, num determinado momento, devido a circunstâncias que não controla" [*CRUZ*: 2009]. Como se pode constatar, este risco é de difícil ou mesmo impossível eliminação, sendo apenas possível à empresa controlar este risco através de uma atenta análise da sua situação conjuntural, desenvolvendo uma atitude proactiva face ao evoluir da envolvente económico-social;

Risco de Negócio ou Operacional – Trata-se de um risco que difere de sector de actividade para sector de actividade, diferindo também de empresa para empresa dentro de um mesmo ramo de negócio. Este tipo de risco engloba todos aqueles que podem resultar em prejuízos inesperados devido a falhas humanas, falhas nos procedimentos, ou outras, cujas causas sejam externas, desta definição excluem-se os riscos estratégicos. Segundo *CRUZ* (2009) a incerteza associada ao risco de negócio pode ter subjacentes aspectos como a instabilidade da procura, a volatilidade do preço, a volatilidade dos custos dos factores, repercutindo-se no preço de venda de um determinado produto.

Ainda neste âmbito e de acordo com *MENESES* (1995), este tipo de risco (risco de negócio ou operacional) encontra-se associado a três tipos de factores:

a) Factores de natureza comercial - Quota de mercado, preços de venda e estrutura de custos, denote-se que estes diferem mediante a empresa e o sector em que cada uma se insere; sendo cada um deles pautado pela incerteza, dada a volatilidade quer de procura, quer de preço, daí o risco considerado;

b) Factores técnico - produtivos – O chamado risco tecnológico, são disso exemplo o nível dos custos variáveis unitários, a adequabilidade dos custos de distribuição;

c) Factores não económicos – Nestes casos temos a politica de investimentos seguida pela empresa, o nível de remuneração dos capitais próprios e o custo dos capitais alheios.

Segue-se uma outra classificação de riscos empresariais, esta dada por *BRASILIANO* (2003), que segmenta os riscos em quatro grandes grupos, sendo eles:

Risco de Mercado – Trata-se de uma medida numérica da incerteza relacionada com o retorno do investimento em virtude das variações das taxas de juro; taxas de câmbio, preços de acções e *commodities*, sendo estes, alguns dos principais factores que influem no risco de mercado;

Risco de crédito – Este retrata a incerteza numérica relacionada com o recebimento de um determinado valor, a ser pago por um tomador de determinado empréstimo. Por outras palavras este mede o grau de incerteza na obtenção do retorno esperado numa determinada aplicação financeira ou investimento realizado. Trata-se de um tipo de risco muito frequente no sector financeiro;

Risco Legal – Este tipo de risco representa as perdas potenciais relacionadas com o facto de um contrato não estar legalmente fundamentado, podendo assim ser anulado, gerando uma perda, tanto por documentação insuficiente, falta de representatividade relativa a uma das partes com contrato, tornando-

se assim ilegal. O risco legal também surge se a aplicação das leis ou regulamentos for pouco clara;

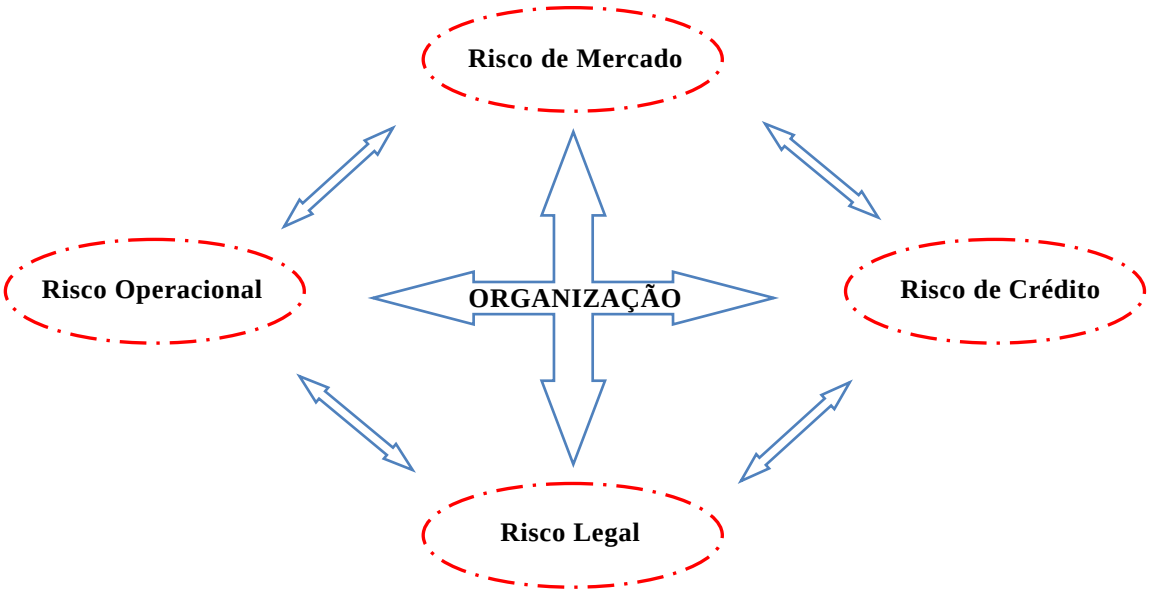
Risco Operacional – Este traduz-se numa medida numérica de incerteza quanto aos retornos de uma empresa, caso os seus SCI sejam inadequados ou ineficazes. Considera-se que este está relacionado com as possíveis perdas resultantes de falhas nos sistemas ou falhas humanas. Pode ainda ser resultado de conluio, utilização indevida de modelos matemáticos ou produtos, alterações no ambiente dos negócios, ou a situações adversas de mercado. O risco operacional pode ser dividido em três grandes áreas, a saber:

a) Risco organizacional - Está relacionado com uma organização ineficiente, administração inconsistente e sem objectivos de longo prazo bem definidos, fluxo de informações internas e externas deficientes, responsabilidades mal definidas, fraudes, acesso a informações internas por parte de concorrentes, entre outros aspectos.

b) Risco de operações - Está relacionado com problemas como *overloads* de sistemas ou seja processamento e armazenamento de dados passíveis de serem alvo de fraudes e erros, confirmações incorrectas ou sem verificação criteriosa.

c) Risco de pessoal - Está relacionado com empregados não qualificados e/ou pouco motivados, personalidade fraca, falsa ambição, e muitas vezes associado a uma fraca remuneração, factor que, por vezes, poderá potenciar o “apelo” à fraude

Figura. Nº 1 - Principais Grupos de Risco



Fonte: Adaptado – JÚNIOR, António Marcos Duarte - *Risco: Definições, Tipos, Medição e Recomendações para seu Gerenciamento*

Daqui se infere que todos estes tipos de risco se inter-relacionam entre si e "gravitam" em torno da organização, estando esta em constante interacção com todos eles, uns mais outros menos, isto, dependendo dos controlos que dispõe para os enfrentar, assim como do sector de actividade em que se insere.

Já *JORION* (2000) apresenta uma classificação mais simples, dividindo os riscos em três grandes grupos, Operacionais, Estratégicos e Financeiros.

O American Institute of Certified Public Accountants (AICPA) elaborou um estudo onde identificou e classificou os riscos empresariais em três grandes grupos:

Riscos relacionados com o Ambiente Empresarial – Sejam eles ameaças ao ambiente empresarial em que esta opera, como os riscos decorrentes da actuação da concorrência, riscos políticos, riscos legais ou normativos,

decorrentes da conjuntura jurídica, riscos financeiros e riscos da mudança da procura;

Riscos relacionados com processos de negócio e os seus activos – Estes riscos reflectem as ameaças aos processos de negócio e a perdas de activos físicos, financeiros e outros;

Riscos relacionados com informações – Ameaças associadas à má qualidade das informações prestadas ao processo de tomada de decisões assim como a que é dada a terceiros.

Ainda no entender deste organismo (*AICPA*), existe a possibilidade de surgirem novos riscos, associados ao aparecimento de novas estruturas organizativas. Considera-se que muitos controlos sobre informações e/ou activos sofrem alterações, tornando-se mais frágeis e até mesmo inexistentes pelo facto de serem feitas reestruturações e processos de *downsizing* dos níveis organizacionais. Pode assim dizer-se que todos estes processos, apesar de muitas das vezes se mostrarem uma solução para a redução de custos e melhoria das condições de operacionalidade de uma empresa, podem, na verdade, tornar-se uma fonte de risco.

Há ainda a salientar a perspectiva acerca da classificação e avaliação de riscos, apresentada pela *PricewaterhouseCoopers*. Segundo esta reconhecida multinacional de auditoria, os riscos deverão ser classificados por natureza e consequente relevância, admitindo a seguinte disposição:

Risco Estratégico – Trata-se do risco associado à forma como a empresa está a ser gerida, estes focam-se em factores competitivos, estrutura

organizacional, desenvolvimento de novos produtos, entre outros, como é o caso da estratégia utilizada pela gestão na formação dos preços dos produtos.

Risco Financeiro – Este é um risco associado à posição financeira de uma determinada empresa. A gestão de riscos financeiros está associada tanto a instrumentos relacionados com a tesouraria e fluxos financeiros como aos riscos relacionados com os relatórios financeiros (internos e externos).

Risco Tecnológico – Trata-se do risco decorrente da tecnologia de informação utilizada, ou seja todas as situações relacionadas com os factores tecnológicos que possam por em causa a fiabilidade e integridade da informação. Estes riscos podem expor significativamente os recursos da empresa, potenciando o risco de perdas.

Risco Operacional – Trata-se do risco associado a todos os procedimentos internos de uma organização, está relacionado com a fiabilidade e aplicação adequada do CI. Foca-se na integridade dos processos que auxiliam no suporte do negócio.

Riscos de Conformidade – São os riscos que estão relacionados com a capacidade e forma como a empresa cumpre com normas e regulamentos aplicáveis no meio onde se insere. A inconformidade com as normas legais, potencia um conjunto de riscos para a empresa, que podem acarretar perdas significativas, tanto a nível financeiro como a nível de imagem, que posteriormente se transformarão inevitavelmente em perdas de cariz financeiro.

Riscos relacionados com o meio ambiente – Trata-se de um tipo de risco cada vez mais frequente nos dias de hoje, daí o esforço que as empresas terão que fazer de modo a minimiza-lo. Tal como acontece com os riscos de conformidade, estes podem afectar a imagem da empresa por não cumprir com os regulamentos vigentes relacionados com o ambiente. As contingências associadas a este tipo de risco prendem-se com a necessidade de reparação das áreas afectadas pela degradação provocada pela actividade da empresa, elevação dos valores pagos com prémios de seguro, indemnizações, multas, a par da consequente e já abordada perda de imagem que poderá acarretar uma futura diminuição dos resultados.

Partindo das diferentes classificações apresentadas propõe-se uma que divide os riscos a que uma empresa está exposta em três tipos, tendo em conta as questões com as quais estão relacionados:

- Riscos relacionados com o mercado, a envolvente da empresa - Envolve questões legais, políticas, sociais, económicas, ambientais, entre outras;
- Risco relacionados com a própria organização – Envolve questões sob a alçada da estrutura organizacional da empresa, como lida com os funcionários, clientes e fornecedores, como conduz a sua estratégia de actuação nas diferentes àreas;
- Risco relacionados com o negócio da empresa – Independentemente do mercado em que opere e da forma como a empresa conduza as suas operações, o negócio tem implícitos certos tipos de riscos. Pode envolver

questões ambientais, de segurança, de obsolescência de itens (em negócios que envolvam alta tecnologia, por exemplo).

Pode constatar-se que dos inúmeros riscos associados à actividade empresarial alguns são controláveis pela empresa e outros nem tanto. Além destes existem ainda outros tipos de risco provenientes do exterior - são os considerados riscos puros ou não sistemáticos [*CRUZ:*2008]. Estes riscos são aqueles que advêm de situações acidentais ou aleatórias associadas ao dia-a-dia de uma empresa. Cabe-lhe decidir como deverá lidar com estes riscos, após a sua identificação e quantificação terá que optar pela sua aceitação, prevenção, redução, eliminação ou a opção de os transferir para terceiros por intermédio de um seguro.

Importa salientar que as empresas não estão todas expostas aos mesmos tipos de risco, pois estes têm diferentes características em função do sector em que uma organização se insere e das suas próprias especificidades como sejam a sua estrutura organizacional ou a estratégia por si seguida.

CAPÍTULO 2 - GESTÃO DE RISCO EMPRESARIAL

2.1 - Definição

> *"A gestão de risco empresarial é um processo, desenvolvido pela administração, gestão e outros colaboradores de uma entidade, aplicado no estabelecimento da estratégia em toda a empresa, desenhado para identificar eventos potenciais que possam afectar a entidade, e gerir o risco dentro da apetência de risco da entidade, para garantir uma segurança razoável na realização dos objectivos."*

Enterprise Risk Management Framework – COSO I

2.2 - O Processo de Análise dos Riscos

De acordo com *BRASILIANO* (2003), após a identificação e descrição dos processos e recursos operacionais, há a necessidade de verificar quais os riscos susceptíveis de afectar o desempenho dos mesmos. Para isso é necessário o conhecimento de cada tipo de risco, verificando qual o seu impacto para uma organização.

Nesta fase é fundamental ter um bom conhecimento do sector de actividade em que a empresa opera, para assim ter uma maior capacidade de avaliar quais os riscos mais comuns para assim se verificar, com maior exactidão, quais são os que a afectam de facto. Pois conforme já foi referido, cada empresa tem uma forma diferente de reagir ao risco, mesmo que integrada no mesmo sector de actividade, daí a importância de conhecer bem os riscos antes de os tentar "combater"e mitigar.

Considera-se pertinente apresentar uma classificação de risco alternativa, ligada às consequências da sua ocorrência para a organização e não à "fonte" do risco. Trata-se da perspectiva de *CRUZ* (2008) que elenca os riscos segundo três classes distintas, sendo elas:

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

É de realçar o facto de muitas vezes a identificação dos riscos internos ficar prejudicada pelo facto de, em muitas organizações, cada pessoa ou departamento tentar encobrir a suas deficiências, chegando mesmo a camuflar os riscos que lhes estão associados, dificultando assim todo o porcesso de gestão de risco [*NAKASHIMA & CARVALHO*: 2004].

Para se conseguir êxito na análise de riscos, permitindo assim uma mais eficaz gestão de riscos, *BRASILIANO* (2003) sugere a realização de entrevistas com os responsáveis operacionais de cada departamento com a finalidade de fazer um levantamento dos factores de risco, ou seja, observação dos factores que podem atingir negativamente o departamento, além disso é comum efectuarem-se outras investigações tais como:

- Histórico de perdas externas - Verificar o que aconteceu em processos similares, mas em outras empresas;
- Histórico de perdas internas – Verificar os dados do que aconteceu dentro da empresa;
- Estruturas estratégicas de riscos – Identificar os riscos operacionais que são controláveis pela empresa, de forma a entender o seu fluxo;
- Práticas de mercado – Perceber o que as outras empresas estão a fazer para gerir da melhor forma os tipos de risco, trata-se de uma espécie de *benchmark*, para recolher a informação sobre as melhores práticas.

2.2.1 - A Matriz de Riscos

Após a identificação, classificação e análise dos riscos, será necessário avaliar cada um em termos da sua ocorrência potencial, e quais os seus impactos tanto Estratégicos e Operacionais como Financeiros.

Esta avaliação far-se-á nos seguintes moldes:

Impacto – Alto, Médio ou Baixo

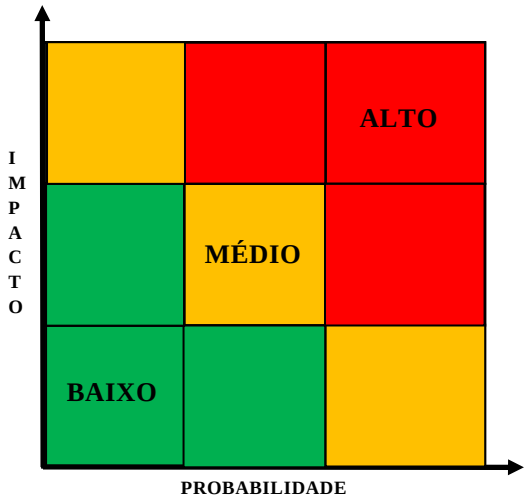
Probabilidade – Alta, Média ou Baixa

De referir que se considerou de extrema importância, nesta fase da análise e avaliação dos riscos, a divisão por classes sugerida por *CRUZ* (2008), feita de acordo com as consequências da ocorrência de cada risco.

Através da análise do binómio Impacto/Probabilidade, será possível obter informações que darão um importante auxílio nas decisões a tomar relativamente à gestão desses mesmos riscos.

Assim se destaca o facto de em cada quadrado da figura seguinte se poderem posicionar diversos tipos de risco aos quais uma determinada organização está sujeita, a título de exempo - Impacto e Probabilidade de ocorrencia baixa, corresponde a uma risco baixo, situando-se este num dos quadrados com a cor verde. A mesma análise poderá ser feita para diveros riscos sendo estes posicionados no quadrado correspondente, permitindo assim que seja feita uma rápida análise visual dos riscos que estão subjacentes à actividade de uma determinada empresa.

Figura nº 2 – Matriz de Risco – Impacto x Probabilidade



Fonte: Adaptado de BEZERRA, Juliana – *A importância do gerenciamento de riscos em projectos*

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

Contudo é de referir que todos os outros riscos, não apenas os de impacto e probabilidade alta, não deverão, de forma alguma, ser descurados por parte das entidades, pois representam também eles riscos e como tal deverão sempre ser acompanhados e monitorizados pelas empresas para assim estas não serem surpreendidas.

2.3 - Estratégias de Gestão de Risco Empresarial

Feita a identificação classificação e análise dos riscos, a empresa irá então decidir como agir (ou apenas reagir) perante cada um deles.

KRUTZ (2003) destaca quatro estratégias possíveis para fazer face ao risco, sendo elas:

Mitigação de Riscos: É a reacção ao risco normalmente evocada em primeiro lugar. Esta contém todas as medidas tomadas pelas empresas contra as ameaças que determinados riscos podem representar para elas.

Aceitação de Riscos: Este caso põe-se desde que o custo da eliminação de um determinado risco for substancialmente superior ao custo para a empresa associado à consequência que este produzirá na mesma. Ou desde que a sua eliminação desvie recursos da eliminação de um outro risco muito mais grave.

Transferência de Riscos: Esta é também uma prática comum no que à gestão de riscos diz respeito, pois em alguns casos é mais prudente transferir o risco para terceiros – seguradora – do que alocar recursos limitados a iniciativas de mitigação que provavelmente farão pouca ou nenhuma diferença.

Contenção de Riscos: Haverá casos em que o custo associado à eliminação de um determinado nível de risco simplesmente não pode ser comportado pela empresa. Nesses casos é melhor evitar totalmente o risco, ou seja retirando o processo em questão, ou antes disso deixando mesmo de o instalar.

Este autor reforça ainda a importância de uma criteriosa análise dos riscos e relembra que será de todo impossível a uma entidade eliminar na íntegra todos os riscos que a rodeiam. *KRUTZ* (2003) afirma que "Se você acha que precisa mitigar todos os riscos que encontrar, seus recursos acabarão antes que você elimine suas vulnerabilidades", acrescentando ainda que, "Você precisa usar uma combinação de estratégias de acordo com a natureza do seu ambiente e com o seu orçamento de segurança."

Fazendo ainda alusão à matriz de riscos, considera-se importante a perspectiva de MACHADO (2009), segundo este autor mediante a classificação de determinado risco, deverão ser tomadas medidas para que este não afecte a empresa, a saber:

- Probabilidade e Impacto elevados – Risco Alto – Acção a tomar – EVITAR (eliminar a actividade que dá origem a este risco).
- Probabilidade elevada e Impacto reduzido – Risco Médio – Acção a tomar – REDUZIR – (implementar e/ou reforçar controlos ou partilhar com terceiros, contratar um seguro).
- Probabilidade baixa e Impacto elevado – Risco Médio – acção a tomar – REDUZIR – (acção igual à anterior)
- Probabilidade baixa e Impacto reduzido – Risco Baixo – Acção a tomar – ACEITAR - (monitorizar).

2.4 - A importância da gestão de riscos para a empresa

O processo de gestão de riscos é por tudo o que se explicou anteriormente, deveras importante para a vida da empresa. Além dos motivos associados à continuidade da empresa, isto é, evitar consequências desastrosas como o encerramento da mesma, o processo de gestão de riscos permitirá de acordo com LEITE (2007), entre outras coisas, que existam reduções nas taxas dos prémios de seguro, a diminuição dos custos de transacções com fornecedores e clientes. Este processo de gestão de riscos poderá ainda permitir o descortinar de novas oportunidades de negócio, assim como atrair novos investidores dada a segurança que um processo destes lhes poderá transmitir.

A gestão de risco está englobada no processo de gestão e administração de uma entidade, este visa encaminha-la no sentido de obter os melhores resultados possiveis com os recursos de que dispõe. É neste sentido que se torna importante abordar a temática do *Corporate Governce,* pois trata-se este de um processo que visa a implementação de controlos para auxiliar em todo o processo de gestão da empresa nomeadamente na gestão de riscos.

2.4.1 - Corporate Governance – definição e objectivos

A expressão *Corporate Governance* tem vindo a fazer parte do léxico comum de muitas empresas, pois esta designa um conjunto de regras, práticas e procedimentos que contribuem para um maior controlo, fazendo assim com que a empresa esteja mais preparada para enfrentar os diversos riscos aos quais está exposta.

Existem algumas definições de *Corpotate Governance* e todas elas se consubstanciam na supervisão da administração e implementação de controlos com

vista à gestão de riscos, sendo esta considerada a Era da moderna administração. Seguidamente se destaca a definição emanada pelo *Instituto Brasileiro de Governança Corporativa (IBGC).*

> **"**Governança Corporativa é o sistema que permite aos accionistas ou cotistas o governo estratégico da sua empresa e a efectiva monitorazação da direcção executiva. As ferramentas que garantem o controlo da propriedade sobre a gestão são o conselho de Administração, a auditoria independente e o conselho Fiscal. As boas Práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilita seu acesso ao capital e contribuir para a sua perenidade."

Muitas outras definições de *Corporate Governance* têm sido emanadas pelas mais diversas organizações todas elas com um conceito chave que se foca na melhoria da confiança dos *stakeholders,* assim como na maior responsabilização da administração por actos de gestão menos cuidados. Outro dos factores sempre implícito no conceito de *Corporate Governance,* foca-se na adopção de boas práticas de governação por parte da administração. As *best practices* como são comummente conhecidas estão intimamente relacionadas com *benchmarking,* que também é considerado na essência do conceito em apreço. A utilização desta técnica consiste na identificação dos resultados das melhores práticas utilizadas nos diferentes processos de negócio e funções empresariais, com especial destaque para aqueles cujo impacto no desempenho permita assegurar e sustentar vantagens competitivas para a empresa.

Do estudo feito constatou-se que a adopção dos princípios de *Corporate Governance* associados a um bom desempenho do DAI, poderá fazer com que

muitos dos riscos inerentes à própria actividade sejam mais facilmente detectados, reportados e desde logo mitigados, conferindo assim valor acrescentado à empresa que opta pela implementação destes princípios cada vez mais em voga.

Os principios supra referenciados, estão intimamente relacionados com a implementação de eficazes CI para assim promover uma maior agilidade na gestão de todos os riscos inerentes à própria actividade, com vista a evitar situações como as que já foram vivenciadas por muitas empresas um pouco por todo o mundo, como são os casos de falencias fraudulentas de várias empresas como a Enron e Parmalat, entre outras. Os princípios de *Corporate Governance* não constituem o garante de uma eficaz gestão de riscos, para isso será necessária a existência de sólidos SCI, para que em aliança confiram valor acrescentado à organização, poupando-a de correr alguns riscos, ou pelo menos ter um maior controlo sobre os mesmos, facto esse que ao não se verificar poderá por em causa a sua continuidade.

Como já foi oportunamente referido, o conceito de *Corporate Govenrance* rege-se por um conjunto de princípios basilares que têm por finalidade acrescentar valor à empresa, fazendo com que esta se possa destacar dos mais directos concorrentes visando assim a melhoria da sua *performance* e consequente continuidade. Seguidamente elencam-se alguns dos principais objectivos e princípios do C*orporate Governance.*

- Assegurar a confiança e integridade da informação;
- Assegurar a observância de políticas, planos, procedimentos e legislação em vigor;
- Assegurar a custódia de activos;

- Assegurar a utilização económica e eficiente dos recursos.
- Acrescentar valor accionista;
- Assegurar a realização dos objectivos e metas fixadas para as operações;
- Avaliar e responsabilizar a gestão por actos praticados;
- Gerir tendo em conta a responsabilidade social.

Como se pode constatar pela explanação feita, todos estes princípios se cruzam de muito perto com os objectivos da AI, daí ser cada vez mais perceptível a interligação e conjugação de factores existentes entre a AI e o *Corporate Governance*.

2.4.2 - Relatório Turnbull

Considera-se importante no âmbito do trabalho em apreço, fazer uma breve referência ao relatório *Turnbull*, dadas as suas características muito baseadas na gestão de risco.

O estudo "*Internal Control: Guidance for directors on the Combined Code*", conhecido por *Turnbull Report*, nasceu nos anos 90 no Reino Unido, como resultado das preocupações em relação ao relato financeiro pouco fidedigno.

O relatório *Turnbull* teve como objectivo não apenas o cumprimento formal de um mero método de controlo e gestão de riscos, mas também, uma oportunidade para que este processo se ligasse aos objectivos da empresa enquanto factor de vantagem competitiva.

De acordo com *MOELLER* (2005) no contexto de *Turnbull*, o que é realmente importante é a ênfase especial atribuída ao desenvolvimento de processos de controlo dirigidos aos riscos com alto impacto e com elevada probabilidade de ocorrência. – matriz de risco.

Ainda de acordo com este autor, possivelmente associado ao facto, de no passado os auditores internos no Reino Unido, algumas vezes, serem vistos mais como um polícia na empresa, *Turnbull* realçou a importância do auditor interno no incremento do *framework* do CI.

Desenvolvido antes da *SOX*, este é um excelente guia para os auditores internos interpretarem os riscos e ajudarem a desenvolver a estrutura de CI em qualquer organização a nível Mundial.

Em suma o relatório *Turnbull*, resulta de um outro, o *Combined Code*, trata-se de um relatório que dá primazia ao risco do negócio, salienta nesta perspectiva que o CI será um importante instrumento para auxiliar na análise do risco de negócio, que ao ser bem analisado trará vantagens competitivas, este paralelamentre ao *Cadbury*, rege-se pelas boas práticas de negócio.

2.4.3 - Basileia – A Gestão de Risco no Sector Bancário

Ainda no ambito da gestão de risco e visto tratar-se de um documento elementar nesta matéria, considera-se importante abordar o acordo Basileia. Trata-se de um acordo assinado em 1988 na cidade de Basileia (Suíça), ratificado por mais de cem países. Constitui este um comité de supervisão bancária que tem por objectivo a criação de exigências mínimas de capital que devem ser respeitadas pelos bancos comerciais, como precaução contra o risco de crédito , desempenhando assim um importante papel na gestão de risco.

Os objectivos deste acordo prendem-se com a criação de novas abordagens de supervisão, através de uma troca de informação entre organismos. Um dos factores prende-se com a assunção de um capital mínimo a ser adoptado pelos bancos, mais propriamente 8% face ao seu total de activos, ou seja deverão possuir um rácio mínimo de solvabilidade, visando assim a manutenção da solidez e estabilidade do SBI.

Contudo, a expansão do crédito baseada numa maior exposição aos diversos riscos terá despoletado a deterioração dos rácios de capital e a falência de grandes bancos internacionais. É então que em Junho de 2004, este comité de supervisão lança um novo documento em substituição do acordo de 1988. O Basileia II, como ficou conhecido, surge como mais uma resposta ao risco, assente num tratamento de dados mais avançado, estruturado em três pilares incluindo um tipo de risco negligenciado no Basileia I, o risco operacional, trata-se assim de uma atitude menos reactiva, abarcando o surgimento de novos ou modificados produtos financeiros, e com estes, outros tipos de risco.

Os objectivos declarados neste novo acordo centram-se no desenvolvimento de uma estrutura que fortaleça a solidez e a estabilidade do SBI e a uniformização de critérios tendo em vista uma adequação do capital não geradora de desigualdades entre os bancos que operam internacionalmente.

Este comité define o risco operacional como "o risco de perdas resultantes de falhas ou inadequação de processos internos, pessoas e sistemas ou devido a factores externos" Através deste acordo são identificadas diversas categorias de risco, das quais se destacam as fraudes, quer sejam internas ou externas, danos em activos físicos, falhas nos sistemas entre outros aspectos que em potência poderiam degenerar em perdas que afectariam a estabilidade da actividade bancária.

A estruturação do novo acordo em três pilares, por seu turno, assenta nos seguintes termos:

- O pilar I (alocação de capital) regula as exigências mínimas de fundos próprios mais sensível ao risco, abarcando a previsão de cobertura dos riscos de crédito, de mercado e operacional;
- O pilar II (supervisão) diz respeito ao processo de convergência das políticas e práticas de supervisão, os princípios daqui emanados podem eventualmente originar medidas de excepção, ou de outro modo, de flexibilização das exigências inicialmente previstas, tais como a fixação de requisitos mínimos diferenciados, em função dos perfis de risco ou da solidez dos sistemas de gestão ou ainda pelo SCI das instituições;
- O pilar III (transparência) destina-se a fixar um conjunto de exigências de divulgação que permitirão ao mercado uma informação mais sustentada sobre o capital, a exposição e o processo de gestão de risco

subjacente a cada banco, sem prejuízo da existência de informações de carácter confidencial.

A combinação desta estrutura resulta numa clara tentativa de assegurar um capital mínimo adequado à cobertura dos vários riscos, como são o de mercado, de crédito e operacional; incentivando os bancos a desenvolverem e utilizarem técnicas de gestão e monitorização dos riscos aos quais estão sujeitos. Isto possibilita a delegação de poderes às entidades de supervisão para controlar a forma como os bancos avaliam as necessidades de capital e risco permitindo assim corresponder às expectativas de informação mais atempada e transparente por parte dos utentes.

No que à AI diz respeito, pode ainda referir-se que para além da função de avaliação do risco operacional, este acordo assume também um papel activo na implantação de um programa de gestão de risco operacional, o que mostra um verdadeiro contributo na mitigação dos riscos associados a este sector, nomeadamente o risco de crédito.

CAPÍTULO 3 - Controlo Interno

*"Um bom controlo interno previne mais desfalques do que os bons auditores encontram" - Arens, A., Elder, R. e Beasley, M. (*2006)

3.1 - Conceito – Definição e Evolução

Antes de partir para a definição e explanação do que consiste o CI importa alertar para o facto de não existir uma uniformidade de pensamento quando à sua definição, apesar de muito se ter evoluído quanto à percepção da sua importância para uma organização.

A essência subjacente a este conceito como hoje se conhece, resulta de uma evolução ocorrida ao longo do tempo e que se deu paralelamente ao desenvolvimento da AI, motivada pela separação entre titularidade do capital e respectiva gestão.

Seguidamente são apresentadas algumas definições de CI, emanadas por diversos organismos e/ou autores, no intuito de melhor evidenciar a essência subjacente ao conceito.

" O controlo interno compreende o plano da organização e o conjunto coordenado de métodos e medidas, adoptados pela empresa, para proteger o seu património, verificar a exactidão e a fidedignidade dos seus dados contabilísticos, promover a eficiência operacional e encorajar a adesão à política traçada pela administração."

American Institute of Certified Public Accountants (AICPA), no Relatório Especial da Comissão de Procedimentos de Auditoria.

Já a Comissão *Treadway* - Criada pelo congresso Americano, que visou inicialmente o estudo de medidas para combater a fraude, tendo evoluído posteriormente para estudos sobre o CI, e que engloba além de elementos do Congresso Americano, elementos de associações profissionais Americanas dos quais alguns membros do Institute of Internal Auditors (IIA) – tinha como definição de controlo interno:

> *"Processo desenvolvido pela administração, gestão e restante pessoal com a finalidade de oferecer uma garantia razoável de que os objectivos da organização são atingidos."*

Outros conceitos se conhecem, como o desenvolvido pelos autores *BOYNTON, W.C. JOHNSON, RN.; Kell, W.G., (2002)* e que consta do seguinte:

> *"Controlo interno é um processo desenvolvido pelo Conselho de Administração e outras pessoas, desenhado para fornecer segurança razoável quanto à consecução de objectivos nas seguintes áreas: confidencialidade de informações financeiras; cumprimento e observância de leis e regulamentos aplicáveis (compliance); eficácia e eficiência das operações."*

De uma forma muito simplista, e segundo uma definição emanada pelo IIA, o CI consta do *"conjunto ou práticas utilizadas para evitar ou detectar actividade não autorizada"*, como é sabido a definição não se esgota nesta frase pois o CI como foi dado a conhecer anteriormente é muito mais do que isto, este tem sempre em consideração a consecução dos objectivos traçados pela empresa.

Considerou-se pertinente apresentar também o conceito SCI presente na Directriz de Revisão e Auditoria (DRA) 410 referente ao SCI:

> *"Sistema de controlo interno significa 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."*

Já o *Public Company Accounting Oversight Board* (PCAOB), define CI como:

> *"Processo desenhado por, ou sob a supervisão da gestão da empresa e por si efectivado, 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 aqueles princípios e procedimentos que:*
>
> - *Respeitam à manutenção dos registos que, com detalhe razoável, precisa e imparcialmente reflectem as transacções e a organização dos activos da empresa;*
> - *Prestam segurança razoável que as transacções são registadas quando necessárias para permitir a preparação das demonstrações financeiras de acordo com os princípios contabilísticos geralmente*

aceites, e que as receitas e as despesas da empresa são efectuadas de acordo com as autorizações da gestão e da direcção da empresa;

- *Promovem segurança razoável quanto à prevenção ou detecção atempada de aquisições não autorizadas, uso ou descarte dos activos da empresa, que possam ter um efeito material nas demonstrações financeiras."*

Perante a análise dos diferentes conceitos pode definir-se SCI como o conjunto de regras, políticas e procedimentos, concebidos pela Administração, como forma de auxiliar a organização a atingir todo um conjunto de objectivos operacionais e não só.

Segundo a perspectiva proposta por JUNIOR (2005), um SCI tem como principal desiderato promover a eficiência e a eficácia das operações, tendo em conta a melhoria da performance, da rentabilidade e da salvaguarda de activos, tendo ainda uma componente direccionada para a fiabilidade do relato financeiro para os *stakeholders*.

3.1.1 - A Lei Sarbannes-Oxley e o Controlo Interno

O organismo acima referido PCAOB nasceu da *Lei Sarbannes-Oxley* (SOX), elaborada pelos senadores *Paul Sarbanes* (Democrata de Maryland) e *Michael Oxley* (Republicano de Ohio). Esta implementou regras e medidas que até então não eram consideradas, incrementou uma nova perspectiva no governo das sociedades, até pela responsabilização criminal atribuída aos administradores, até então um pouco descurada.

A Lei *SOX* privilegia assim o papel crítico do CI como um processo implementado pela administração ou por outras pessoas da empresa que impulsionam o sucesso dos negócios em três categorias:

- Eficácia e eficiência das operações;
- Confiança do relato financeiro;
- Cumprimento de leis e regulamentos aplicáveis.

Esta está dividida em onze capítulos ou títulos, no ambito do estudo apresentado destaque-se a seção 404, dado que esta se debruça sobre a responsabilização do CEO e CFO pelo estabelecimento e manutenção de um adequado SCI, garantindo que este se ajusta à estrutura organizacional.

Trata-se de uma Lei cujo contributo para as empresas foi bastante pronunciado, pese embora o facto de ter sido criada posteriormente à ocorrência de alguns factos fraudulentos, como é o caso do escândalo financeiro da *Enron* nos EUA, constata-se que peca apenas por ser uma lei tardiamente criada.

3.2 - Sistema de Controlo Interno na Gestão de Risco – Vantagens e Limitações

A implementação de um SCI numa empresa afigura-se repleta de vantagens, pois, antes de mais, permite que haja um maior controlo sobre um conjunto de factores que poderão degenerar em riscos associados à sua actividade e a toda a sua envolvente. Para que a sua implementação seja, realmente, vantasoja é necessário desenvolver todo um trabalho de levantamento das reais necessidades, áreas mais susceptíveis e avaliação dos diversos riscos associados à actividade como um todo, assim como aqueles ligados a situações mais específicas. Destaca-se assim a importancia que terá o DAI no auxílio que poderá dar na informação prestada e contributo na implementação de um SCI.

Daqui se infere a extrema importância que tem um bom sistema de informação, dentro de uma organização, pois se este tiver um potente fluxo, poderão ser identificadas situações que carecem de melhoria, dando assim origem à tomada de importantes decisões.

Contudo, há que ter em conta que os SCI não são uma grantia no que diz respeito à consecução dos objectivos propostos pela administração, pois estes por si só, não asseguram que a empresa consiga alcançar todos os intentos a que se propõe. Uma empresa por ter implementado um SCI, não consegue afiançar, aos diversos *stakeholders*, que as informações contidas nas suas DF são absolutamente reais e desprovidas de erros materiais, pois os SCI não estão imunes a atitudes fraudulentas que consigam ludibriar o sistema, facto este que infelizmente nos dias que correm cada vez mais acontece.

Desta forma constata-se que existem inúmeros agentes que poderão fragilizar um SCI, contudo, entende-se que um dos factores que poderá minimizar, e muito, as falhas ocorridas dentro de uma empresa prende-se com a consciência ética e brio profissional que todos os colaboradores deverão ter. Estes ao terem uma conduta de ética e postura profissional contribuem à partida para uma melhoria no funcionamento do CI, pois este por muito bom que seja não conseguirá resitir a atitudes de índole fraudulenta e de falta de ética.

Finalmente e no que se refere à gestão de riscos empresariais, considera-se que a implementação de um SCI contribui para uma melhor identificação dos riscos decorrentes de falhas operacionais, mesmo que estas sejam não intencionais. Um bom SCI permite a identificação dessas mesmas deficiências minimizando-as, isto se não for de todo possível a sua total eliminação, contribuindo assim para uma melhoria dos procedimentos que consequentemente terão reflexo nos resultados da empresa.

Daqui se conclui que um SCI deverá fazer parte da cultura e da gestão da própria empresa e assim permitir responder com rapidez aos riscos relacionados com o negócio.

Contudo, considera-se que um mecanismo de controlo só deverá ser implementado caso o seu benefício, em termos operacionais, seja superior ao seu custo, tornando-se assim favorável e suportável pela empresa.

3.3 - Modelos de Controlo Interno

Existem vários modelos de CI, todos eles divulgados por organizações profissionais, segundo a opinião de BOWEN (2002), os mais relevantes são:

- COBIT – *Control Objectives for Information and Related Technology* – Trata-se de um *framework* que funciona como um guia de boas práticas aplicado às Tecnologias de Informação. Este possibilita a implementação de controlos objectivos que irão auxiliar na gestão e optimização de Tecnologias de Informação.

- SAC – "*System Auditability and Control"* – Trata-se de um sistema editado em 1991 por "*Internal Auditors Research Foundation*", posteriormente revisto em 1994 que pretende dar suporte aos auditores internos no controlo de sistemas de informação e tecnologia.

- COSO – "Internal Control – Integrated Framework" – Criado em 1992 pelo "*Comittee of Sponsoring Organizations of the Treadway Commission*". Este documento é constituído por um conjunto de recomendações de como avaliar, relatar e melhorar os SCI das entidades.

- CoCo – "*Criteria of Control Board – Guidance on Assessing Control – The CoCo Principles*" - Este documento foi editado em Junho de 1997 pelo "*The Canadian Institute of Chartered Accountants"*.

Todos os modelos anteriormente apresentados têm aplicabilidade um pouco por todo o Mundo, no desenho e implementação de um SCI, não se verificando a obrigatoriedade da aplicação de um modelo em concreto.

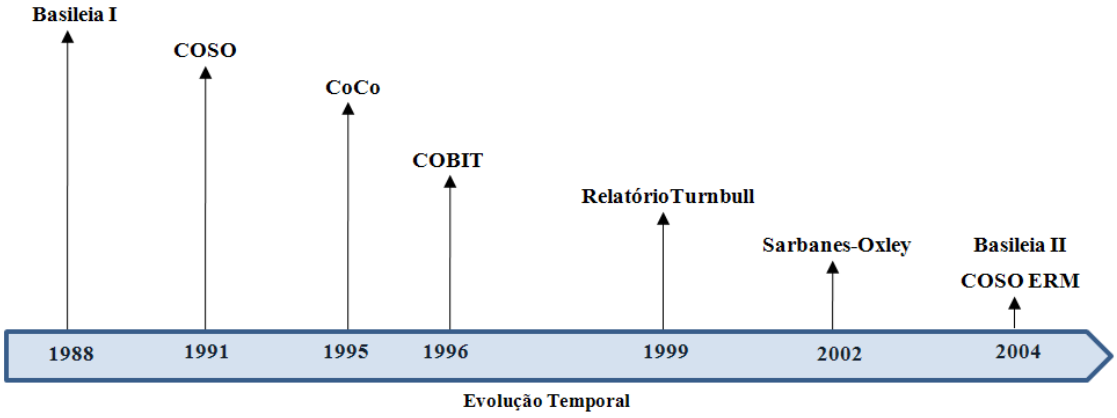
Destes se destaca o modelo do COSO, sendo o mais conhecido, até porque de todos os apresentados é aquele que se afigura transversal a toda a organização tendo sido inclusivamente introduzido pela Comissão Europeia como modelo de suporte ao SCI. [MORAN 2001 apud SANTOS *et al.*].

Muitas organizações profissionais de auditoria consideram que a aceitação do Modelo do COSO como estrutura base de CI, aumentará as possibilidades de ter um sistema de controlo fiável, isto pelas características que este modelo congrega.

No capítulo seguinte será feita uma análise a este modelo, nomeadamente no que respeita à sua origem e objectivos, transformações sofridas e aos seus componentes.

Apresenta-se seguidamente um esquema representativo e cronológicamente ordenado da evolução de alguns modelos de CI, assim como normas e regulamentos que contribuiram para a evolução desenvolvida ao longo dos tempos.

Figura nº 3 – Evolução dos normativos e modelos de CI



Fonte: Elaboração Própria

3.3.1 - Modelo do COSO

Tal como referido, em 1992 foi criado o COSO, formado nos Estados Unidos e composto por uma comissão das principais associações de profissionais ligadas à área, entre elas *AICPA*, *IIA*, *AAA*, *IMA e FEI*, que em conjunto desenvolveram o protocolo *COSO I*, também conhecido como *"The COSO Report"*. Este relatório visava uma maior observância na análise e gestão de riscos internos e externos inerentes a toda a actividade de uma organização. [BERGAMINI. 2005].

O COSO tem como finalidade principal analisar e melhorar a performance e desempenho dos CI implementados por uma entidade, tendo em vista o cumprimento dos objectivos propostos. Para isso construiu uma estrutura integrada baseada em três princípios fundamentais:

i) Eficácia e eficiência das operações;

ii) Fiabilidades do relato financeiros;

iii) Conformidade com leis e regulamentos.

O *COSO I* é ambém conhecido por *COSO Report*, constitui um modelo de controlo que deve ser adaptado às necessidades e particularidades de cada empresa para assim poder resultar de forma eficaz na avaliação e análise de CI. Este pretende tornar-se num instrumento que viabiliza e promove a obtenção de um elevado grau de transparência das Demonstrações Financeiras.

3.3.1.1 - Princípios do *COSO*

O referencial COSO baseia-se nos seguintes princípios básicos:

- O CI constitui um processo: é um meio e não um fim;
- O CI depende de cada um: não se limita a uma recolha de procedimentos, necessita da intervenção de todos em cada um dos níveis da estrutura organiacional – Transversal a toda a organização;
- O CI deve procurar uma segurança razoável (mas não absoluta) de uma gestão e de uma administração cumpridora do quadro legislativo;
- O controlo interno deve ser adaptado à concretização efectiva dos objectivos.

Figura nº 4 – Cubo do COSO

Fonte: COSO 2004

O referencial COSO define o CI como um processo em execução pelos diferentes níveis de dirigentes da organização, destinado a fornecer uma razoável segurança quanto à realização dos três objectivos seguintes:

1. Realização e optimização das operações;
2. Fiabilidade das informações financeiras;
3. Conformidade legal e regulamentar.

A combinação destes três objectivos dos cinco componentes (ambiente de controlo, definição e análise de riscos, actividades de controlo, informação e comunicação, acompanhamento e monitorização) e das estruturas da organização, vistos sob três eixos de análise distintos, constituem o designado cubo do COSO representado na figura acima.

3.3.2 - COSO II – Enterprise Risk Management - ERM

Com o passar do tempo, particularmente pela ocorrência de alguns escândalos financeiros, o COSO passou a reconhecer o interesse não apenas no controlo dos processos, mas também numa gestão efectiva e eficaz do risco. Daqui resultou a elaboração de um novo modelo que surge em 2001, o *Enterprise Risk Management - Integrated Framework,* intitulado COSO II ou COSO ERM, que pode ser visto como uma versão melhorada do COSO I ou COSO Report.

O COSO ERM, além de preservar a estrutura integrada do anterior modelo, explora o CI mais extensivamente no que se refere à gestão de risco de uma organização. A premissa subjacente à gestão de risco empresarial é definida como um processo

efectuado e aplicado na empresa, disposto a projectar e identificar os eventos potenciais que podessem afectar a entidade, reduzindo o risco de forma a fornecer uma garantia razoável a respeito da realização dos objectivos da entidade [*COSO*: 2006].

Para a realização dos objectivos fundamentais estabelecidos na missão e visão da organização, o modelo estrutural sugerido no relatório *Enterprise Risk Management - ERM,* que a gestão de riscos precisa de definir 4 factores principais:

Estrategic - As estratégias*;*

Operations – Utilização eficaz e eficiente dos recursos;

Reporting - Reproduzir através de relatórios as decisões e resultados*;*

Compliance - Respeitar as leis e regulamentos impostos pela gestão.

O quadro apresentado pelo supracitado modelo contempla uma nova estratégia mais baseada na gestão de risco, destacando-se a noção de "*risk appetite*" como a principal novidade do COSO II, comparativamente ao COSO I. Trata-se do 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. Distintas estratégias colocarão a empresa exposta a diferentes tipos de riscos.

Figura nº 5 – Cubo do COSO ERM

Fonte: COSO – The Commitee of sponsiring Organizations of the Treadway Commission – PEREIRA.

Da análise do cubo é possível observarem-se quatro tipos de objectivos: Estratégicos, Operacionais, de Comunicação e Conformidade, estando estes posicionados verticalmente na estrutura do referido cubo. Observam-se ainda os oito componentes da gestão de risco, dispostos de forma horizontal, finalmente existem as quatro unidades de uma organização, constituindo assim uma terceira dimensão. Todos eles se inter-relacionam entre si de forma a alcançar uma melhor gestão de todos os riscos inerentes a uma determinada actividade ou sector de negócio onde uma organização se insere.

O modelo tridimensional de gestão de risco – COSO ERM sofreu, tal como anteriormente se verificou, um incremento de mais três elementos comparativemente ao que se passava no COSO I, desta feita destacam-se os elementos que o constituem:

Ambiente Interno – Tal como já acontecia no modelo anterior, este abrange a cultura da organização. O ambiente interno é a base para todos os outros

componentes da gestão de risco, sendo muito dominado pela própria história e cultura da empresa bem como pela filosofia da administração. Trata-se, portanto, de um componente muito influenciado pelo modo como são estabelecidas as estratégias e os objectivos da empresa, estruturados e identificados os negócios, avaliados e geridos os riscos. É através deste componente (ambiente de interno) que se define a filosofia de gestão do risco, assim como a integridade, valores éticos e ambiente em que a entidade opera.

Definição de Objectivos - Os objectivos são fixados no âmbito estratégico, estabelecendo uma base para os objectivos operacionais, de comunicação e de cumprimento de normas. Toda a organização enfrenta uma variedade de riscos oriundos de fontes externas e internas, sendo a fixação de objectivos um pré-requisito para a identificação eficaz de situações de potencial risco. Os objectivos são alinhados com o "*risk appetite*", o qual direcciona os níveis de tolerância ao risco que a organização está disposta a assumir.

Identificações de Eventos – Todos os acontecimentos, quer sejam internos ou externos, podem afectar a execução dos objectivos da empresa, desta forma, devem ser identificados sendo posteriormente agrupados e classificados enquanto riscos e oportunidades. Desta feita, as oportunidades serão canalizadas e concertadas em função dos objectivos da entidade, sendo os riscos tratados em conformidade com a política de gestão de risco da empesa, tendo sempre em conta o seu "*risk appetite"*.

Avaliação do Risco – Este componente alerta para a importância existente na análise e avaliação do risco, pois os riscos detectados deverão ser analisados tendo em conta o binómio probabilidade/impacto, tal como explicado no capítulo de

Gestão de Risco Empresarial, por forma a ser promovida uma adequada estratégia de abordagem ao risco.

Resposta ao Risco - Feita a devida análise ao risco e tendo sempre em conta até onde a empresa está disposta a aceitá-lo – *risk appetite* – há que delinear a estratégia a seguir – EVITAR, REDUZIR ou ACEITAR – de acordo com a abordagem feita no capítulo subordinado à Gestão de Risco Empresarial. Sendo a responsabilidade da decisão sobre qual a estratégia a adoptar relativamente ao risco exclusivamente da administração.

Actividades de Controlo – Trata-se de todo o conjunto de políticas, mecanismos e procedimentos estabelecidos e utilizados para ajudar a dar resposta aos riscos aos quais a entidade pode estar exposta;

Informação e Comunicação – Hoje em dia cada vez mais se denota a importância assumida pela informação e comunicação dentro de uma organização, sendo esta considerada por muitos, uma vantagem relativamente aos demais concorrentes. Toda a informação digna desse nome, isto é, a que é efectivamente considerada relevante, é identificada analisada e difundida hierarquicamente por toda a organização, permitindo assim uma melhor e mais eficaz definição de responsabilidades, minimizando a probabilidade de ocorrência de distorções por má interpretação das funções e/ou procedimentos estipulados;

Monitorização – Trata-se de uma importantíssima etapa no processo de gestão de riscos, pois permite observar o evoluir e adaptação da empresa aos riscos por si incorridos, permitirá também realizar adaptações e modificações graduais às alterações propostas, caso estas sejam necessárias.

CAPÍTULO 4 - AUDITORIA INTERNA

4.1 - Evolução e Definição de Auditoria Interna

Como já foi oportunamente referido, o conceito de AI como hoje é conhecido resultou de um conjunto de modificações sucessivas que foram ocorrendo desde a sua génese até aos dias que correm.

Ao contrário da contabilidade que teve no Frade *Luca Paccioli* o seu início, a história da auditoria não é tão precisa, segundo relatam os escritos esta surgiu através de um então eficiente guarda-livros ao serviço de um mercador italiano do Séc. XV ou XVI, que pela sua reputação e sabedoria em matéria contável começou a ser consultado por outros mercadores para analisar a escrituração das suas transacções.

Outras teorias há que apontam no sentido dos primórdios de auditoria remontarem ao Egipto e à Babilónia, em que a auditoria se consubstanciava no apuramento e exactidão dos registos. Há ainda quem considere que esta surge como forma de audição das contas das fazendas privada dos feudos.

Epistemologicamente a palavra auditoria teve a sua origem no verbo latino "*audire*" que significa ouvir, o que levou a que se formasse a palavra auditor, que deriva igualmente do Latim "*Auditore*", aquele que ouve, o responsável por ouvir, dado que inicialmente os então auditores baseavam as suas análises e posteriores conclusões apenas na matéria que ouviam, não havendo nenhum outro tipo de evidência a não ser aquela.

A evolução da auditoria tal como é hoje, é um reflexo do que aconteceu no passado, em muito influenciada pela revolução industrial que começou na Grã-Bretanha por volta de 1780.

Esta revolução permitiu o surgimento de muitas empresas industriais cuja estrutura funcional e burocrática era já de uma dimensão considerável para a época, obrigando a uma procura de financiamentos externos para passar a projectos mais ambiciosos e consequente expansão. Isto gerou a necessidade de avaliação dessas empresas, de forma a verificar a capacidade de retorno dos investimentos.

Começava então a notar-se um distanciamento entre a posição de detentor do capital e a de gestor desse mesmo capital, o que motivou o aparecimento da função de auditoria nos moldes actuais.

4.1.1 - Mudança de Paradigma

A AI é hoje uma função bastante mais conhecida do que há alguns anos, este aumento de notoriedade faz com que haja um maior reconhecimento da própria profissão, permitindo assim que ocorram trocas de experiências e que de alguma maneira esta se desenvolva um pouco mais. [PINHEIRO 2005]

Anteriormente um dos principais objectivos desta função centrava-se na detecção de fraudes ocorridas dentro da empresa cometidas pelos próprios colaboradores, daí existir ainda hoje o estigma relativamente a AI, pois tratava-se de uma função não muito apreciada pela generalidade dos colaboradores da organização, dado o seu cariz de fiscalização – forma como era encarada por estes. A AI tinha a missão de promover a salvaguarda de activos, assim como a segregação de funções de maneira a haver um maior controlo em toda a hierarquia da organização, a par de tudo isto,

competia ainda ao departamento de AI garantir a fidedignidade dos registos contabilísticos.

Segundo PINHEIRO (2005), deu-se uma evolução deste conceito, pois a profissão foi evoluindo e atingindo os seus propósitos e objectivos de acordo com o que se esperava dela, como anteriormente foi referido. Começou a notar-se uma necessidade de repensar a função do auditor, nessa altura a auditoria passou a ter um papel não só de detecção de fraude, mas também centrou o seu foco na prevenção da mesma. Entre outras valências esta função acabou por ter um cariz mais proactivo, tentando estar sempre um passo a frente, para assim desempenhar cabalmente a missão para a qual foi projectada.

A partir de 1980 a AI ganha uma maior projecção, assistindo-se assim a um alargamento progressivo do seu âmbito, passando este trabalho a incluir um conjunto muito mais amplo de análise às operações, recursos e controlos. Passados dez anos a Auditoria assume, de facto, a importância que se conhece actualmente, apesar de ainda hoje em Portugal se considerar que tem muito para progredir. Trata-se de uma função muito mais abrangente e sistemática do que já foi e a sua actividade baseia-se cada vez mais no auxílio na identificação e gestão dos riscos das organizações.

A Eficiência, Eficácia e Economia passaram a ser dos aspectos mais importantes e a ter em conta para a função de AI, um dos intuitos desta é facultar informações à empresa que lhe permitam tomar as melhores decisões, dai ser importante ter preocupações de cariz económico, tendo sempre em vista a eficiência e eficácia das operações, alocando apenas os recursos necessários a um determinado objectivo. [BEURAN 2000]

Verifica-se assim que a função da AI está hoje intimamente ligada à gestão de risco, dado que é esta função que permite à gestão de topo ter acesso a um conjunto de informações que a auxiliarão numa eficaz tomada de decisões sobre a forma como deverá ser encarada a abordagem e fazer face ao risco a que a empresa está sujeita.

Foi esta evolução traduzida na mudança de paradigma acima evidenciada que conduziu às actuais definições de AI que seguidamente se apresentam.

Segundo a perspectiva do *IIA – The Institute of Internal Auditors, Inc*. temos que:

> *"Auditoria Interna é uma função de apreciação independente no seio da organização, para contribuir para uma gestão adequada dos recursos e dos meios colocados à disposição dos elementos constituintes da organização."*

A anterior definição sofreu algumas alterações, sendo dada uma maior relevância à relação existente entre o auditor interno e a empresa, numa perspectiva de *Corporate Governance*, ou seja, incremento de valor, surgindo assim uma nova definição:

> *"Actividade independente, de avaliação objectiva e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste a organização na consecução dos seus objectivos, através de uma abordagem sistemática e disciplina, na avaliação da eficácia dos processos de gestão de risco, o controlo e governação."*

Existem ainda muitas outras definições emanadas pelos mais diversos organismos e entidades, como é o exemplo da que é considerada pela empresa *Jonhson & Jonhson*, que consta do seguinte:

> *"A Auditoria Interna tem a função de apoiar os gestores centrais e operacionais da empresa na execução efectiva e eficiente das suas responsabilidades fornecendo-lhes critérios, objectivos, análise, avaliações, observações, recomendações relacionadas com a melhoria de controlo dentro de toda a organização. A auditoria interna gere a integridade de desempenho da gestão, a eficiência operacional e a correcção os relatórios financeiros".*

Como se verificou pela análise das diversas definições aqui expostas, todas elas têm um elo em comum, que se prende com o facto da função de AI ser considerada um importante auxílio para a gestão de uma organização. Contribuido das mais diversas formas para que esta esteja preparada para os riscos que poderá correr, permitindo uma eficaz alocação recusros, que consequentemente reverterá numa diminuição de potenciais perdas.

4.2 - O Departamento de Auditoria Interna – Principais características

Importa exaltar a importância associada à independência que um DAI deverá manter, para assim cumprir da melhor forma a função para a qual foi implementado. Neste departamento deverão ser verificados requisitos que permitam uma total imparcialidade e independência nas análises efectuadas, tais como possuir uma diferenciada posição hierárquica, relativamente aos departamentos ou elementos alvo da auditoria. Só assim o trabalho terá o desiderato pretendido, permitindo o reporte, dando assim importantes informações que permitirão a implementação de medidas correctivas no sentido de optimizar procedimentos auxiliando também no processo de gestão de riscos.

A AI deverá ser implementada ou requerida através de expressa vontade da administração ou dos demais *stakeholders,* sendo estes os primeiros interessados em que esta funcione bem e seja eficaz, daí terem um importante papel no esforço a fazer para que isso aconteça.

No que à independência diz respeito, muito se tem vindo a discutir ao longo dos tempos, pois esta deverá ser exigida relativamente às áreas objecto de análise. Considera-se que por vezes poderá da-se o caso desta se dissipar um pouco, aquando da avaliação do SCI, pois este, ao ser desenhado e implementado pela administração, poderá fazer com que o auditor interno ao opinar negativamente sobre o mesmo poderá estar, em certa medida, a pôr em causa o trabalho executado pelo seu mais directo responsável hierárquico. Este facto é passivel de não ser bem aceite, o que poderá colocar o auditor e o seu departamento numa situação pouco confortável perante a sua mais directa chefia.

Esta situação, teoricamente, não acontece, mas percepciona-se que em algumas condições muito concretas a teoria distancia-se um pouco do que acontece na prática, sendo esta apenas uma mera opinião.

Em suma a independência exigida num trabalho de auditoria externa difere um pouco da independência pretendida num trabalho de AI, pois no primeiro caso, deverá ser mais explícita quer perante os *stakeholders* e sociedade em geral, sendo de aplicar a esta a célebre frase: " à mulher de César não basta sê-lo há que parecê-lo".

No que respeita à AI, o auditor deverá ter uma independência que lhe permita efectuar uma análise crítica e isenta dos procedimentos e processos, para assim poder emitir informação útil que permita à empresa uma adequada tomada de decisões, no sentido de alcançar os objectivos que estão para si estabelecidos.

Pode assim concluir-se que em AI a verdadeira independência possibilita que a crítica feita relativamente a procedimentos e métodos de trabalho estabelecidos se converta, efectivamente, uma mais-valia para a melhoria da performance da organização.

Considera-se importante que um DAI consiga reflectir a *Missão*, a *Visão* e os *Valores* pelos quais se rege a empresa, para que assim seja mais fácil atingir os *Objectivos estratégicos* da organização.

4.2.1 - O Trabalho do Departamento de Auditoria Interna

Todo o trabalho de AI, deverá ter como ponto de partida um detalhado e exaustivo planeamento de todas as tarefas a efectuar, pois, é a partir daqui que se consegue delinear a estratégia a seguir para a consecução dos objectivos estabelecidos. Nesta

fase deverá ser delineado um plano de acções de forma a cobrir com transversalidade todas as áreas da empresa onde exista risco associado, pois não fará sentido alocar recursos a um sector onde o risco seja materialmente irrelevante.

Outro aspecto importante prende-se com o "timing" dos resultados, pois um trabalho de auditoria só terá o efeito desejado, isto é, incrementar valor na empresa caso seja tempestivamente reportado, permitindo que ocorram assim melhorias significativas no CI e consequentemente nas várias áreas da empresa, permitindo que sejam tomadas decisões que poderão fazer a diferença entre manter uma posição sólida no mercado ou mesmo perde-la.

4.2.1.1 - Fases do trabalho de uma Auditoria Interna

Antes de se dar inicio a um trabalho de AI é necessário ter em conta vários factores que poderão influenciar o resultado do mesmo, será neste caso fundamental adquirir um profundo conhecimento dos processos internos da empresa, da estrutura orgânica e funcional, assim como de todo o SCI.

Planeamento

O planeamento num trabalho de AI, reveste-se de uma importância capital, pois é por esta parte que começa a delinear-se todo o trabalho a realizar. É aqui que se verificam quais os principais factores de risco associados à empresa e ao sector de actividade em que esta opera, permitindo assim adaptar melhor o trabalho a efectuar e testar as áreas mais susceptíveis, tendo sempre em conta os objectivos da actividade alvo do trabalho de auditoria.

Seguidamente elencam-se alguns factores de risco que deverão ser tidos em consideração aquando do planeamento de um trabalho de AI, para que a análise do risco associado ao negócio seja fidedigna, permitindo assim ao DAI ou responsável pelo trabalho optimiza-lo ao máximo.

- - Risco de mercado – Trata-se da análise que é feita ao sector de actividade em que a empresa se encontra inserida, e de qual o seu comportamento dentro do mesmo, ou seja, qual a sua performance em mercado aberto tendo em conta toda a concorrência, situações de monopólio entre outros factores.

- - Complexidade das operações – Trata-se de um factor importante para a quantificação do nível de risco a que uma empresa está sujeita, pois o risco aumenta na proporção da complexidade e quantidade das operações desenvolvidas por uma determinada entidade. A melhor forma de mitigar o risco será fazer com que a complexidade e ponderação do CI acompanhem o aumento da complexidade das operações

- - Qualidade do sistema de controlo – Considera-se também este um importante factor auxiliar na quantificação do risco, pois a qualidade e fiabilidade dos SCI, irá influenciar fortemente todo o funcionamento operacional de uma entidade, logo se poderá inferir que quanto mais fraco for o SCI, maior será a probabilidade de ocorrência de erros fraudes ou omissões, conduzindo assim a empresa a estar exposta a um maior nivel de risco.

- - Dimensão da empresa – A dimensão da empresa é *per se* um elemento que poderá influenciar muito o risco a si associado, pois ao ocorrer um aumento de dimensão da empresa que não seja acompanhado por um aumento da complexidade e extensão dos controlos, faz com que exista, desde logo, um aumento do risco.

- - Liquidez dos activos – Este é um aspecto muito importante para a AI, pois uma empresa ao ter muitos bens materiais, com um elevado grau de liquidez poderá fazer com que ocorram intenções fraudulentas. Desta feita se considera que quanto mais líquidos forem os activos de uma determinada entidade, maior controlo deverá existir sobre estes. Logo maior cuidado e preocupação deverá haver por parte da AI relativamente a estes activos.

- - Operações pouco usuais – uma entidade onde ocorram operações pouco usuais faz com que os recursos humanos, materiais e os controlos não estejam muitas vezes "habituados" a tais situações, o que poderá fazer com que ocorram erros com uma maior facilidade, daí se poder dizer que este é, de facto, um grande factor de risco.

Após esta breve incursão pelos factores de riscos que se podem detectar e ainda incluído na fase de planeamento procede-se ao diagnóstico da área a auditar, aqui é feita a análise de procedimentos e SCI, possibilitando a identificação das fragilidades e/ou procedimentos ineficazes e por isso passíveis de serem eliminados. É de destacar o facto do diagnóstico ou levantamento preliminar a ser feito dever ter em conta a área a auditar, pois os procedimentos não serão os mesmos consoante se tratar da área financeira ou da produção.

Execução do trabalho de campo

A execução do trabalho de campo constitui o *core* de AI dado que é nesta fase que, entre outras acções, se efectuam todos os tipos de teste aos procedimentos de CI, para assim se poderem retirar informações suficientes que permitam retirar elações sobre o funcionamento global do SCI da entidade ou de uma determinada área específica. É também nesta parte que se detectam alguns tipos de risco, ao ser feita a análise dos controlos existentes e de quais as consequências da sua não aplicação ou das falhas do mesmo.

Recomendações

Esta é a parte que precede a execução dos testes anteriormente descritos, pois serão aqui delineadas as possíveis alterações ou correcções a efectuar, resultantes da detecção de situações passíveis de serem melhoradas. Estas recomendações deverão ser veiculadas por intermédio de um relatório, constituindo este o produto final de todo o trabalho de AI. Trata-se de um documento formal onde o Auditor Interno relata o trabalho efectuado, qual a metodologia utilizada na realização dos testes. Neste relatório é também feita referência à análise global da organização. São também relatados os métodos e procedimentos utilizados e ainda qual a apreciação do auditor relativamente ao SCI. Deste documento constam também todas as propostas e recomendações resultantes dos testes e análises efectuadas. Este relatório é fruto do trabalho de toda uma equipa, onde também se inclui o auditado, apesar da responsabilidade recair na sua totalidade sobre o auditor. Todas as recomendações contidas no referido relatório, deverão ser discutidas com os auditados antes da sua aplicação, para assim surgirem oportunidades de melhorar e

envolver os mesmos na busca de soluções para a mitigação dos riscos incorridos, tendo sempre em consideração os objectivos estratégicos da entidade.

Follow-up

Follow-up's, são outro dos aspectos importantes e a ter em conta aquando da execução de um trabalho desta natureza, pois permitem que sejam monitorizadas as acções resultantes das recomendações dadas, trata-se precisamente do acompanhamento. É considerada uma parte fundamental do trabalho de auditoria, pois, se esta não for desenvolvida, as recomendações resultantes do relatório poderão não ser seguidas da forma mais conveniente podendo assim degenerar numa perda do valor que se pretendia obter com o trabalho. Em suma, esta parte do trabalho é de facto a monitorização com o intuito de assegurar que o plano de acções será cumprido de forma a optimizar todo o processo, permitindo assim a verificação efectiva das acções correctivas, resultantes de todo o trabalho que deu origem ao relatório.

Durante esta fase há que ter em conta a importância dos problemas identificados, isto é, qual o seu impacto na empresa. É também de primordial importância fazer uma análise da relação "custo – benefício" no ambito da resulução do problema detectado.Como já foi referido, é também importante, analisar aprofundadamente o risco associado ao facto da implementação de uma recomendação não ser bem sucedida ou não reflectir o efeito pretendido. Muito importante será também o tempo dispendido na aplicação de uma recomendação, pois nos dias que correm, considera-se a tempestividade uma variável que poderá fazer a diferença.

Tudo o que acima foi vertido possibilita que o trabalho de AI efectuado se traduza em melhorias significativas permitindo uma melhor detecção, gestão e mitigação do risco associado a uma empresa e/ou sector de actividade.

O trabalho de auditoria é finalizado quando as recomendações ficam implementadas e após o acompanhamento se constata que estas estão a funcionar e a mostrar-se de facto numa mais-valia para a entidade.

Comprova-se assim a visão proactiva da AI, pois esta não se limita à avaliação, análise e diagnóstico, mas também à implementação de soluções e medidas correctivas certificando-se que a sua aplicação incrementará na entidade um ponto passível de ser considerado valor acrescentado.[PINHEIRO 2005]

III – ESTUDO DE CASO

Apresenta-se seguidamente um estudo de caso que se considerou de todo o interesse para o desiderato do trabalho em apreço, ressalve-se para o facto de se tratar de uma empresa hipotética perante um caso real.

A Mestranda, S.A. dedica-se à montagem e instalação eléctrica em obra. Está a implementar desde 2008 as normas ISO (*International Organization for Standardization*), tendo o seu departamento de qualidade pedido ao DAI auxílio na construção de uma matriz de riscos a que estão expostos os colaboradores da Mestranda S.A. aquando da prestação dos seus serviços em obra.

A empresa dado o seu *core business*, está sujeita a diversos riscos quer sejam danos físicos e pessoais dos seus colaboradores (quedas, electrocuções) como danos materiais por avarias e perdas resultantes de uma má istalação/ manuseamento dos componentes, falhas na execução ou qualquer outro factor decorrente do seu trabalho. Estes riscos deverão ser analisados e tidos em consideração, caso contrário, poderão resultar em avultadas perdas para a empresa, pois quer se esteja a falar em danos materias ou pessoais, para esta, traduzir-se-ão em gastos.

Foi criada uma matriz de risco, que tem em conta as diversas variaveis que poderão influenciar a concretização ou não de um determinado risco.

A partir dessa matriz pretende-se criar procedimentos de resposta aos riscos identificados, tendo para isso em conta o seu impacto e a probabilidade de ocorrencia dos mesmos.

O que se pretende demosntrar neste exemplo prático é todo o processo inerente à construção dessa matriz de risco (contributo do DAI) que levará depois à definição de estratégias a seguir por parte da Administração da Mestranda, S.A.

DESCRIÇÃO DO PROCEDIMENTO

1– Método Simplificado de Avaliação de Riscos

Esta metodologia permite quantificar a magnitude dos riscos existentes e hierarquizar racionalmente a sua prioridade de prevenção.

Para tal, parte-se da detecção das deficiências existentes nos locais de trabalho para se estimar a probabilidade de ocorrencia de um acidente e, tendo em conta a magnitude esperada das consequências, avaliar o risco associado a cada uma das ditas deficiências.

Nesta metodologia considera-se que o nível de probabilidade (NP) é função do nível de deficiência e da frequência ou nível de exposição à mesma.

O nível de risco (NR) será por seu lado função do nível de probabilidade (NP) e do nível de consequências (NC), e pode expressar-se como:

NR = NP x NC

1.1 - Nível de Deficiência

Designa-se nível de deficiência (ND) à magnitude da relação esperada entre o conjunto de factores de risco considerados e a sua relação causal directa com o possível acidente. Os valores numéricos empregues nesta metodologia e o significado dos mesmos indicam-se no seguinte quadro:

Quadro Nº 1 - Nível de Deficiencia

ND - NÍVEL DE DEFICIÊNCIA		
MD - Muito Deficiente	10	Detectaram-se factores de risco significativos que determinam como muito possível a geração de falhas. O conjunto de medidas preventivas existentes em relação ao risco resulta ineficaz
D - Deficiente	6	Detectou-se algum factor de risco significativo que precisa de ser corrigido. A eficácia do conjunto de medidas preventivas existentes vê-se reduzida de forma apreciável
M - Melhorável	2	Detectaram-se factores de risco de menor importância. A eficácia do conjunto de medidas preventivas existentes em relação ao risco não se vê reduzida de forma apreciável
A - Aceitável	0	Não se detectou nenhuma anomalia destacável. O risco está controlado. Não se valoriza.

Fonte: Elaboração Própria

1.2– Nível de Exposição

O nível de exposição (NE) é uma medida da frequência com que se dá a exposição ao risco.

Para um risco concreto, o nível de exposição estima-se em função dos tempos de permanência nas áreas de trabalho, operações com máquinas, etc.

Os valores numéricos do nível de exposição são inferiores aos dos níveis de deficiência, uma vez que, se a situação de risco está controlada, uma exposição alta não deverá ocasionar o mesmo nível de risco que uma deficiência alta com exposição baixa.

Quadro Nº 2 – Nível de Exposição

NE - NÍVEL DE EXPOSIÇÃO		
EC - Continuada	4	Continuamente. Várias vezes durante a jornada laboral com tempo prolongado.
EF - Frequente	3	Várias vezes durante a jornada de trabalho, se bem que com tempos curtos.
EO - Ocasional	2	Alguma vez durante a jornada de trabalho e com um período curto de tempo.
EE - Esporádica	1	Irregularmente.

Fonte: Elaboração Própria

1.3- Nível de Probabilidade (NP)

Em função do nível de deficiência das medidas preventivas e do nível de exposição de risco, determina-se o **nível de probabilidade (NP)**, o qual se pode expressar como o produto de ambos os termos.

NP = ND x NE

Quadro Nº 3- Nível de Probabilidade

Valores de NP		Nível de Exposição (NE)			
		4	3	2	1
Nível de Deficiência (ND)	10	40	30	20	10
	6	24	18	12	6
	2	8	6	4	2
	0	0	0	0	0

Fonte: Elaboração Própria

No próximo quadro reflecte-se o significado dos quatro níveis de probabilidade estabelecidos.

Quadro Nº 4- Significado dos Valores NP

	Valores NP	Significado
Muito alta (MA)	Entre 40 e 24	Situação deficiente com exposição continuada, ou muito deficiente com exposição frequente.
Alta (A)	Entre 20 e 10	Situação deficiente com exposição frequente ou ocasional, ou situação muito deficiente com exposição ocasional ou esporádica.
Média (M)	Entre 8 e 6	Situação deficiente com exposição esporádica ou situação melhorável com exposição continuada ou frequente.
Baixa (B)	Entre 4 e 2	Situação deficiente com exposição ocasional ou esporádica. Não se espera que se materialize o risco ainda que possa ser admissível.

Fonte: Elaboração Própria

1.3– Nível de Consequência

Consideram-se igualmente quatro níveis para a classificação das consequências (NC).

Estabelece-se um duplo significado: por um lado, classificaram-se os danos físicos e por outro os danos materiais. Ambos os significados devem ser considerados independentemente, tendo mais peso os danos às pessoas que os danos materiais. Quando as lesões não são importantes, então a consideração dos danos materiais, estes devem ajudar a estabelecer prioridades com um nível de consequências estabelecido para pessoas.

Os acidentes com baixa consideram-se como consequência grave.

Quadro Nº 5 –Nível de Consequência

(NC) Nível de Consequência		Danos Pessoais	Danos Materiais
M - Morte ou catastrófico	100	1 morto ou mais	Destruição total do sistema (difícil renová-lo)
MG - Muito Grave	60	Lesões graves que podem ser irreparáveis	Destruição parcial do sistema (completa e custosa reparação)
G - Grave	25	Lesões com incapacidade laboral temporária	Requer-se paragem do processo para efectuar a reparação
L - Leve	10	Pequenas lesões que não requerem hospitalização	Reparação sem necessidade de paragem do processo

Fonte: Elaboração Própria

1.2 - Nível de Risco e Nível de Intervenção

O próximo quadro permite determinar o nível de risco e estabelecer prioridades das intervenções, através do estabelecimento também de quatro níveis (indicados no quadro com algarismos romanos).

Para priorizar um programa de investimentos e melhorias, é imprescindível introduzir a componente económica e o âmbito de influência da intervenção. Assim, perante resultados similares, estará mais justificada uma intervenção prioritária quando o custo for menor e a solução afecte um colectivo de trabalhadores maior.

NR = NP x NC

Quadro Nº 6 Nivel de Risco / Matriz de Risco

NIVEL DE CONSEQUENCIA (NC)	NIVEL DE PROBABILIDADE (NP)			
	40 - 24	20 - 10	8 - 6	4 - 2
100	I 4000-2400	I 2000-1200	I 800-600	II 400-200
60	I 2400-1440	I 1200-600	II 480-360	II 240
25	I 1000-600	II 500-250	II 200-150	III 100-50
10	II 400-240	II 200	III 80-60	III 40

Fonte: Elaboração Própria

O nível de risco, como se mostra no ponto 1.4, vem determinado pelo produto do nível de probabilidade pelo nível de consequências.

O quadro seguinte estabelece o agrupamento dos níveis de risco que originam os níveis de intervenção e qual o seu significado.

Quadro Nº 7 – Agrupamento de Níveis de Risco por Níveis de Intervenção

NÍVEL DE INTERVENÇÃO	NR	SIGNIFICADO
I	4000-600	Situação critica. Correcção urgente
II	500-150	Corrigir e adoptar medidas de controlo
III	120-40	Melhorar se for possível. Seria conveniente justificar a intervenção e rentabilidade
IV	20	Não intervir, salvo se justifique por uma análise mais precisa

Fonte: Elaboração Própria

IV – CONCLUSÃO

Ao chegar ao final deste estudo resta fazer uma breve retrospectiva do que aqui foi abordado, enunciar as conclusões a que se chegou e arrolar algumas questões que foram surgindo ao aprofundar o tema e que se julga serem pertinentes possibilidades para uma futura investigação.

Tal como referido ficou no capítulo da introdução as diversas falências a que se assistiu nos últimos anos, motivaram uma "chamada de atenção" para a questão dos riscos empresariais e, mais importante ainda, para a problemática da sua gestão.

Começaram então a surgir questões preocupantes, que cada vez mais inquietavam os gestores e que urgiam em ser resolvidas,tais como:

Quais os riscos a que as empresas estão expostas?

Como podem esses riscos ser tratados de forma a serem mitigados?

Qual o papel da AI no processo de gestão de riscos?

A resposta a estas questões poderia fazer a diferença entre manter-se e prosperar no mercado competitivo e global dos dias de hoje, ou deixar de fazer parte dele. Desta feita no ambito da gestão de riscos,tornava-se imperioso encontrar uma parceria que auxiliasse a solucionar estas questões da forma mais eficiente possível.

Considera-se que o estudo vertido nestas páginas dará o seu contributo na descoberta de algumas respostas a estas e outras questões.

No Capítulo I – Riscos empresariais, insidiu-se sobre a primeira questão e foram apresentadas diferentes definições de riscos empresariais e possíveis classificações dos mesmos, dadas por diversos autores.

Aqui se concluiu que embora diferentes, as definições apresentadas traduzem a mesma ideia de fundo e que correr riscos é um facto intrínseco à própria existência da empresa, sendo esta a visão de CRUZ (2005), ao referir que "toda a actividade empresarial consubstancia a assunção de riscos, de incerteza da ocorrência de perdas económicas" concepção esta que acolhe integral concordancia.

É certa a existência de riscos empresariais e do que estes representam no desenvolvimento da actividade normal de uma empresa, importa então classificá-los de forma a , responder cabalmente à primeira questão.

Partindo das diferentes classificações apresentadas propôs-se uma que divide os riscos a que uma empresa está exposta em três tipos, de acordo com as questões com as quais estão relacionados:

- Riscos relacionados com o Mercado, a envolvente da empresa – Como já foi oportunamente refedido, estes estão associados a questões legais, políticas, sociais, económicas, ambientais entre outras;

- Riscos relacionados com a própria organização – São os riscos que envolvem questões sob a alçada da estrutura organizacional da empresa, como esta lida com os funcionários, clientes e fornecedores, como conduz a sua estratégia de actuação nas diferentes àreas;

- Riscos relacionados com o negócio da empresa – Independentemente do mercado em que opere e da forma como a empresa conduza as suas

operações, o negócio tem implícitos certos tipos de riscos. Pode envolver questões ambientais, de segurança, de obsolescência de itens (em negócios que envolvam alta tecnologia, por exemplo).

Com a elaboração do estudo, houve oportunidade de constatar que dos inúmeros riscos associados à actividade empresarial alguns são controláveis pela empresa enquanto que sobre outros esta não tem qualquer controlo. CRUZ *(*2008)

Tendo isto em consideração será importante focar a forma como a empresa pode mitigar estes riscos, já que os outros são de controlo muito mais difícil se não mesmo impossível. Desta feita, há a possibilidade de ser dada uma resposta à segunda questão anteriormente colocada: como podem estes riscos ser eliminados?

O Capítulo II – Gestão de risco empresarial, foi dedicado a essa questão. Aqui se dissecou o processo de análise dos riscos, tendo-se verificado que é fundamental um bom conhecimento do sector de actividade em que a empresa opera, para assim ter acesso ao conhecimento de quais os riscos mais comuns e posteriormente verificar quais são os que a afectam de facto. Da análise feita a esta questão concluiu-se que um instrumento fundamental no processo de gestão de risco empresarial é a matriz de riscos, sendo fundamental na construção desta a classificação de riscos por classes/consequências proposta por CRUZ (2008). Também fundamental aqui, tal como sugerido por BRASILIANO (2003), é a realização de entrevistas com os responsáveis operacionais de cada departamento, com a finalidade de fazer um levantamento dos factores que podem afectar negativamente esse mesmo departamento, além de se efectuarem outras investigações como por exemplo analisar as práticas de mercado, a par do que é executado através das técnicas de *Benchmark*.

Como se pode verificar foi precisamente aqui, na elaboração da matriz de riscos, que se concluiu que a AI poderia dar um valioso contributo para a detecção e mitigação dos riscos, pois esta ferramenta possibilita que cada risco seja analisado separadamente verificando-se de que forma este afecta a empresa e o seu funcionamento, para assim poderem ser projectadas as correspondentes medidas correctidas mais acertadas.

Contudo a contrução desta matriz terá sempre que ter em conta o *risk apetitte* assumido pela organização, pois mediante este ser alto ou baixo deverão ser diferentes as medidas a tomar no que à mitigação e controlo de risco diz respeito.

Não deve contudo ser esquecido que o contributo que se poderá esperar desta função, prende-se com a divulgação de importantes informações sobre o SCI que auxiliarão no seu ajustamento, manutenção, avaliação e monitorizaçao, nomeadamente num contexto COSO-ERM, abordado no Capítulo III – Controlo Interno, contributo esse que cada vez mais é considerado de extrema importância.

A análise apresentada focou-se na colaboração prestada pelo DAI à gestão no âmbito da construção da matriz de riscos, para isso analisou-se detalhadamente o funcionamento do mesmo e das suas fases de trabalho.

O capítulo IV deste trabalho foi dedicado à AI propriamente dita, fazendo-se uma análise histórica da sua evolução. A importância que passou a ser atribuída à gestão de risco na sequência das falências anunciadas exaltou a pertinência da função de AI e colocou-se a questão de “como pode o auditor interno contribuir no processo de gestão de risco empresarial?”.

Verificou-se uma alteração de mentalidades - mudança de paradigma – esta permitiu que ocorressem trocas de experiências e desenvolvimento da profissão [PINHEIRO 2005]. Passou a existir uma maior estruturação da função, o que de seguida se estudou foram as característica de um DAI e as respectivas fases do seu trabalho.

A decomposição das fases do trabalho de AI, em ligação com o anteriormente estudado acerca do processo de gestão de risco empresarial permitiu tirar as seguintes conclusões:

- O instrumento por excelência no processo de gestão de risco empresarial é a matriz de risco, pois esta confere uma percepção imediata de quais os tipos de risco associados a uma entidade, e qual o seu impacto na estrutura organizacional. Isto possibilita delinear cuidadosamente quais as medidas acertivas para combater e mitigar cada um deles.
- A manutenção de um adequado SCI é indispensável para uma eficaz e eficiente gestão do risco; pois este será ajustado mediante a avaliação da sua performance na mitigação de situações de risco, para assim desempenhar de forma eficiente a função a que se destina.
- É na monitorização e validação do SCI, bem como na identificação, quantificação e relato de factores relevantes para a construção da matriz de riscos que a AI poderá dar o seu mais valioso contributo para a gestão de riscos.

Com a elaboração deste estudo conseguiu-se averiguar que é nos diferentes momentos ou fases do trabalho de AI, que serão detectados, identificados e

analisados e posteriormente relatados alguns dos factores acima referidos, nomeadamente os riscos com os quais as empresas se deparam diariamente, a saber:

- Planeamento – Nesta fase o auditor interno tem que delinear o trabalho que vai desenvolver, tendo em conta os riscos a que a empresa está sujeita e fazer a partir daí uma análise de modo a adaptar o trabalho em função dos mesmos. Nesta fase o contributo é pouco visível, mas existe, pois ao ter em conta esses riscos o trabalho deverá focar-se no teste das áreas mais susceptíveis. Ao planear testes em áreas consideradas críticas contribuirá para verificar se os controlos existem e se estão ou não a funcionar como deveriam.

O contributo nesta fase é dado de forma discreta, isto é, direccionam-se para os risco já identificados – ou para áreas mais críticas onde seja necessáriso mais monitorização de risco – vendas e cobranças – área em que podem não estar ainda identificados todos os riscos susceptíveis de ocorrer, tendo em conta o sector de actividade onde a empresa se insere assim como que tipo de controlos que esta tem implementado:

- Execução do trabalho de campo – Esta fase constitui o *core* do trabalho de AI. Aqui se concluiu que o auditor interno contribui de duas formas. Por um lado, ao efectuar testes aos controlos, verifica se os mesmos estão a funcionar convenientemente. Por outro lado, ao longo do trabalho de campo o auditor identifica riscos que poderão ainda não ter sido reconhecidos, pois uma das características deste profissional é estar sempre alerta para tudo o que o rodeia e respeite à actividade da empresa, possibilitando que sejam feitos ajustamentos aos controlos, tornando-os assim mais eficientes;

- Recomendações – Aqui o contributo manifesta-se sob a forma das considerações que o auditor deverá emitir sobre inconformidades nos controlos ou potenciais riscos, assim como todas as recomendações fruto dos testes feitos, com o intuito de melhorar a performance dos controlos;
- *Follow-up* – Considerada a fase de monitorização do processo, o contributo do auditor interno consiste em verificar que as recomendações dadas por si estão, de facto, a ser implementsdas e postas em prática. Destaque-se o facto do *follow-up* ser um processo de análise, identificação e melhoramento contínuo em que se vão identificando paulatinamente novas situações.

Alerte-se para o facto de todas estas fases serem sempre reportadas e acompanhadas pelo auditado, de forma a que em conjunto se constituam sinergias no sentido de melhorar substanciamlente o trabalho realizado, permitindo neste caso concreto uma mais eficiente mitigação dos riscos.

É com base no contributo acima evidenciado que deverá ser construida a matriz de riscos, nomeadamente porque no realizar do seu trabalho de campo o auditor quantifica a probabilidade de ocorrência dos riscos identificados, possibilitando depois a escolha de uma das estratégias de resposta ao risco: mitigação, aceitação, transferência ou contenção de riscos [KRUTZ 2003].

O estudo de caso feito, consistiu na análise do processo de construção da matriz de riscos para posterior criação de respostas a estes, no caso de riscos de trabalhadores em obra numa empresa de instalação eléctrica. É aqui comprovado precisamente tudo o que acima se concluiu, nomeadamente foi a função de auditoria interna que

ao longo das várias fases do seu trabalho recolheu os dados necessários à construção da referida matriz.

Ao alcançar este ponto resta referir algumas questões surgidas ao longo deste estudo, consideradas passiveis de serem alvo de uma investigação futura.

Como encaram os gestorese administradores das empresas a colaboração dada pela AI no processo de gestão de risco? E os auditores internos, qual a visão que têm do contributo do seu próprio trabalho neste processo?

Estas duas questões são bastante pertinentes no sentido de se analisar se existe algum “expectation gap” entre o que os gestores esperam que seja o papel da AI no processo de gestão de risco e aquilo que os auditores internos consideram ser realmente a utilidade da sua função. Ao avaliar esta questão será possível desenvolver novas formas de contribuição e assim acrescentar valor à profissão de auditor interno.

V - BIBLIOGRAFIA

Livros

- ✓ ARENS, A.; Elder, R.; Beasley, M. - *Auditing and assurance services: An integrated approach*. 11nd ed.: Prentice Hall, 2006. ISBN 0-13-186712-1.
- ✓ BARALDI, P.- *Gerenciamento de Riscos Empresariais*. - Rio de Janeiro: Campus, 2005.
- ✓ BEJA, Rui. - *Risk Management; Gestão, Relato e Auditoria dos Riscos do Negócio*, Áreas editora, 2004. ISBN 972-8472-69-2.
- ✓ BOYNTON,W. C.; Johnson, R. N. – *Modern Auditing: assurance services and the integrity of financial reporting*. 8th ed.: John Wiley & Sons, 2006. ISBN 978-0-471-23011-3
- ✓ CAIADO, Anibal Campos e Caiado, Jorge - *Gestão de Instituições Financeiras*. 1ª ed.Lisboa : Sílabo, 2006. ISBN 972-618-400-2.
- ✓ COSO – Enterprise risk management: integrated framework. New Jersey: COSO, 2004. 2 Vols.
- ✓ COSTA, Carlos B. – *Auditoria Financeira: Teoria e Prática*. 8ª ed.: Rei dos Livros, 2007. ISBN 978-972-51-1127-7
- ✓ CRUZ, Manuel Mendes – *Gestão do Risco Empresarial*, 2008: ISCAL,. SEBENTA DE APONTAMENTOS.
- ✓ FERNANDES, António J. – *Métodos e regras para a elaboração de trabalhos académicos e científicos*. 2ª ed.: Porto editor, 1995. ISBN 972-0-34204-8

- JORION, P. - *Value at Risk-The New Benchmark for Managing Financial Risk*. 3rd ed. New York: MacGraw-Hill, 2007. ISBN 978-007-126047-3
- MARQUES, Madeira - *Auditoria e Gestão*. Lisboa: Presença, 1997.ISBN 972-23-2151-X.
- MAUTZ, R.F. - *Princípios de Auditoria.* 3ª ed. São Paulo: Atlas, 1980. ISBN 0-86539-002-9
- MENEZES H. Caldeira - *Pincípios de Gestão Financeira.* 11ªed.: Editorial Presença, 2008. ISBN: 978-972-23-1403-9
- MORAIS, Georgina e Martins, Isabel - *Auditoria Interna - Função e Processo.* 2a ed.,actualiz: Área editora, 2003.ISBN 972-8472-544-4
- MORAIS, Maria G. – *Auditoria Interna e a importância do controlo interno preventivo***.** Lisboa Instituto Superior das Ciências do Trabalho e da Empresa, 2000. Dissertação de Mestrado
- MOTA, António Gomes; Nunes, João Pedro e Ferreira, Miguel Almeida. *Finanças Empresariais – Teoria e Prática*. Publisher Team. 2004. ISBN 989-601-002-1
- PINHEIRO, J. Leite - *Auditoria Interna; Manual Prático para Auditores Internos.*Lisboa editora Rei dos Livros 2008. ISBN 978-972-51-1137-6
- SILVA, A., Vitorino, A., Alves, C., Cunha, J. A. e Monteiro, M. A. - *Livro Branco sobre Corporate Governance em Portugal*. Lisboa: Instituto Português de Corporate Governance. 2006. ISBN 972-99974-0-3

Recursos Electrónicos (web-sites relevantes para o tema):

www.corpgov.net – *Corporate Governance*

www.audit-commission.gov.uk – *Audit Commission*

www.cmvm.pt – *Comissão do Mercado de Valores Mobiliários*

www.ecgi.org – *European Corporate Governance Institute*

www.ipai.pt – Instituto Português de Auditoria Interna

www.theiia.org – The Institute of Internal Auditors

www.coso.org - Committee of Sponsoring Organizations of the Treadway Commission

www.ecgi.org – Instituto Português de Corporate Governance

http://www.ferma.eu – Federation of European Risk Management Associations

Artigos

- ✓ ALMEIDA, Domingos M. S.- *Gestão de Risco e Governo das Sociedades* - Revista de Auditoria Interna Lisboa Nº 22 (Out. /Dez.2005), p.9-14
- ✓ BEZERRA, Juliana – *A importância de gerenciamento de riscos em projectos* – [Consult. 20 Nov. 2009]. Disponível em http://www.tenstep.com.br/br/Newsletter/AImportanciadoGerenciamentodeRisco.htm
- ✓ BRASILIANO, *Antonio Celso Ribeiro – Entendendo Riscos Corporativ*os – [Consult. 12 Out. 2009]. Disponível em http://www.brasiliano.com.br/blog/?p=274

- CASTANHEIRA, Nuno - *Gestão de risco operacional na actividade bancária: o papel da Auditoria Interna* – Revista Revisores & Empresas Lisboa. ISSN 0870 – 3566. Nº 30 (Jul./Set. 2005), p.8-10.

- COLBERT, J. L. and BOWEN, P. L., - A Comparison of Internal Controls: COBIT; SAC, COSO and SAS 55/78 - Information Systems Audit and Control Association Eds 2002.

- CRUZ, Manuel da – G*estão do Risco Empresarial e dos Negócios* – XII congresso de contabilidade respondendo a mudança. [Consult. 17 Ago.. 2009]. Disponível em http://www.brasiliano.com.br/blog/?p=1296

- CRUZ, Manuel da – *Perspectivas da Gestão do Risco Empresarial* - Gestão Contemporânea, Porto Alegre, Ano 2, Nº1 (Jan/Dez 2005),p.66-72

- JUNIOR, Sebastião Bergamini – *Controles Internos como um Instrumento de Governança Corporativa* – Revista do BNDES, Rio de Janeiro. V12 N. 24. (Dez 2005), p.149-188.

- KRUTZ, George - Medindo os Riscos para Analisar a Vulnerabilidade. [Consult. 9 Set. 2009] em http://www.mcafee.com/br/enterprise/security_insights/measuring_risk_gauge_vulnerability.html

- LEITE, Roberto Cintra - *Por que Adotar um Sistema de Governança Corporativa* - [Consult. 6 Jul. 2009]. Disponível em http://www.empresario.com.br/artigos/artigos_html/artigo_a_270406.html

- LINSMEIER, T. J., PEARSON, N.D. – Risk measuring: an introduction to value-at-risk. (1996). (Office for futures and Options Research Working Paper 4 p.44

- MARTINS, Nuno – *Auditoria Interna Baseada no Risco* – Metodologia ERM (Seminário, IPAI, Lisboa, 2007)

- NAKASHIMA, D. T. V., CARVALHO M. M. - Identificação de riscos em projetos de TI: XXIV Encontro Nac. de Eng. de Produção: Florianópolis, SC, Brasil, 03 a 05 de Nov de 2004 [Consult. 16 Mai. 2009]. Disponível em: http://www.abepro.org.br/biblioteca/ENEGEP2004_Enegep0802_1822.pdf

- MCNAMEE, David – Para uma teoria geral de Auditoria Interna – Cadernos de Auditoria Interna. – Lisboa : Banco de Portugal, 1998 – ano 1, N. 1 (Jan. 1998), p.11-31

- OECD - *Os Princípios da OCDE sobre o Governo das Sociedades* - [Consult. 2 Jun. 2009]. Disponível em http://www.oecd.org/dataoecd/1/42/33931148.pdf

- PEREIRA, Eduardo. - COSO – The Commitee of Sponsiring Organizations of the Treadway Commission – 2004.

- PINHEIRO, J. Leite - Auditoria Interna – criar sucesso - Revista de Auditoria Interna, Lisboa. Nº 22, (Out. /Dez.2005), p.4-6

- SANTOS, Carlos; VASCONCELOS, André; TRIBOLET, José. Da Framework CEO à auditoria de Sistemas de Informação. [Consult. 7 Jun. 2009]. Disponível em http://www.inesc-id.pt/pt/indicadores/Ficheiros/2114.pdf