



**LISBOA
SCHOOL OF
ECONOMICS &
MANAGEMENT**

**MESTRADO
GESTÃO E ESTRATÉGIA INDUSTRIAL**

**TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO**

**GESTÃO DE RISCOS ESTRATÉGICOS –
ACTION RESEARCH NUMA EMPRESA DE
TECNOLOGIAS DE INFORMAÇÃO**

LUÍS FERNANDO FONSECA DE OLIVEIRA

SETEMBRO - 2013

**MESTRADO EM
GESTÃO E ESTRATÉGIA INDUSTRIAL**

**TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO**

**GESTÃO DE RISCOS ESTRATÉGICOS –
ACTION RESEARCH NUMA EMPRESA DE
TECNOLOGIAS DE INFORMAÇÃO**

LUÍS FERNANDO FONSECA DE OLIVEIRA

ORIENTAÇÃO:

PROF.^a DOUTORA CLÁUDIA SARRICO

SETEMBRO - 2013

Resumo

Objetivo da investigação

Este estudo pretende determinar de que forma a gestão dos riscos estratégicos e o planeamento estratégico e controlo de gestão podem ser integrados, de forma a contribuir para a sustentabilidade e criação de valor nas organizações.

Metodologia

A investigação baseou-se na realização de *action research* numa empresa de média dimensão que atua na área das TIC. Os resultados foram obtidos através de um processo iterativo, baseado na análise da teoria disponível sobre gestão estratégica e gestão de risco, realização de experiências e reflexão sobre os resultados obtidos.

Resultados

Os riscos estratégicos foram definidos como os riscos internos ou externos, que podem ocorrer tanto na definição como na implementação da estratégia e com potencial para alterar significativamente a posição competitiva da organização. Do estudo resultou um modelo conceptual de integração dos processos de gestão dos riscos estratégicos e de planeamento estratégico e controlo de gestão. O modelo sugere que a incorporação de sistemas de controlo especialmente dedicados à gestão da incerteza promove a antecipação estratégica, a aprendizagem e o aparecimento de estratégias emergentes.

Implicações teóricas

Os resultados obtidos são de natureza qualitativa e baseados numa investigação conduzida numa organização singular. A generalidade do modelo proposto pode ser testada com a realização de estudos de caso de aplicação noutras organizações.

Originalidade

O estudo explicita uma forma clara de integrar a gestão estratégica com a gestão dos riscos estratégicos, consubstanciada num modelo conceptual.

Palavras-chave: Gestão de risco empresarial, risco estratégico, gestão estratégica, sistemas de controlo de gestão, alavancas de controlo.

Abstract

Purpose

The aim of this study is to ascertain how strategic planning and management control can be integrated with the management of strategic risks in order to contribute to value creation and the sustainability of organizations.

Methodology

The research was conducted by doing action research in a medium-sized ICT company. The results were achieved through an iterative process of studying the available theory on strategic management and risk management, conducting experiments and reflecting on the results.

Results

Strategic risks are defined as internal or external risks that can occur both in strategy formulation and strategy implementation and which have the potential to significantly alter the competitive position of the organization. A conceptual model for integrating the management of strategic risks with strategic planning and management control is suggested. We find that the incorporation of control systems designed to specifically manage uncertainty promotes strategic anticipation, learning and the emergence of new strategies.

Theoretical implications

The results are based on research conducted in a single organization and are qualitative in nature. Case studies can be conducted in other organizations to test the generality of the results.

Originality

The new conceptual model offers a clear way to integrate strategic planning and control with the management of strategic risks.

Keywords: Enterprise risk management, strategic risk, strategic management, management control systems, levers of control.

For gods perceive things in the future, ordinary people things in the present, but the wise perceive things about to happen.

Philostratus

Agradecimentos

Ao José Luís Pereira e ao Carlos Silva, por me terem acolhido na família SINFIC;

aos colegas da área financeira e de risco da SINFIC que contribuíram diretamente para a investigação realizada neste trabalho, João Nuno Martins e (o outro) Luís Oliveira;

aos restantes colaboradores da SINFIC, em Portugal e pelo Mundo;

aos meus colegas da Novageo, especialmente o Rui Andrade;

à minha orientadora, Professora Cláudia Sarrico, pelo apoio prestado durante a elaboração da tese;

aos meus amigos;

à Sofia, agora foi a tua vez de esperar, e à sua família;

à minha família, principalmente a minha mãe, a quem dedico esta tese, não só pelo apoio incondicional ao longo da realização deste trabalho final de mestrado, mas também de todo o meu percurso.

Índice geral

Resumo.....	ii
Abstract	iv
Agradecimentos.....	vii
Índice geral	viii
Índice de figuras.....	xi
Lista de abreviaturas	xii
1. Introdução	1
2. Revisão da literatura	2
2.1. Gestão de Risco Empresarial e gestão de riscos estratégicos	2
2.1.1. Risco	2
2.1.2. Gestão de risco	2
2.1.3. Gestão de Risco Empresarial.....	3
2.1.4. Modelos de Gestão de Risco Empresarial	6
2.1.5. Classificação dos riscos	10
2.1.6. Limitações dos modelos de Gestão de Risco Empresarial.....	14
2.2. Planeamento estratégico e controlo de gestão.....	16
2.2.1. Planeamento estratégico.....	16
2.2.2. Controlo de gestão	17

3. Gestão de risco na SINFIC, SA	22
3.1. Enquadramento da SINFIC, SA	22
3.2. Práticas de gestão de risco na SINFIC, SA	23
4. Síntese e questão de investigação	24
5. Metodologia.....	26
6. Relevância teórica e empírica do estudo	27
7. Integração do planeamento estratégico e controlo de gestão com a gestão de risco	28
7.1. Integração dos processos de Gestão de Risco Empresarial e planeamento estratégico e controlo de gestão	29
7.2. Registo de riscos e mapa de riscos.....	30
7.3. O CIMA <i>Strategic Scorecard</i>	31
8. Resultados da investigação	33
8.1. Definição de riscos estratégicos.....	34
8.2. Modelo conceptual de integração da gestão dos riscos estratégicos com o planeamento estratégico e controlo de gestão	34
9. Conclusão.....	40
9.1. Principais conclusões.....	40
9.2. Limitações e sugestões para investigação futura	41
Referências bibliográficas	42
Anexos.....	53

Anexo I – ISO 31000:2009 – Princípios, estrutura e processo.....	53
Anexo II – Business Risk Model™	56
Anexo III – Definições de risco estratégico.....	57

Índice de figuras

Figura 1: Gestão de Risco Empresarial: uma nova perspectiva (DeLoach, 2000)	5
Figura 2: Cubo COSO ERM (COSO, 2004)	9
Figura 3: Modelo genérico de Gestão de Risco Empresarial (Henriksen & Uhlenfeldt, 2006)	10
Figura 4: Modelo das Alavancas de Controlo (Simons, 1995)	19
Figura 5: CIMA <i>Strategic Scorecard</i> (IFAC, 2004)	32
Figura 6: Modelo conceptual de integração dos processos de gestão dos riscos estratégicos e de planeamento estratégico e controlo de gestão (Elaboração própria)	35
Figura 7: ISO 31000:2009 - Estrutura da gestão de risco (ISO, 2009)	54
Figura 8: ISO 31000:2009 - Processo de gestão de risco (ISO, 2009)	55
Figura 9: Taxonomia de riscos do Business Risk Model™ (DeLoach, 2000)	56

Lista de abreviaturas

AIRMIC – Association of Insurance and Risk Managers in Industry and Commerce

BIS – Bank for International Settlements

BSC – Balanced Scorecard

CAS – Casualty Actuarial Society

CEB – Corporate Executive Board

CIMA – Chartered Institute of Management Accountants

COSO – Committee of Sponsoring Organizations of the Treadway Commission

EIU – Economist Intelligence Unit

ERM – Enterprise Risk Management

ERP – Enterprise Resource Planning

FERMA – Federation of European Risk Management Associations

GR – gestão de risco

GREmp – Gestão de Risco Empresarial

I&D – investigação e desenvolvimento

ICAEW – Institute of Chartered Accountants in England and Wales

IFAC – International Federation of Accountants

IMA – Institute of Management Accountants

IRM – Institute of Risk Management

ISO – International Standards Organization

S&P – Standard & Poor's

SGQ – sistema de gestão da qualidade

SOA – Society of Actuaries

SWOT – strengths, weaknesses, opportunities and threats

TIC – tecnologias de informação e comunicação

1. Introdução

A Gestão de Risco Empresarial (GREmp) representa uma mudança de paradigma na gestão de risco (GR) (DeLoach, 2000). Enquanto a GR tradicional se preocupa com os prejuízos que podem decorrer dos riscos puros, financeiros e operacionais, a GREmp pretende, para além disso, identificar e gerir os riscos estratégicos da organização e contribuir para a sua sustentabilidade e criação de valor (Nocco & Stulz, 2006). A gestão dos riscos estratégicos só é possível no contexto da formulação, implementação e controlo da estratégia (COSO, 2004), pelo que se torna necessário interligar os processos de GREmp e de planeamento estratégico e controlo de gestão para geri-los eficazmente (Arena *et al.*, 2010). No entanto, as organizações têm encontrado vários obstáculos para materializar essa integração, entre os quais a dificuldade de definir e quantificar os riscos estratégicos (Gates, 2006). Este estudo pretende contribuir para o debate sobre a GREmp e a gestão dos riscos estratégicos de duas formas: (a) apresentando uma definição de risco estratégico que incorpora as características essenciais deste tipo de risco; e (b) apresentando um novo modelo conceptual de integração dos processos de GREmp e de planeamento estratégico e controlo de gestão. A investigação desenvolvida teve por base a realização de *action research* numa empresa de média dimensão a atuar na área das tecnologias de informação e comunicação.

A revisão da literatura aborda o tópico da GREmp na secção 2.1 e o planeamento estratégico e o controlo de gestão na secção 2.2. A secção 3 fornece informação sobre a empresa onde se realizou a investigação e as práticas de GR aí existentes no início do estudo. A secção 4 explicita a questão de investigação e a secção 5 explana a metodologia de investigação utilizada. A secção 6 discute a relevância teórica e empírica do estudo. A secção 7 descreve a

investigação realizada, que se baseou no processo iterativo preconizado pela *action research*, alternando a pesquisa teórica com experiências no domínio da integração da gestão de risco e gestão estratégica. A secção 8 apresenta os resultados da investigação: uma definição de risco estratégico e um modelo integrado de planeamento estratégico e controlo de gestão com a gestão dos riscos estratégicos. Na secção 9 são apresentadas as conclusões, limitações e sugestões para investigação futura que resultaram da investigação.

2. Revisão da literatura

2.1. Gestão de Risco Empresarial e gestão de riscos estratégicos

2.1.1. Risco

Hopkin (2012) define risco como “a combinação da probabilidade de um evento e da sua consequência. As consequências podem ser positivas ou negativas”. A norma ISO 31000:2009 (ISO, 2009) define risco como o “efeito da incerteza na consecução dos objetivos”, referindo também que “um efeito é um desvio, positivo ou negativo, relativamente ao esperado”, que o risco é “caracterizado pela referência aos **eventos** potenciais e **consequências**” e que pode ser “expresso como a combinação das consequências de um dado evento [...] e a respetiva **probabilidade**¹”.

2.1.2. Gestão de risco

Para assegurar a concretização dos objetivos e a continuidade das operações, as organizações necessitam de controlar os efeitos da incerteza. Segundo Collier (2009), a GR é o “processo de compreender e gerir os riscos que a organização enfrenta quando procura

¹ Ênfase no original.

atingir os seus objetivos“. A GR pode também ser definida como as “atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco” (ISO, 2009).

A GR nas organizações teve a sua origem na indústria seguradora, nas décadas de 1940 e 1950. Nos primórdios da atividade, a sua função principal era proteger os ativos da organização contra os riscos puros, tais como o risco de incêndio, através da realização de seguros, de forma a minimizar eventuais prejuízos (Dickinson, 2001). Nas décadas de 1970 e 1980 a GR desenvolveu uma perspetiva financeira, adicionando o objetivo de gerir a volatilidade da atividade económica e dos resultados financeiros, por forma a otimizar o desempenho da organização (Dickinson, 2001). A GR tradicional, tal como é ainda praticada na maioria das empresas, acrescenta às duas perspetivas anteriores a gestão dos riscos decorrentes da atividade operacional da organização (CAS, 2003). A GR tradicional é motivada pela conformidade com os regulamentos e leis vigentes, sendo realizada de forma independente por vários intervenientes, que não partilham, nem entre si nem com a organização, informação sobre os riscos que gerem e as suas consequências potenciais (Mikes, 2009). Esta configuração não permite a construção de um *portfolio* agregado de riscos e o desenvolvimento de uma estratégia de gestão integrada dos riscos (Arena *et al.*, 2011).

2.1.3. Gestão de Risco Empresarial

A GREmp surgiu no fim da década de 1990 como uma abordagem unificadora e transversal, que considera todos os processos da organização de forma integrada e tem como foco a criação de valor (Deloach, 2000; Lam, 2003). Através de uma metodologia estruturada e disciplinada, identifica e avalia todos os riscos que afetam a organização, gerindo-os de forma holística e coordenada (COSO, 2004; SOA, 2006). Hopkin (2012) define a GREmp como

sendo o “conjunto de atividades que uma organização desenvolve para atingir os resultados mais favoráveis e reduzir a volatilidade e variabilidade desses resultados”. A definição de GREmp citada mais frequentemente é a da COSO (2004):

“A Gestão de Risco Empresarial é um processo, desenvolvido pela gestão de topo, órgãos de gestão e demais colaboradores, aplicado na definição da estratégia e abrangendo toda a organização, que tem como objetivo a identificação dos eventos potenciais que podem afetar a organização e gerir os riscos de forma alinhada com o apetite pelo risco pretendido, com vista a fornecer uma segurança aceitável relativamente ao cumprimento dos objetivos definidos pela organização.”

O conceito de apetite pelo risco referido na definição da COSO consiste no entendimento que a organização deve possuir sobre a exposição ao risco que está disposta a aceitar no desenvolvimento da sua atividade, podendo ser definido em termos quantitativos ou qualitativos (Rittenberg & Martens, 2012). Na perspetiva da GREmp, a propensão para assumir riscos de forma responsável, prevenindo ameaças e explorando oportunidades, é uma fonte de vantagem competitiva (Collier, 2009; Lam, 2003) e contribui positivamente para o desempenho sustentável e a criação de valor (Chapman, 2006; Miccolis *et al.*, 2001). A Figura 1 (DeLoach, 2000) contrasta a visão tradicional da GR com a visão moderna da GREmp.

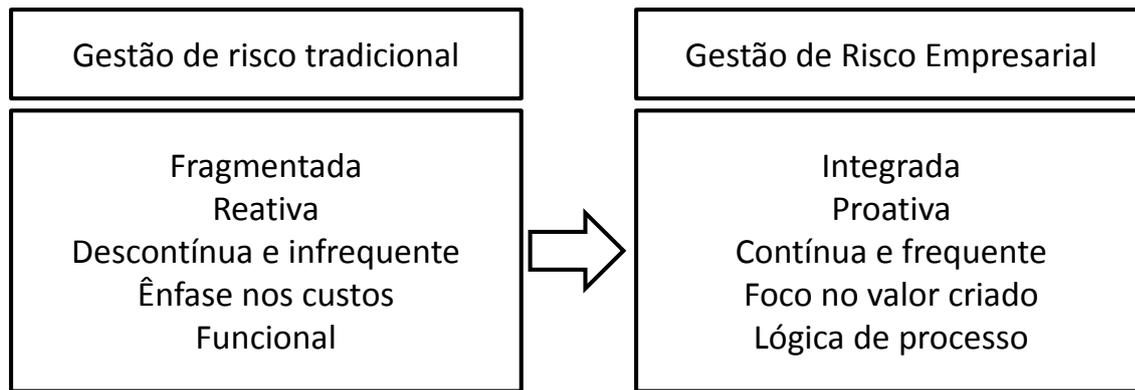


Figura 1: Gestão de Risco Empresarial: uma nova perspectiva (DeLoach, 2000)

A evolução no sentido de abordagens à GR cada vez mais completas e integradas está relacionada em larga medida com as vagas de escândalos financeiros e empresariais que têm assolado as economias avançadas desde os anos 1980, onde se incluem, como exemplos mais recentes, o colapso da Enron em 2001 e a crise financeira de 2008 (Andersen & Schrøder, 2010). Estes acontecimentos conduziram a: (a) elevação da GR ao estatuto de requisito fundamental das boas práticas de governo societário (Spira & Page, 2003); (b) várias reformas legislativas que tornam obrigatória a GR nas organizações, de que o exemplo mais conhecido é a lei Sarbanes-Oxley Act, introduzida nos EUA em 2002 com o objetivo de impedir a fraude no relato financeiro (Power, 2007); (c) surgimento de acordos de regulação em sectores específicos, como os acordos de Basileia II (BIS, 2004), que incluem recomendações para a indústria financeira sobre as melhores práticas a adotar na gestão dos riscos financeiros e operacionais.

O surgimento da GREmp foi também impulsionado pela explosão do número de riscos que afetam as organizações (Arena *et al.*, 2010) e pela perceção de que os riscos de cariz estratégico não são abordados de forma sistemática (Slywotzky & Drzik, 2005). Estes riscos,

decorrentes da globalização das cadeias de valor e dos mercados de capitais, das tecnologias em mutação constante e dos ciclos de vida dos produtos cada vez mais curtos, podem danificar gravemente a posição estratégica e financeira das organizações (Andersen & Schrøder, 2010). Mas enquanto os riscos de tipo tradicional são geridos de forma eficaz, os riscos estratégicos recebem pouca atenção, apesar de serem os mais ameaçadores (PwC, 2012).

A atenção devotada ao tema por acadêmicos e profissionais tem-se traduzido num número crescente de publicações dedicadas à GREmp, bem como guias de implementação propostos por várias associações profissionais (AIRMIC, CIMA, COSO, FERMA, ICAEW, IFAC, IRM, ISO) e uma panóplia de serviços propostos por consultoras (Deloitte, Ernst & Young, KPMG, PwC). As empresas incluem agora quase sempre um espaço, tanto nos relatórios anuais de gestão como nos seus *sites*, dedicado a descrever a forma como gerem os seus riscos. Acompanhando esta tendência, as agências de notação começaram a avaliar o processo de GREmp como uma componente adicional da análise do perfil de crédito das empresas, considerando a sua eficácia como uma marca distintiva de bom governo (S&P, 2008).

2.1.4. Modelos de Gestão de Risco Empresarial

Os proponentes da GREmp argumentam que uma abordagem formal promove uma maior consciencialização sobre a importância da gestão dos riscos, que se traduz em melhores decisões estratégicas e operacionais e num melhor desempenho (Liebenberg & Hoyt, 2003; Miccolis *et al.*, 2001). Outras alegadas vantagens da GREmp incluem um menor custo do capital; um custo dos seguros mais reduzido; um aumento da capitalização bolsista devido a uma menor variabilidade dos resultados; uma melhoria da reputação e imagem; melhores relações com as partes interessadas; uma garantia de integridade dos processos de negócio

críticos; uma maior certeza de que a estratégia planeada é efetivamente realizada; uma melhor compreensão relativamente aos riscos que afetam a organização e uma otimização do *portfolio* de riscos; uma redução na volatilidade dos fluxos de caixa; uma melhor definição de prioridades de investimento; uma conformidade melhorada com leis e regulamentos; um menor número de acontecimentos imprevistos e consequentes perdas; respostas mais rápidas e uma maior aptidão para a mudança; e uma maior propensão para o risco na busca de maiores retornos (Collier, 2009; COSO, 2004; Hoyt & Liebenberg, 2011; Lam, 2003; Liebenberg e Hoyt, 2003; Mikes, 2009, 2011; Miccolis *et al.*, 2001; Nocco & Stulz 2006; Simons, 2000). Segundo Hoyt & Liebenberg (2011), há uma correlação positiva entre o valor empresarial e a utilização da GREmp. Para estes autores, o facto de o ritmo de adoção da GREmp continuar elevado dá credibilidade adicional à visão de que a GREmp contribui para o desempenho organizacional. No entanto as evidências empíricas que confirmam essa relação ainda são limitadas e não são baseadas em medidas robustas da adoção de GREmp (Gates *et al.*, 2012; McShane *et al.*, 2011; Pagach & Warr, 2009).

2.1.4.1. COSO Enterprise Risk Management

A COSO é uma organização criada em 1985, com a finalidade de melhorar o relato financeiro nos EUA. Em 1992 apresentou um modelo de controlo interno, *Internal Control – Integrated Framework* (COSO, 1992), que contém um capítulo dedicado à GR. O COSO-ERM ou COSO 2 (2004) é um desenvolvimento desse esforço inicial, impulsionado pelas exigências da lei de Sarbanes-Oxley de 2002. O novo guia, intitulado *Enterprise Risk Management – Integrated Framework* (COSO, 2004), tem sido promovido pela indústria como o modelo de referência da GREmp e pretende definir as componentes essenciais, uma linguagem comum e uma direção clara para a GREmp.

As componentes do COSO 2 são: (a) Ambiente interno: descrição da organização e da sua abordagem à gestão do risco, fornecendo a base para descrever e analisar os riscos; (b) Definição de objetivos: é da responsabilidade da gestão de topo a definição e comunicação de objetivos, assegurando que estes se encontram alinhados com a missão da organização de forma consistente com o seu apetite pelo risco; (c) Identificação de eventos: reconhecer acontecimentos internos e externos, tanto ameaças como oportunidades; (d) Avaliação dos riscos: análise e avaliação dos riscos, considerando a sua probabilidade de ocorrência e o seu impacto; (e) Resposta aos riscos: decisão sobre a resposta a dar aos diferentes riscos, baseada na exposição ao risco pretendida; (f) Atividades de controlo: políticas e procedimentos que asseguram que as respostas aos riscos são eficazes; (g) Informação e comunicação: mecanismos que asseguram de forma eficiente a identificação, captura e transmissão de informação entre todos os membros da organização; (h) Monitorização: acompanhamento e introdução de modificações no processo quando necessário. O modelo COSO (2004) é representado pelo cubo da Figura 2, em que uma das faces apresenta as oito componentes agora referidas; os quatro ambientes – Estratégico, Operações, Relato e Conformidade – constituem outra face; e os quatro níveis organizacionais – Organização, Divisão, Unidade de Negócio e Subsidiária – se agrupam na face restante.

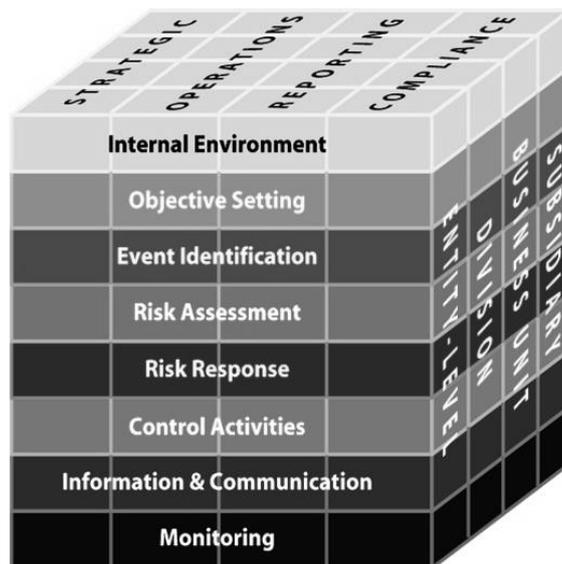


Figura 2: Cubo COSO ERM (COSO, 2004)

2.1.4.2. ISO 31000:2009

A ISO 31000:2009 – Gestão do Risco – Princípios e Linhas de Orientação (ISO, 2009) é uma norma ISO que pretende ser um auxiliar no desenvolvimento, planeamento e melhoria contínua de uma estrutura que integre o processo de GR na cultura, no governo, na estratégia, na gestão e nos processos de toda a organização (Purdy, 2010). A arquitetura proposta pela ISO para gerir os riscos de forma eficaz é composta por 11 princípios, uma estrutura e um processo (ISO, 2009), que se encontram reunidos no Anexo I. Um dos elementos mais importantes da estrutura é a política de risco da organização, que define “as intenções gerais e a direção da organização no que se refere à gestão de risco” (ISO, 2009).

2.1.4.3. Um modelo genérico de Gestão de Risco Empresarial

Existem outros modelos formais de GREmp, sendo dois dos mais utilizados o *Business Risk Model™* (DeLoach, 2000) e o *Risk Management Standard²* (IRM, 2002). Apesar de os vários modelos exibirem abordagens e definições diferentes, o processo de GR segue a mesma

² Idêntico ao modelo da FERMA (2003).

estrutura genérica descrita na Figura 3: uma origem na definição da estratégia e dos objetivos, seguida pela identificação dos riscos, avaliação, tratamento e atividades de monitorização e comunicação (Henriksen & Uhlenfeldt, 2006).



Figura 3: Modelo genérico de Gestão de Risco Empresarial (Henriksen & Uhlenfeldt, 2006)

Os modelos formais de GREmp apresentam ainda outras características comuns, que os distinguem da GR tradicional: (a) são aplicáveis a qualquer tipo de organização; (b) preconizam que a GR deve abarcar todas as unidades de negócio e áreas funcionais, estar incorporada em todos os processos da organização e ser uma atividade contínua; (c) abarcam todos os riscos em todas as categorias; (d) reconhecem que os riscos podem ter consequências positivas e negativas; e (e) definem o vocabulário usado (Arena *et al.*, 2011; Henriksen & Uhlenfeldt 2006).

2.1.5. Classificação dos riscos

Os riscos podem ser tipificados de várias formas e muitas organizações consideram importante definir o seu universo de riscos (DeLoach, 2000), agrupando os riscos em categorias genéricas ou desenvolvendo taxonomias complexas (Chapman, 2006; Lam, 2003).

A taxonomia do *Business Risk Model*[™] (DeLoach, 2000) pode ser consultada no Anexo II. Alguns sectores de atividade económica, como a banca, têm os seus riscos tipificados pelos reguladores (BIS, 2004). Há modelos formais de GREmp que definem as categorias de risco que devem ser consideradas (DeLoach, 2000; IRM, 2002), enquanto outros não o fazem. Mais importante do que uma classificação “correta” dos riscos é a inclusão de todos os riscos relevantes. A classificação dos riscos facilita a identificação dos responsáveis mais apropriados para a sua gestão e contribui para uma melhor definição do apetite pelo risco da organização (Hopkin, 2012). A classificação seguinte, com referência a alguns exemplos representativos, é largamente adotada no meio empresarial (IMA, 2011; IRM, 2002): (a) Riscos puros: incêndio, danos na propriedade, roubo, invalidez, interrupção do negócio, doença, litigação; (b) riscos financeiros: flutuações de preço, taxas de juro, liquidez, crédito, inflação, cambial; (c) riscos operacionais: áreas funcionais, infraestrutura de TIC, orçamentação, contabilidade; (d) riscos estratégicos: reputação, concorrência, novas necessidades, tendências demográficas e socioculturais, inovação, regulação.

2.1.5.1. Classificação dos riscos segundo Kaplan e Mikes

Kaplan & Mikes (2012) propõem uma classificação dos riscos em três categorias: riscos evitáveis, riscos estratégicos e riscos externos. Os riscos evitáveis correspondem aos riscos associados à atividade operacional da empresa. Os eventos que lhes estão associados nunca trazem benefícios e devem por isso ser minimizados. Os riscos externos incluem os riscos relacionados com eventos que estão largamente fora do controlo da empresa. Podem, na melhor das hipóteses, ser identificados e, em caso de ocorrência, mitigados. Os riscos estratégicos correspondem aos riscos deliberados que a empresa assume como indispensáveis para gerar o retorno pretendido e são controláveis em alguma medida. São

os ingredientes essenciais da atividade empresarial, ao apresentarem tanto a possibilidade de ganho como de perda, podendo conduzir a consequências desejáveis ou indesejáveis.

2.1.5.2. Riscos estratégicos

O foco nos riscos estratégicos é a característica principal que distingue a GREmp da GR tradicional (Frigo & Laessoe, 2012). De entre todos os riscos empresariais, Slywotzky & Drzik (2005) consideram o risco de tipo estratégico como “o maior risco de todos”. Entre 1998 e 2009, de entre as 200 maiores companhias do Fortune *Top 1000* que tiveram, no período de um ano, um declínio de valor bolsista superior a 50% (128 casos), 68% admitiram a ocorrência de um risco estratégico como causa desse declínio acentuado (CEB, 2010). Este efeito pronunciado deve-se em grande medida ao facto de não haver formas evidentes de compreender e controlar os riscos estratégicos, uma vez que se encontram ligados a variáveis organizacionais e ambientais caracterizadas por elevado grau de complexidade e incerteza, o que torna difícil a sua quantificação em termos de impacto e probabilidade (Gates, 2006; PwC, 2012). A sua natureza interconetada e difusa contribui para outra característica específica dos riscos estratégicos, a não existência de uma definição consistente de risco estratégico na literatura e na prática, ao contrário do que acontece com os outros tipos de risco, o que também dificulta a sua gestão.

Para caracterizar os riscos estratégicos foi efetuada uma pesquisa das definições existentes na literatura. Para este efeito, é importante ter conhecimento do facto de “*business risk*” ser usado como sinónimo de “*strategic risk*” nalgumas áreas, com relevo para as instituições financeiras (Doff, 2008). As definições selecionadas encontram-se reunidas no Anexo III. Os temas principais que emergem são: (a) Ligação aos objetivos estratégicos. Os riscos estratégicos encontram-se ligados à definição da estratégia, à implementação da estratégia

ou a ambas simultaneamente. (b) Origem interna ou externa. Os riscos estratégicos têm origem na própria organização ou no ambiente externo. (c) Ameaça ou oportunidade com impacto significativo. Os riscos estratégicos podem colocar em causa a sobrevivência da empresa, mas também podem ser uma fonte de vantagem competitiva.

A pesquisa da literatura revela também que “*Strategic Risk Management*” tanto pode denotar “gestão dos riscos estratégicos” como pode ser usada com o significado de “gestão estratégica dos riscos”. Na segunda aceção é um sinónimo de GREmp, englobando todos os tipos de risco e não apenas os estratégicos. Outras expressões equivalentes de GREmp utilizadas frequentemente incluem: *Enterprise-wide risk management* (EWRM), Gestão de risco holística, Gestão de risco integrada, *Corporate risk management* e *Business risk management* (CAS, 2003; DeLoach, 2000; Drew *et al.*, 2006; Henriksen & Uhlenfeldt, 2006; Hoyt & Liebenberg, 2011; Miccolis *et al.*, 2001).

2.1.5.3. Riscos estratégicos ou incertezas estratégicas?

É feita frequentemente uma distinção entre risco e incerteza, originária em Knight (1921), segundo a qual um risco é um evento para o qual é possível estimar uma probabilidade, enquanto em face da incerteza as probabilidades não são computáveis (Bernstein, 1996). Os acionistas podem apoiar as suas decisões de investimento em modelos matemáticos e estatísticos (Markowitz, 1959; Sharpe, 1964), pelo que o seu risco se pode considerar “*knightiano*”. Os gestores, por seu lado, não dispõem de forma geral de dados históricos que permitam prever com exatidão as consequências das suas decisões. As probabilidades associadas podem quando muito ser atribuídas subjetivamente dentro de uma gama e os impactos são difíceis de avaliar. Os gestores estão assim sujeitos, não a riscos, mas a verdadeira incerteza (Sull, 2006). Em face das definições de Knight (1921) sobre risco e

incerteza, os riscos estratégicos poderiam ser designados com maior propriedade como incertezas estratégicas.

2.1.6. Limitações dos modelos de Gestão de Risco Empresarial

Devido à natureza embrionária do conhecimento acumulado sobre o tema, Mikes (2012) considera prematuras as tentativas de codificação da GREmp. As ambições elevadas dos criadores dos modelos chocam com a natureza complexa, incongruente e politizada das organizações e com o “pantanal de problemas desarrumados, confusos e sem soluções técnicas” que a incerteza estratégica produz (Mikes, 2012). Henriksen & Uhlenfeldt (2006) analisam quatro modelos formais de GREmp, concluindo que são particularmente deficientes naquele que devia ser o seu elemento distintivo, a gestão dos riscos estratégicos. A própria COSO (2004) ressalva que a existência de um modelo de GREmp formalizado apenas fornece um grau de segurança razoável de que os objetivos da organização podem ser alcançados, não constituindo uma garantia absoluta de que isso aconteça. Além disso, os erros humanos são frequentes, devido por exemplo a erros de percepção, podendo conduzir a avaliações e decisões incorretas.

Segundo Power (2007), a GREmp reifica um sistema ideal de boa gestão que não se adequa à natureza dinâmica e complexa das organizações modernas, devido ao seu caráter simplista e racionalista. Power (2009) considera problemático o conceito de apetite pelo risco introduzido pela COSO, que assume ser possível definir inequivocamente uma exposição ao risco pretendida com a qual é possível alinhar todos os gestores e áreas da organização. Este pressuposto contradiz os estudos produzidos pela teoria comportamental, que sugerem que as abordagens individuais ao risco são idiossincráticas (Shapira, 1994). Allan & Beer (2006) referem que é impossível identificar todos os riscos que afetam a organização, como

pretendem os modelos. As ameaças estratégicas são muitas vezes potenciadas pela sua natureza interconetada, extravasando a capacidade dos gestores de responderem a várias alterações incrementais simultâneas e impercetíveis ou a vários riscos interdependentes que ocorrem num curto espaço de tempo (Allan & Beer, 2006). Os gestores poderiam intervir mais cedo e assim obter resultados mais favoráveis se detetassem os sinais precoces de alerta que muitas vezes precedem os riscos estratégicos, mas estes sinais não são capturados pelos modelos de GREmp (Allan & Beer, 2006). Como os gestores, seguindo a tendência da população, tendem a associar os riscos com as consequências negativas de acontecimentos indesejados (Shapira, 1994), deixam passar despercebidas as oportunidades associadas aos riscos estratégicos.

A origem dos modelos de GREmp no controlo interno (COSO, 1992) e a sua conotação com os códigos de governo societário (Woods, 2008) desaguam numa tendência para gerir os riscos através da elaboração de controlos detalhados, suportados por uma documentação abundante, seguindo uma abordagem típica do processo de auditoria (Martin & Power, 2007; Power, 2004, 2009) que faz degenerar o processo de GREmp numa conformidade cerimonial com leis e regulamentos para a satisfação de terceiras partes, não tornando a GR numa parte integrante dos processos de negócio e da tomada de decisão dos gestores (Arena *et al.*, 2010; Power, 2007). A prevalência de “formulações de gestão de risco decorativas e perfeccionistas” (Power, 2007) é corroborada por um estudo da Accenture (2011), em que o cumprimento das obrigações legais foi o principal uso da GREmp apontado pelos respondentes, à frente de “Contribuir para crescimento rentável no longo prazo” (2º lugar) e “Rendibilidade futura sustentável” (3º lugar).

2.2. Planeamento estratégico e controlo de gestão

O processo de definição e implementação da estratégia compreende tanto atividades de planeamento como de controlo (Johnson *et al.*, 2008). É possível argumentar que a distinção normalmente efetuada entre planeamento e controlo é artificial, uma vez que o planeamento procura alcançar um estado futuro mais favorável do que aquele que ocorreria na sua ausência e é por isso uma forma de controlo (Merchant & Otley, 2007). No entanto, este estudo adota a visão de Malmi & Brown (2008), que separa os sistemas de tomada de decisão dos sistemas de controlo de gestão.

2.2.1. Planeamento estratégico

2.2.1.1. Estratégia e gestão estratégica

Johnson *et al.* (2008) definem estratégia como “a direção e o âmbito no longo prazo de uma organização, de forma a obter vantagem num ambiente em mudança através da configuração dos seus recursos e competências, com o objetivo de satisfazer as expectativas das partes interessadas” e definem a gestão estratégica como sendo um processo composto por três elementos: a análise estratégica, a escolha estratégica e a implementação da estratégia. Segundo Rumelt (2011), a análise estratégica consiste na identificação dos aspetos cruciais da situação em análise; a escolha estratégica reflete a abordagem geral escolhida para ultrapassar os principais obstáculos identificados; e a implementação da estratégia é efetuada através de planos de ação coerentes entre si e com o diagnóstico e os objetivos gerais. Uma estratégia viável implica uma harmonização dos três elementos (Rumelt, 2011).

2.2.1.2. Gestão estratégica e incerteza

O problema estratégico principal que confronta as organizações é a tomada de decisões sob condições de incerteza significativa relativamente aos estados futuros do mundo (Teece *et al.*, 1997). As decisões estratégicas são as mais complexas que a organização enfrenta, não só devido às interdependências existentes entre os diversos fatores ambientais, mas também devido à incerteza associada às reações dos clientes, respostas dos concorrentes e mudanças tecnológicas e no mercado (Teece, 2009).

Num contexto estratégico, em que o número de variáveis é elevado, os gestores veem a sua capacidade de conhecer e compreender o ambiente bastante reduzida (Simon, 1955). As ideias preconcebidas e as heurísticas dos gestores, juntamente com a cultura da organização são os fatores que mais influenciam as opções tomadas (Shapira, 1994; Tversky & Kahneman, 1974). As limitações cognitivas dos gestores contribuem assim para aumentar ainda mais o efeito da incerteza sobre as decisões estratégicas.

2.2.2. Controlo de gestão

2.2.2.1. Sistemas de controlo de gestão

Merchant & Van der Stede (2007) definem sistemas de controlo de gestão como os instrumentos utilizados para motivar os colaboradores no sentido de tomarem decisões e empreenderem ações benéficas para a organização. Os sistemas de controlo de gestão têm dois propósitos principais: fornecer informação útil aos gestores e ajudar a assegurar que os colaboradores assumem padrões de comportamento viáveis, de forma a atingir os objetivos da organização. Simons (1995, 2000) argumenta que os sistemas de controlo de gestão são “os procedimentos e rotinas formais, baseados na troca de informação, utilizados pelos

gestores para manter ou alterar padrões nas atividades da organização”. O modelo teórico de sistemas de controlo de gestão de Simons (1995) é desenvolvido na secção 2.2.2.3.

2.2.2.2. Pacotes de sistemas de controlo de gestão

O conceito de sistemas de controlo de gestão tem vindo a expandir o seu âmbito, partindo de um foco inicial na comunicação de informação financeira para auxílio na tomada de decisão e avaliação de desempenho, para um âmbito mais lato, que inclui informação não financeira relacionada com processos de produção, informação externa relacionada com mercados, clientes e concorrentes, informação previsional, controlo físico dos ativos, sistemas de orçamentação, procedimentos e políticas e uma gama larga de controlos informais, tanto pessoais como sociais (Chenhall, 2003; Langfield-Smith, 2007).

As organizações não devem focar-se num único sistema de controlo, como por exemplo a medição do desempenho, mas em vários sistemas de controlo a trabalhar em conjunto (Widener, 2007), formando um pacote de sistemas de controlo de gestão (Malmi & Brown, 2008). Os sistemas de controlo de gestão adotados pela organização influenciam significativamente as práticas de gestão (Chenhall, 2003), nomeadamente a formulação da estratégia, a sua implementação e a apetência para a mudança (Langfield-Smith, 2007).

2.2.2.3. O modelo das Alavancas de Controlo

Simons (1995, 2000) desenvolveu um modelo conceptual que pretende explicar a forma como os vários sistemas de controlo de gestão são utilizados como “Alavancas de Controlo” na definição e implementação da estratégia. Existe uma tensão natural entre inovação e controlo, rendibilidade e crescimento, objetivos individuais e organizacionais, os objetivos dos gestores e dos subordinados e entre as inúmeras oportunidades de criar valor no

mercado e o tempo e a atenção limitados que os gestores podem dedicar à sua análise. Um pacote de sistemas de controlo de gestão só é eficaz se consegue reconciliar estas tensões (Simons, 2000). Segundo Simons, são quatro as alavancas de controlo que os gestores têm à sua disposição para gerir estas tensões: sistemas de crenças, sistemas de fronteiras, sistemas de controlo através de diagnóstico e sistemas de controlo interativo.

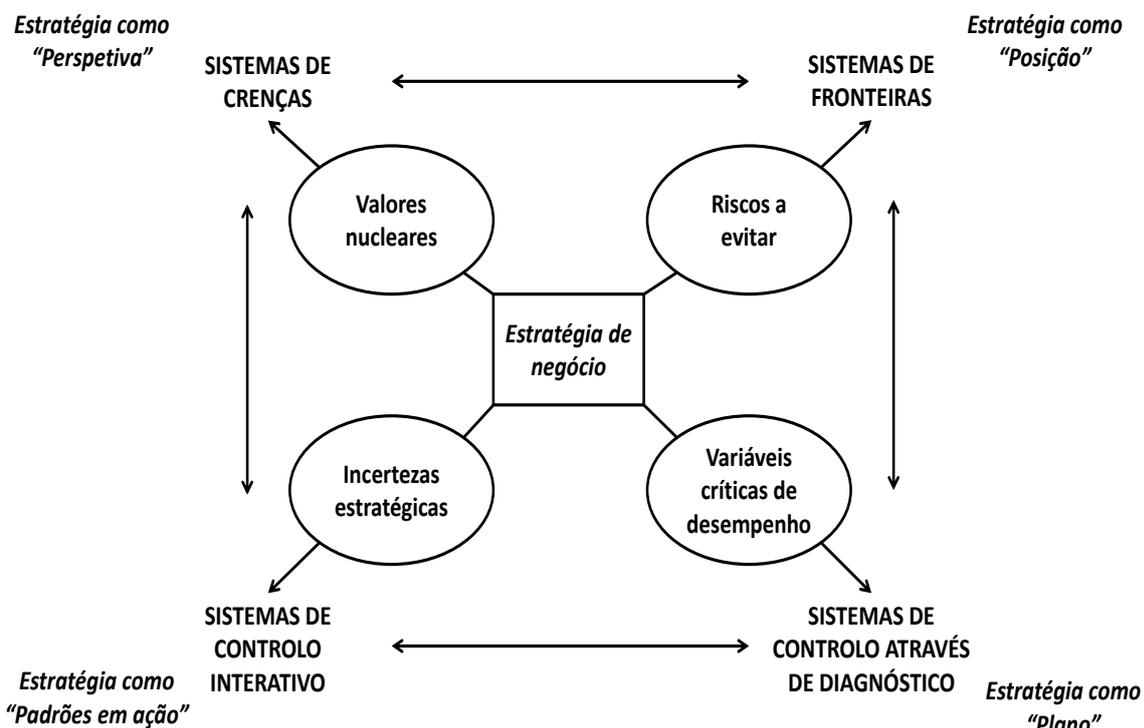


Figura 4: Modelo das Alavancas de Controlo (Simons, 1995)

Os sistemas de crenças definem os valores, a visão e a missão da organização, que são comunicados através de documentos formais e reforçados sistematicamente. São utilizados como inspiração e guias na busca de novas oportunidades (Simons, 1995, 2000).

Os sistemas de fronteiras definem os limites aceitáveis para o campo de atuação onde se desenrolam as atividades dos membros da organização. Uma vez que os gestores não

conseguem estar a par de todos os riscos da organização, ao invés de imporem as oportunidades específicas que devem ser prosseguidas, utilizam os sistemas de fronteiras para colocar limites, tanto nas estratégias possíveis como nas condutas aceitáveis (Simons, 1995).

Os sistemas de controlo através de diagnóstico são usados para motivar, monitorizar e recompensar a obtenção dos resultados pretendidos. O controlo através de diagnóstico abarca todos os sistemas formais utilizados pelos gestores para monitorizar e comunicar as variáveis de desempenho críticas e corrigir os desvios em relação a metas de desempenho predeterminadas. São utilizados para confirmar que tudo se está a desenrolar conforme o previsto e sem percalços (Simons, 1995).

Os sistemas de controlo interativo são usados para estimular a aprendizagem organizacional e a emergência de novas ideias e estratégias, envolvendo os gestores regularmente e pessoalmente nas decisões dos subordinados (Simons, 1995). Ao focarem-se nas incertezas estratégicas, estes sistemas de controlo permitem aos gestores antecipar e responder a oportunidades e ameaças emergentes (Simons, 1995, 2000). As características principais dos sistemas de controlo interativo são (Simons, 1995, 2000): (a) a informação gerada pelo sistema é importante e recorrente na agenda da gestão de topo; (b) focam-se em assuntos que requerem uma atenção regular e frequente dos gestores em todos os níveis da organização; (c) os dados e a informação gerados pelo sistema são interpretados e discutidos face a face em reuniões com superiores, pares e subordinados; e (d) a informação gerada pelo sistema é um catalisador para debater e desafiar continuamente os pressupostos, dados e planos de ação subjacentes.

Para assegurar a implementação com sucesso da estratégia da organização, os gestores têm de compreender os diferentes propósitos que cada um dos quatro tipos de sistemas serve e a forma como se interligam (Simons, 1995). Enquanto os sistemas de crenças e o controlo interativo se baseiam em forças positivas e inspiradoras que encorajam a inovação, os sistemas de fronteira e de diagnóstico asseguram a conformidade com as regras e planos estabelecidos, através de restrições à ação (Simons, 1995). Enquanto os sistemas de crenças e de fronteira são usados em conjunto para enquadrar o domínio estratégico das atividades da organização, os sistemas de diagnóstico e interativos são utilizados para controlar a implementação da estratégia. Mas enquanto os sistemas de controlo através de diagnóstico se concentram na monitorização dos resultados e análise dos desvios em relação às metas definidas, auxiliando os gestores na tradução das estratégias planeadas em estratégias realizadas, os sistemas de controlo interativo focam-se nas incertezas estratégicas e em novas oportunidades, encorajando a experimentação, a aprendizagem e o diálogo, de forma a permitir, não só a concretização das estratégias planeadas, como o surgimento de estratégias emergentes.

Os conceitos de controlo através de diagnóstico e controlo interativo têm relações muito fortes com outros conceitos da literatura. O controlo da implementação da estratégia através de diagnóstico recorre a mecanismos de *feedback*, que acionam aquilo que Argyris & Schön (1978) designam por aprendizagem de *single loop*, enquanto o controlo interativo se baseia em mecanismos de informação *feedforward*, com uma função de aprendizagem de *double loop*, que avaliam continuamente a validade da estratégia e auxiliam na identificação de estratégias emergentes. A aprendizagem *single loop* mantém um processo dentro dos

seus limites definidos, enquanto a aprendizagem *double loop* questiona os fundamentos da estratégia (Simons, 1995).

Widener (2007) considera que a incerteza estratégica e os riscos estratégicos constituem os fatores determinantes na escolha dos sistemas de controlo utilizados. Merchant & Van der Stede (2007) afirmam que a incerteza tem um efeito poderoso sobre a configuração do pacote de sistemas de controlo de gestão, requerendo dos gestores um maior envolvimento pessoal, mais análises preventivas e reuniões presenciais com os subordinados e um maior uso da observação e supervisão direta. O papel central que os riscos e as incertezas estratégicas desempenham no modelo das Alavancas de Controlo justifica a sua escolha neste estudo para enquadrar a introdução da GREmp como um mecanismo adicional de planeamento e controlo na organização. O modelo de Simons tem sido discutido e aplicado em vários estudos académicos (Merchant & Otley 2007; Widener, 2007), por ser considerado útil e significativo no estudo de sistemas de controlo de gestão, especialmente no que se refere à interação destes com a estratégia.

3. Gestão de risco na SINFIC, SA

3.1. Enquadramento da SINFIC, SA

A SINFIC, SA é uma empresa portuguesa que oferece serviços na área das TIC. Em 2012, o seu volume de negócios atingiu cerca de 10 milhões de euros, 80% dos quais realizados em Angola, tendo obtido um resultado operacional de cerca de 2,5 milhões de euros. Foi criada em 1990 e tem cerca de 200 colaboradores, organizados em 12 áreas tecnológicas: ERP, sistemas de fidelização, biometria e geoespacial, entre outras. Gere um programa de projetos baseado nesse *portfolio* de tecnologias, realizando a I&D e produção em Portugal e

as vendas maioritariamente em Angola (SINFIC, 2012). O seu negócio principal desde há uma década tem sido a realização de projetos estruturantes em mercados emergentes, baseados em sistemas de software, mas o seu foco está a mudar para a criação e venda de produtos. É detida na sua totalidade pelos empreendedores originais, com destaque para o acionista principal, que detém cerca de dois terços do capital e é o responsável pela definição da estratégia da empresa, refletindo um estilo de gestão centrado no empreendedor (Mintzberg, 1973).

3.2. Práticas de gestão de risco na SINFIC, SA

Numa fase preliminar da investigação procedeu-se à identificação das práticas de GR existentes na empresa. Os riscos puros são geridos pelas áreas financeira e de logística com recurso à atividade seguradora, que é utilizada para segurar os riscos de acidentes dos colaboradores e os riscos relacionados com os ativos tangíveis. As viaturas estão além disso equipadas com dispositivos de localização, o que diminui o risco de furto.

A GR em projetos constitui o foco principal da GR na empresa. Os riscos são identificados e controlados de acordo com o guia de gestão de projetos PMBOK (PMI, 2004), sendo o seu impacto no projeto avaliado em termos de custo, tempo e qualidade. A gestão dos riscos é efetuada de forma contínua ao longo dos projetos, tanto de forma preventiva como através de ações de mitigação e contingência, no âmbito do sistema de gestão da qualidade da empresa. A GR das TIC é assegurada pela unidade de serviços partilhados, com base em dois modelos específicos de GR e segurança da informação em TIC: COBIT – *Control Objectives for Information and Related Technologies* (IT Governance Institute, 2000) e ISO 27001 (ISO, 2005). A continuidade do negócio, a segurança e privacidade da informação e a proteção contra fraude são fatores críticos para uma empresa que atua na área das TIC.

O processo anual de orçamentação e definição dos planos operacionais das áreas de negócio é uma prática de gestão do risco financeiro, da responsabilidade da área financeira, em colaboração com os gestores e o Conselho de Administração. O resultado do processo são orçamentos por área de negócio, que são depois agregados num orçamento consolidado. O controlo da incerteza consiste na análise mensal ex-post dos desvios encontrados em relação aos resultados previstos que, se forem desfavoráveis, deverão despoletar medidas corretivas pelos gestores das áreas de negócio. Outros instrumentos de gestão de risco financeiro utilizados são uma previsão a curto prazo dos fluxos de caixa e uma análise do risco de crédito dos clientes mais importantes.

Adicionalmente, a empresa é certificada pela norma ISO 9001, o que contribui para a prevenção e correção de erros. A conformidade com o SGQ é assegurada pela auditoria interna, enquanto a auditoria externa se foca na conformidade do relato financeiro. O cumprimento das regras de higiene e segurança no trabalho assegura a integridade física dos colaboradores e o departamento legal lida com os riscos contratuais.

4. Síntese e questão de investigação

Na SINFIC, SA, tal como na maioria das organizações, os riscos estratégicos não são geridos de forma sistemática e de forma integrada com a estratégia. Por outro lado, não existe na literatura referência a um modelo que realize a integração da gestão dos riscos estratégicos com o planeamento estratégico e o controlo de gestão. Este estudo pretende efetuar uma contribuição para o preenchimento desta lacuna teórica e empírica, através da exploração

dos conceitos, modelos e ferramentas da GREmp e da gestão estratégica num contexto prático, aproveitando a posição do seu autor como analista de risco na SINFIC, SA.

É necessário sublinhar que a não existência de uma prática de GR formalizada não significa a sua ausência. A própria sobrevivência da empresa implica a presença da gestão dos riscos estratégicos sob alguma forma, já que a sua existência prolongada não teria sido possível sem pelo menos alguma consciência dos riscos que a afetam (Likierman, 2007). A gestão dos riscos estratégicos é realizada pelo acionista principal e pelo Conselho de Administração da empresa, de maneira informal.

Os riscos estratégicos são uma das justificações da alta taxa de mortalidade das pequenas e médias empresas (Likierman, 2007). Os menores recursos financeiros de uma empresa de média dimensão significam que a ocorrência de um risco estratégico singular pode ser o suficiente para afetar gravemente a sua posição competitiva, pelo que são de esperar benefícios significativos de uma implementação de GREmp numa empresa deste tipo.

Assim, no seguimento da revisão da literatura efetuada e da análise da situação inicial da SINFIC, SA no referente à GR, o presente estudo procura encontrar resposta para a seguinte questão de investigação:

Como podem ser integrados a gestão dos riscos estratégicos e o planeamento estratégico e controlo de gestão nas organizações, de forma a contribuir para a sua sustentabilidade e criação de valor?

5. Metodologia

O ponto de partida descrito na secção anterior sugere a adoção da *action research* como metodologia para conduzir a investigação. A sua característica principal consiste no desenvolvimento de uma colaboração entre o investigador e elementos da organização designados, no sentido de diagnosticar e resolver um problema de especial relevância para a organização (Bryman & Bell, 2007; Eden & Huxham, 1996). A *action research* é uma metodologia qualitativa multifacetada, existindo um debate considerável entre académicos sobre a sua natureza (Bryman & Bell, 2007).

A variante adotada neste estudo é a descrita em Eden & Huxham (1996), que refere as seguintes características adicionais: (a) Utilização de um processo iterativo de identificação do problema, planeamento, ação e avaliação, que conduz à emergência de novos avanços teóricos em pequenos passos incrementais; (b) os resultados da investigação devem ter implicações teóricas que vão para além da resolução do problema concreto da organização; e (c) a investigação deve conduzir a generalizações que possam ser expressas através de ferramentas, técnicas, modelos e métodos aplicáveis noutras situações.

A *action research* é especialmente indicada para indivíduos que escolhem um problema da organização onde se encontram inseridos como foco do seu estudo. A familiaridade com a organização permite-lhes navegar a sua cultura, compreender o calão utilizado e saber a quem se devem dirigir para obter a informação relevante. O nível de compreensão que advém da imersão profunda na organização e do facto de ser um ator no fenómeno em estudo é muito superior ao que um mero observador poderia atingir (Bryman & Bell, 2007).

É usual conduzir a investigação numa única organização e por esse motivo muitos dos procedimentos utilizados são semelhantes aos do estudo de caso. A recolha de dados pode basear-se em diários com impressões subjetivas, documentação sobre o problema, notas de reuniões, questionários e entrevistas (Bryman & Bell, 2007). As principais fontes de informação utilizadas neste trabalho foram a observação direta, conversas informais com um leque alargado de colaboradores da empresa, incluindo dois elementos do Conselho de Administração e vários documentos da empresa sobre estratégia e risco não acessíveis ao público. A investigação desenvolveu-se entre Novembro de 2012 e Julho de 2013.

6. Relevância teórica e empírica do estudo

Nocco & Stulz (2006) consideram que os riscos estratégicos necessitam de ser melhor compreendidos, mesmo não sendo possível quantificá-los com precisão. Gates (2006) considera que a identificação dos riscos estratégicos e a sua gestão no contexto de um processo integrado de GR não têm recebido atenção suficiente por parte do meio académico. Berry & Otley (2009) consideram a relação entre risco e controlo como um tema emergente e sugerem a realização de mais estudos focados na forma como os mecanismos de controlo da GREmp são aplicados na prática. Arena *et al.* (2010) indicam que existem poucas contribuições explorando o funcionamento da GREmp na prática e que tem sido dada pouca atenção à implementação da GREmp em empresas não financeiras. Malmi & Brown (2008) indicam que tem havido muito pouca investigação teórica e empírica sobre o conceito de sistemas de controlo de gestão a funcionar como um pacote, apesar de o conceito já ter várias décadas de existência na literatura de gestão. Chenhall (2003) sugere que se sabe muito pouco sobre o desenho dos sistemas de controlo de gestão apropriados

para lidar com forças complexas e em conflito e propõe a investigação de controlos interativos modernos como forma de gerir as implicações do ambiente externo.

7. Integração do planeamento estratégico e controlo de gestão com a gestão de risco

Mintzberg *et al.* (1976) afirmam que “a tomada de decisão estratégica compreende tanto a exploração de oportunidades como a reação a problemas e a crises”. Se os riscos associados à definição da estratégia não são identificados e geridos, a estratégia está incompleta e em risco de falhar e destruir valor (IMA, 2011). Todos os modelos formais de GReq mencionam explicitamente o papel que a GR deve ter na definição e implementação da estratégia (COSO, 2004; ISO, 2009). O modelo de GReq do IRM (2002) atribui à gestão de risco “um papel central na gestão estratégica de qualquer organização”. Contudo, as diferenças de abordagem e de atores envolvidos no planeamento estratégico e na GR criam uma parceria desajeitada (Holmquist, 2012). As duas perspetivas devem ser entrançadas de modo a obter um todo mais resistente do que a soma das partes (Holmquist, 2012), mas nenhum modelo fornece indicações claras de como esta integração pode ser conseguida na prática (Henriksen & Uhlenfeldt 2006).

Devido a esta lacuna, persiste a prática de encarar a GR e a gestão estratégica como atividades separadas e distintas (Andersen & Schrøder, 2010) e a identificação e análise dos riscos estratégicos é marginalizada (PwC, 2012). Um estudo efetuado pela Economist Intelligence Unit (2010) revela que apenas 44% das organizações respondentes consideram os contributos da GR na definição da estratégia. Num estudo da Ernst & Young (2013), em resposta à questão “Com que frequência são tidas em conta as considerações sobre gestão

de risco nas decisões de planeamento estratégico da organização?”, apenas 27% dos gestores responderam “Sempre” e 39% responderam “Nas decisões mais importantes”. Em muitas organizações, a gestão dos riscos estratégicos ainda não atingiu o nível de maturidade suficiente (EIU, 2010).

A investigação desta problemática decorreu de acordo com o processo iterativo preconizado pela *action research*, oscilando entre a análise da teoria disponível, a realização de experiências utilizando vários modelos e ferramentas da GREmp e da gestão estratégica e a reflexão sobre os resultados obtidos. A repetição destes passos foi conduzindo progressivamente a um aprofundamento do conhecimento sobre o tema e ao desenvolvimento de um modelo conceptual integrado de gestão de riscos estratégicos com o planeamento estratégico e controlo de gestão.

7.1. Integração dos processos de Gestão de Risco Empresarial e planeamento estratégico e controlo de gestão

A melhor forma de aprofundar a viabilidade da estratégia da organização é ligar formalmente os processos de planeamento estratégico e de GREmp (Durfee, 2004). No entanto, para além da reiteração da necessidade de ligar os objetivos estratégicos à identificação dos riscos (DeLoach, 2000), os escassos exemplos descritos na literatura apenas esboçam a forma como a integração processual deve ser efetuada. Andersen & Schrøder (2010) referem que ambos os processos são compostos pela mesma sequência lógica de passos analíticos, o que facilita a sua integração: (a) identificação, recolha de dados e análise; (b) avaliação e planeamento; e (c) planos de ação e monitorização dos resultados.

Woods (2008) considera a maneira como os dois processos devem estar interligados, mas estabelece apenas que a definição da estratégia influencia o apetite pelo risco e que a comunicação dos riscos influencia a definição da estratégia. Na prática, a integração resume-se habitualmente a uma identificação e análise dos riscos estratégicos quando é efetuada a análise SWOT da organização como parte do diagnóstico estratégico, mas sem a frequência e o nível de detalhe adequados (Durfee, 2004).

7.2. Registo de riscos e mapa de riscos

As ferramentas clássicas da GR são o registo de riscos, uma lista de todos os riscos identificados, com a designação dos responsáveis pela sua gestão e as respostas adotadas para cada um, e o mapa dos riscos (*heat map*), uma representação gráfica dos riscos em função da sua probabilidade e impacto (Hopkin, 2012). A utilidade destas ferramentas para a gestão dos riscos estratégicos é discutível, uma vez que a quantificação destes em termos de probabilidade e impacto é difícil e a definição de planos de ação e atribuição de responsabilidades pela sua gestão são problemáticos. Martin & Power (2007) ironizam sobre a facilidade de preencher a coluna da identificação dos riscos, em comparação com os espaços em branco que depois se verificam na coluna dos planos de ação. A manutenção destes documentos é normalmente da responsabilidade da Auditoria Interna, mas Henriksen & Uhlenfeldt (2006) e Frigo & Laessoe (2012) consideram que a GR associada à definição da estratégia deve ser separada da GR nos outros processos e gerida com recurso a métodos e atores organizacionais distintos, sendo uma responsabilidade da gestão de topo. Hopkin (2012) aponta outras desvantagens da utilização destas ferramentas: (a) Fomentam a visão de que as atividades da GR são separadas das outras atividades de gestão e sob a alçada de uma função especializada; (b) representam uma fotografia das atividades de GR da

organização, mas não são revistas com regularidade suficiente; e (c) são documentos estáticos que pouco contribuem para a gestão da organização.

7.3. O CIMA Strategic Scorecard

Alguns autores afirmam que é possível utilizar o *Balanced Scorecard* (Kaplan & Norton, 1996) para ligar as práticas de GR a medidas de gestão de desempenho (Beasley *et al.*, 2006; Calandro & Lane, 2006; IMA, 2011; Kaplan & Mikes, 2012; Woods, 2008). Mas apesar de representarem duas perspectivas complementares, a GREmp e o planeamento estratégico apresentam algumas diferenças que tornam difícil a sua integração no mesmo sistema de controlo (Calandro & Lane, 2006; Woods, 2008). O BSC é inestimável quando se trata de traduzir a estratégia em ação e focar a atenção nos indicadores chaves de desempenho relevantes, mas tem menos sucesso a lidar com a incerteza (IFAC, 2004), devido à natureza difusa e não quantificável dos riscos estratégicos e ao carácter retrospectivo dos sistemas de controlo através de diagnóstico (Palermo, 2011). Além disso, a avaliação de desempenho preocupa-se tipicamente com os resultados a curto prazo da implementação da estratégia, enquanto a perspectiva da GR é mais alargada, focando a atenção nos riscos estratégicos de longo prazo (Palermo, 2011). A insistência na utilização do BSC para todos os propósitos decorre de uma visão míope do controlo, que leva os gestores a conceptualizar os sistemas de controlo de gestão exclusivamente como controlo através de diagnóstico (Simons, 1995, 2000), quando é possível utilizar vários sistemas de controlo de gestão em conjunto, com finalidades diferentes (Malmi & Brown, 2008).

A utilização de um *scorecard* exclusivo para a gestão dos riscos estratégicos pode ser uma abordagem mais adequada (Calandro & Lane, 2006). O *CIMA Strategic Scorecard* é uma ferramenta desenvolvida pela CIMA no âmbito do seu modelo teórico de governo societário,

designado por *Enterprise Governance*, que é composto por duas dimensões: Desempenho (*Business governance*) e Conformidade (*Corporate governance*). Segundo a CIMA, o sucesso empresarial é obtido alcançando um equilíbrio entre estas duas perspetivas. O *Strategic Scorecard* auxilia a gestão de topo na identificação dos problemas chave sobre os quais é necessário tomar decisões, na avaliação das opções estratégicas a tomar, no faseamento da implementação da estratégia, e na identificação e mitigação dos riscos estratégicos, contribuindo para gerir a perspetiva Desempenho de uma forma preventiva e proativa (IFAC, 2004). A representação esquemática do *Strategic Scorecard* encontra-se na Figura 5.

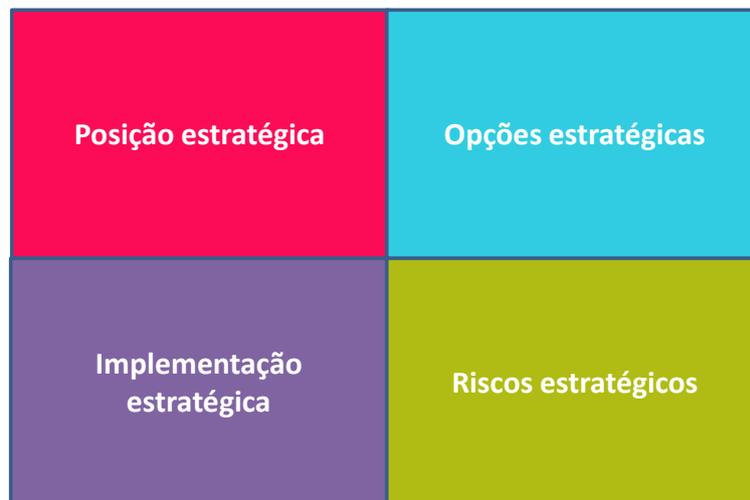


Figura 5: CIMA *Strategic Scorecard* (IFAC, 2004)

Posição estratégica: Esta dimensão foca-se na informação necessária para avaliar a posição estratégica atual da organização. Engloba informação externa, tal como desenvolvimentos a nível económico, político, regulamentar ou de mercado e fatores internos tais como competências e recursos (CIMA, 2007).

Opções estratégicas: As opções estratégicas são aquelas que possuem o maior potencial para criar ou destruir valor. Tipicamente, não haverá mais de quatro ou cinco opções estratégicas ativas simultaneamente. Os gestores selecionam as que consideram mais adequadas para serem detalhadas em planos de negócio formais (CIMA, 2007).

Riscos estratégicos: Neste quadrante a gestão foca-se exclusivamente nos riscos estratégicos que constituem as maiores ameaças à concretização da estratégia e propõe planos de mitigação ou a exploração de oportunidades. Isto pressupõe que a organização tem o seu apetite pelo risco definido de forma clara (CIMA, 2007).

Implementação estratégica: O foco é na identificação de pontos temporais que permitam monitorizar a implementação da estratégia. Se esta não estiver a decorrer de acordo com o plano, poderão ser necessárias medidas corretivas. O objetivo não é a imersão da gestão de topo nos detalhes operacionais, mas sim garantir que os planos de ação suportam a implementação com sucesso da estratégia, uma vez que uma análise cuidada de nada serve se a estratégia não é bem executada (CIMA, 2007).

O *Strategic Scorecard* não é um substituto do plano estratégico. Destina-se a ajudar a gestão de topo a assegurar que todos os componentes do processo estratégico foram devidamente contemplados, assim como os riscos estratégicos associados (CIMA, 2007).

8. Resultados da investigação

A *action research* efetuada na empresa convergiu, ao fim de várias iterações, numa proposta de definição de risco estratégico e num modelo conceptual de integração do planeamento estratégico e controlo de gestão com a gestão dos riscos estratégicos.

8.1. Definição de riscos estratégicos

Uma definição possível de riscos estratégicos, que considera os temas dominantes na literatura, é a seguinte:

Os riscos estratégicos são os riscos internos ou externos, que podem ocorrer tanto na definição como na implementação da estratégia e com potencial para alterar significativamente a posição competitiva da organização.

A posição competitiva da organização pode ser avaliada em termos de recursos disponíveis, situação financeira, quota de mercado ou rendibilidade, entre outros. Esta definição de risco estratégico não requer uma quantificação em termos de probabilidade, que é problemática, pelo que é necessário exercer julgamento ao decidir se um risco estratégico com impacto significativo mas probabilidade residual deve ou não ser considerado como relevante.

8.2. Modelo conceptual de integração da gestão dos riscos estratégicos com o planeamento estratégico e controlo de gestão

Enquanto a gestão estratégica lida com as decisões estratégicas e oportunidades de investimento, a identificação dos riscos que lhes estão associados prepara a organização para acontecimentos inesperados. O modelo conceptual para a realização de uma abordagem integrada da gestão dos riscos estratégicos com as atividades estratégicas da organização é apresentado na Figura 6, seguido da sua descrição.

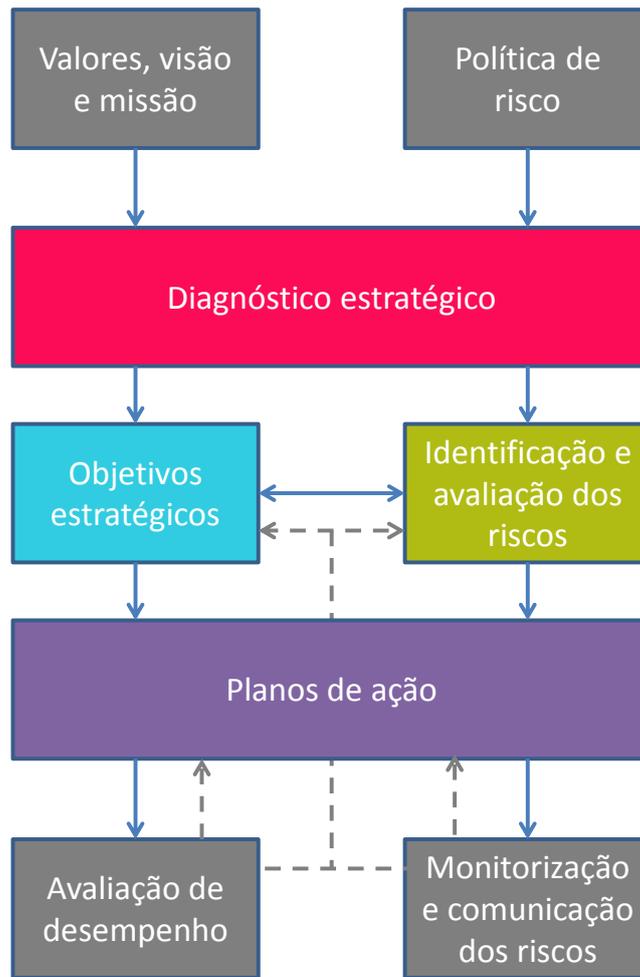


Figura 6: Modelo conceptual de integração dos processos de gestão dos riscos estratégicos e de planeamento estratégico e controlo de gestão (Elaboração própria)

Domínio do planeamento:

O processo de GREmp começa pela definição do contexto, que engloba o diagnóstico estratégico e a definição de objetivos (ISO, 2009), dois elementos que são comuns à gestão estratégica. A definição dos objetivos estratégicos e a identificação e avaliação dos riscos são duas componentes interatuantes. Uma estratégia planeada pode ser inviabilizada pela identificação de certos riscos, enquanto os riscos identificados no ambiente limitam à partida as estratégias que podem ser seguidas. Os planos de ação derivam da análise conjunta dos objetivos estratégicos e da identificação e avaliação dos riscos associados,

sendo artificial a distinção efetuada habitualmente entre planos de ação estratégicos e planos de resposta aos riscos.

Domínio do controlo:

O modelo aplica o conceito de pacote de sistemas de controlo de gestão (Malmi & Brown, 2008), instanciado pelo modelo das alavancas de controlo de Simons (1995, 2000).

(a) Os valores, visão e missão da organização corporizam um sistema de crenças (Simons, 2000).

(b) Os elementos principais da política de risco são a definição do apetite pelo risco da organização, as responsabilidades na gestão do risco e o vocabulário comum. No que respeita à gestão dos riscos estratégicos, a política de risco define: (a) a responsabilidade da gestão de topo na gestão dos riscos estratégicos; e (b) o que constitui um risco estratégico, utilizando-se a definição proposta em (8.1.). O potencial para alterar significativamente a posição competitiva da organização, referido na definição, é uma avaliação que dependerá do apetite pelo risco da organização, que é definido no âmbito mais geral da política. A política de risco é um sistema de controlo que tem essencialmente características de fronteira (Simons, 2000). Ajuda a organização a definir o seu território de atuação e a limitar os comportamentos dos colaboradores, ao definir explicitamente o que são considerados riscos estratégicos.

Os valores, visão e missão da empresa e a sua política de risco estão intimamente ligados, refletindo a visão dos acionistas sobre a relação entre recompensa e risco que consideram

desejável. O apetite pelo risco influencia a escolha dos mercados e dos sectores de atividade económica em que a empresa atua e vice-versa.

(c) O sistema habitual para controlar a implementação da estratégia é o BSC, mas podem ser utilizados adicionalmente muitos outros sistemas de controlo através de diagnóstico (Simons, 2000), como por exemplo o controlo orçamental. Palermo (2011) propõe que a GR é eficaz se os resultados obtidos para os indicadores chave de desempenho estão sistematicamente dentro das tolerâncias, ou seja, dos limites aceitáveis de variação definidos pela organização (IMA, 2011) que decorrem do seu apetite pelo risco. Além da interpretação óbvia dos desvios desfavoráveis como sintomas de riscos não identificados, os resultados muito acima das expectativas podem significar que as metas foram mal definidas ou que os riscos associados não foram bem compreendidos, podendo os resultados favoráveis no curto prazo estar a ser obtidos à custa de riscos futuros (Palermo, 2011; Van der Stede, 2009).

(d) A monitorização e comunicação dos riscos estratégicos são feitas com recurso ao CIMA *Strategic Scorecard*. Este tem o carácter de um controlo predominantemente interativo (Simons, 1995), já que (a) aborda as incertezas estratégicas que são determinantes para os objetivos da organização; e (b) pode ser usado regularmente pela gestão de topo como ferramenta de discussão e envolvimento com os restantes elementos da organização. A utilização do *Strategic Scorecard* para controlar a incerteza associada à estratégia incorpora um elemento de “ceticismo quantitativo”, que contrabalança o “entusiasmo quantitativo” (Mikes, 2009) normalmente associado aos sistemas de controlo através de diagnóstico baseados em indicadores de desempenho.

Relações entre planeamento e controlo:

A atuação conjunta da avaliação de desempenho e da monitorização dos riscos estratégicos assemelha-se ao que Schreyögg & Steinmann (1987) e Preble (1992) designam por controlo estratégico, constituído pelo controlo da implementação, controlo das premissas e vigilância estratégica. O controlo das premissas é um processo contínuo de monitorização do ambiente externo que questiona constantemente a validade dos pressupostos que foram assumidos na definição da estratégia (Preble, 1992; Schreyögg & Steinmann, 1987). A vigilância estratégica é uma atividade de espetro largo que envolve perscrutar o ambiente de uma forma permanente, de forma a detetar antecipadamente acontecimentos ou questões relevantes, tanto dentro como fora da organização, que possam desestabilizar significativamente a direção estratégica assumida (Schreyögg & Steinmann, 1987).

Enquanto a avaliação de desempenho controla a implementação da estratégia com recurso ao BSC e sugere medidas corretivas aos planos de ação utilizando mecanismos de *feedback*, o *Strategic Scorecard* corporiza um controlo *feedforward* que auxilia a organização no controlo das premissas e na vigilância estratégica, sugerindo alterações aos objetivos. Um dos objetivos do controlo estratégico é permitir às organizações operar estrategicamente de uma maneira mais fluida e flexível (Preble, 1992; Schreyögg & Steinmann, 1987), assinalando a necessidade de uma reformulação estratégica se as condições ambientais tornarem os objetivos estratégicos definidos irrelevantes ou inválidos (Schreyögg & Steinmann, 1987). Enquanto a definição dos valores, visão, missão e política de risco é da responsabilidade dos acionistas, o controlo estratégico é da responsabilidade da gestão de topo.

Monitorização e comunicação:

Hopkin (2012) defende que a informação sobre os riscos da organização não deve ser analisada isoladamente mas sim integrada com a restante informação de gestão. A integração, num mesmo relatório, de informação sobre avaliação de desempenho, com recurso ao BSC e sobre a monitorização dos riscos estratégicos, através do *Strategic Scorecard*, fornece uma visão a grande altitude dos objetivos gerais da organização, dos riscos estratégicos associados e do progresso da implementação.

Aplicação do modelo na SINFIC, SA:

As várias práticas de GR não integradas e quase independentes encontradas no início da investigação constituem a situação típica quando se inicia uma implementação de GREmp (Frigo & Laessoe, 2012). A adição da gestão formalizada dos riscos estratégicos às práticas já existentes de gestão dos riscos puros, financeiros e operacionais permite instanciar um modelo de GREmp adaptado à SINFIC, SA. Esta implementação separa claramente a gestão dos riscos estratégicos, efetuada pela gestão de topo, da gestão dos outros tipos de risco, da responsabilidade das áreas operacionais, pelo que pode ser considerada contrária ao espírito holístico da GREmp. É também, no entanto, a abordagem sugerida por Henrikssen & Uhlenfeldt (2006) e em utilização na LEGO (Frigo & Laessoe, 2012). Um dos princípios da ISO 31000 refere que a GR é feita à medida (ISO, 2009) e Arena *et al.* (2011) referem que as implementações de GREmp apresentam muitas variações na prática.

9. Conclusão

9.1. Principais conclusões

Este estudo pretendeu determinar de que forma a gestão dos riscos estratégicos e o planeamento estratégico e controlo de gestão podem ser integrados, de forma a contribuir para a sustentabilidade e criação de valor nas organizações. A investigação baseou-se na realização de *action research* numa empresa de média dimensão, da qual resultaram uma definição de risco estratégico e um novo modelo conceptual de integração dos processos de gestão dos riscos estratégicos e de planeamento estratégico e controlo de gestão.

Os riscos estratégicos foram definidos como os riscos internos ou externos, que podem ocorrer tanto na definição como na implementação da estratégia e com potencial para alterar significativamente a posição competitiva da organização (8.1). A definição na política de risco do que constitui um risco estratégico contribui para a explicitação do apetite pelo risco, melhores decisões estratégicas, planos de ação mais eficazes e uma maior concretização dos objetivos.

O modelo integrado de gestão estratégica e gestão dos riscos estratégicos que resultou da investigação promove a antecipação estratégica, a aprendizagem e o aparecimento de estratégias emergentes, ao incorporar sistemas de controlo de gestão especialmente dedicados ao risco e à incerteza (8.2.). A política de risco delimita de forma mais precisa o campo de atuação da empresa do que o recurso exclusivo à definição dos valores, visão e missão.

9.2. Limitações e sugestões para investigação futura

A *action research* é criticada pela imprecisão associada à sua definição e pela dificuldade de replicação dos estudos (Bryman & Bell, 2007), observação que também é válida para grande parte das metodologias qualitativas. Nem toda a informação relevante pode ser capturada e transmitida aos gestores através de sistemas de controlo formais. A limitação científica mais importante é a exclusão dos controlos informais do âmbito do estudo. Estes recebem normalmente pouca atenção apesar de serem um elemento significativo dos pacotes de sistemas de controlo de gestão (Malmi & Brown, 2008). Fica por resolver a questão de como reconhecer precocemente um conjunto de vários pequenos riscos operacionais com potencial para se transformar num risco com impacto estratégico. Os resultados desta tese podem servir como veículos teóricos para a realização de mais investigação na área da GREmp, nomeadamente estudos de caso de aplicação do modelo desenvolvido.

Referências bibliográficas

- Accenture (2011). *Report on the Accenture 2011 Global Risk Management Study*. [Em linha]. Disponível em: <http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Global-Risk-Management-Study-2011.pdf> [Acesso em: 2013-09-27].
- Allan, N. & Beer, L. (2006). *Strategic risk: It's all in your head*. [Em linha]. Disponível em: <http://www.bath.ac.uk/management/research/pdf/2006-01.pdf> [Acesso em: 2013-09-27].
- Allen, B. (2007). *The best-laid plans...* [Em linha]. Disponível em: <http://www.risk.net/risk-magazine/analysis/1506621/the-laid-plans> [Acesso em: 2013-09-27].
- Andersen, T. J., & Schrøder, P. W. (2011). *Strategic Risk Management Practice: How to Deal Effectively with Major Corporate Exposures*. Cambridge (UK); New York: Cambridge University Press.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, 35(7), 659–675.
- Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real? *Journal of Risk Research*, 14(7), 779–797.
- Argyris, C., & Schön, D. A. (1978). *Organizational Learning; A Theory of Action Perspective*. Reading, Mass.: Wesley.
- Baird, I. S., & Thomas, H. (1985). Toward a contingency model of strategic risk taking. *Academy of Management Review*, 10(2), 230–243.
- Bank for International Settlements (2004). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. [Em linha]. Disponível em: <http://www.bis.org/publ/bcbs107.htm>. [Acesso em: 2013-09-27].
- Beasley, M. S., Chen, A., Nunez, K., & Wright, L. (2006). Working hand in hand: Balanced Scorecards and Enterprise Risk Management. *Strategic Finance*, 87(9), 49–55.

- Bernstein, P. L. (1996). *Against the Gods: The Remarkable Story of Risk*. New York: J. Wiley & Sons.
- Berry, A. J., Coad, A. F., Harris, E. P., Otley, D. T., & Stringer, C. (2009). Emerging themes in management control: A review of recent literature. *The British Accounting Review*, 41(1), 2–20.
- Bryman, A., & Bell, E. (2007). *Business Research Methods*. Oxford: Oxford University Press.
- Calandro Jr, J., & Lane, S. (2006). An introduction to the Enterprise Risk Scorecard. *Measuring Business Excellence*, 10(3), 31–40.
- Casualty Actuarial Society (2003). *Overview of Enterprise Risk Management*. [Em linha]. Disponível em: <http://www.casact.org/area/erm/overview.pdf>. [Acesso em: 2013-09-27].
- Chapman, R. J. (2006). *Simple Tools and Techniques for Enterprise Risk Management*. Chichester: John Wiley.
- Chartered Institute of Management Accountants (2007). *CIMA Strategic Scorecard: Boards engaging in strategy*. [Em linha]. Disponível em: http://www1.cimaglobal.com/Documents/ImportedDocuments/tech_execrep_strategic_scorecard_boards_engaging_in_strategy_mar_2007.pdf. [Acesso em: 2013-09-27].
- Chenhall, R. H. (2003). Management control systems design within its organizational context: findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, 28(2–3), 127–168.
- Collier, P. M. (2009). *Fundamentals of Risk Management for Accountants and Managers Tools & Techniques*. Amsterdam; Boston; London: Elsevier/Butterworth-Heinemann.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), *Internal Control – Integrated Framework*. New York: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise Risk Management - Integrated Framework*. New York: American Institute of Certified Public Accountants.

Corporate Executive Board (2010). *Audit Director Roundtable: Root Causes of Corporate Decline 1998-2009*. [Em linha]. Disponível em: http://www.executiveboard.com/blogs/uploads_views/2011/02/Audit-Director-Roundtable-Root-Causes-of-Corporate-Decline.pdf. [Acesso em: 2013-09-27].

Crouhy, M., Galai, D., & Mark, R. (2006). *The Essentials of Risk Management*. New York: McGraw-Hill.

DeLoach, J. (2000). *Enterprise-Wide Risk Management: Strategies for Linking Risk & Opportunity*. Harlow: Financial Times Management.

Dickinson G. (2001). Enterprise risk management: Its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance*, 26(3), 360–6.

Doff, R. (2008). Defining and measuring business risk in an economic-capital framework. *Journal of Risk Finance*, 9(4), 317–333.

Drew, S. A., Kelley, P. C., & Kendrick, T. (2006). CLASS: Five elements of corporate governance to manage strategic risk. *Business Horizons*, 49(2), 127-138.

Durfee, D. (2004). Watch your back: As companies map their growth strategies, they should pay more attention to potential hazards. *CFO*, 20(10), 61-62.

Economist Intelligence Unit (2010). *Fall guys: Risk management in the front line*. [Em linha]. Disponível em: <http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/iarcs-erm.pdf>. [Acesso em: 2013-09-27].

- Eden, C., & Huxham, C. (1996). Action research for management research. *British Journal of Management*, 7(1), 75-86.
- Emblemsvåg, J., & Kjølstad, L. E. (2002). Strategic risk analysis – a field version. *Management Decision*, 40(9), 842–852.
- Ernst & Young (2013). *Business Pulse: Exploring dual perspectives on the top 10 risks and opportunities in 2013 and beyond*. [Em linha]. Disponível em: [http://www.ey.com/Publication/vwLUAssets/Business_Pulse_-_top_10_risks_and_opportunities/\\$FILE/Business%20pulse%202013.pdf](http://www.ey.com/Publication/vwLUAssets/Business_Pulse_-_top_10_risks_and_opportunities/$FILE/Business%20pulse%202013.pdf). [Acesso em: 2013-09-27].
- Federation of European Risk Management Associations (2003). *A Risk Management Standard*. [Em linha]. Disponível em: <http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-version.pdf>. [Acesso em: 2013-09-27].
- Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*, 22(3), 81–88.
- Frigo, M. L., & Laessoe, H. (2012). Strategic risk management at the LEGO Group. *Strategic Finance*, 93(8), 27.
- Gates, S. (2006). Incorporating strategic risk into Enterprise Risk Management: A survey of current corporate practice. *Journal of Applied Corporate Finance*, 18(4), 81–90.
- Gates, S., Nicolas, J.-L., & Walker, P. L. (2012). Enterprise risk management: A process for enhanced management and improved performance. *Management Accounting Quarterly*, 13(3), 28.
- Glassman, C. (2001). Strategic Risk: Quadruple Jeopardy. *RMA Journal*, 84(1), 52

- Henriksen, P. & Uhlenfeldt, T. (2006). Contemporary Enterprise-Wide Risk Management Frameworks: A Comparative Analysis in a Strategic Perspective. In: Andersen, T. J., (Ed.) *Perspectives on Strategic Risk Management*. Køge, Denmark; Herndon, VA: Copenhagen Business School Press, pp. 107-129
- Holmquist, E. (2012). Risk Management and Business Strategy. *RMA Journal*. 95(7-8), 40-45
- Hopkin, P. (2012). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management* (2nd ed.). London: Kogan Page.
- Hoyt, R. E., & Liebenberg, A. P. (2011). The value of Enterprise Risk Management. *Journal of Risk and Insurance*, 78(4), 795–822.
- Institute of Management Accountants (2011). *Enterprise Risk Management: Frameworks, Elements, and Integration*. [Em linha]. Disponível em: http://www.imanet.org/PDFs/Public/Research/SMA/ERM_Frameworks,%20Elements,%20and%20Integration.pdf. [Acesso em: 2013-09-27].
- Institute of Risk Management (2002). *A Risk Management Standard*. [Em linha]. Disponível em: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf. [Acesso em: 2013-09-27].
- International Federation of Accountants (2004). *Enterprise Governance: Getting the Balance Right*. [Em linha]. Disponível em: <http://www.ifac.org/sites/default/files/publications/files/enterprise-governance-gett.pdf>. [Acesso em: 2013-09-27].
- ISO (2005). *ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*. Geneva: International Standards Organization.

- ISO (2009). *ISO 31000:2009 – Risk Management – Principles and Guidelines*. Geneva: International Standards Organization.
- IT Governance Institute (2000). *CobiT. Control Objectives for Information and Related Technologies* (3rd ed.). Rolling Meadows, IL: IT Governance Institute.
- Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy*. Harlow: Financial Times Prentice Hall.
- Kaplan, R. S., & Norton, D. P. (1996). *The Balanced Scorecard: Translating Strategy into Action*. Boston, MA: Harvard Business Press.
- Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, 90(6), 48–60.
- Knight, F. (1921). *Risk, Uncertainty and Profit*. [Em linha]. Disponível em: <http://www.econlib.org/library/Knight/knRUP.html>. [Acesso em: 2013-09-27].
- Lam, J. (2003). *Enterprise Risk Management: From Incentives to Controls*. Hoboken, N.J.: Wiley.
- Langfield-Smith, K. (2007). A Review of Quantitative Research in Management Control Systems and Strategy. In: Chapman, C. S., Hopwood, A. G., & Shields, M. D., (Eds.) *Handbook of Management Accounting Research [Volume 2]*. Amsterdam; Boston: Elsevier, pp. 753-783.
- Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37–52.
- Likierman, A. (2007). Risk in Performance Measurement. In: Neely, A. D. (Ed.) *Business Performance Measurement: Unifying Theories and Integrating Practice*. Cambridge; New York: Cambridge University Press, pp. 261-278.

- Malmi, T., & Brown, D. A. (2008). Management control systems as a package – Opportunities, challenges and research directions. *Management Accounting Research*, 19(4), 287–300.
- Markowitz, H. M. (1959). *Portfolio Selection: Efficient Diversification of Investments* (1st ed.). New York: John Wiley & Sons.
- Martin, D., & Power, M. (2007). *The End of Enterprise Risk Management*. [Em linha]. Disponível em: http://regulation2point0.org/wp-content/uploads/downloads/2010/04/RP07-22_topost.pdf. [Acesso em: 2013-09-27].
- McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value?. *Journal of Accounting, Auditing & Finance*, 26(4), 641-658.
- Merchant, K. A. & Otley, D. T. (2007). A Review of the Literature on Control and Accountability. In: Chapman, C. S., Hopwood, A. G., & Shields, M. D. (Eds). *Handbook of Management Accounting Research [Volume 2]*. Amsterdam; Boston: Elsevier, pp. 785-802.
- Merchant, K. A., & Van der Stede, W. A. (2007). *Management Control Systems: Performance Measurement, Evaluation and Incentives* (2nd ed.). Harlow: Pearson Education.
- Miccolis, J. A., Hively, K., Merkley, B. W. (2001). *Enterprise Risk Management: Trends and Emerging Practices*. Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation.
- Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18–40.
- Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, 36(4–5), 226–245.
- Mikes, A. (2012). The Struggle to Codify Risk Management. *Risk & Regulation*, 24(4), 18–19.
- Mintzberg, H. (1973). Strategy-Making in Three Modes. *California Management Review*, 16(2), 44-

- Mintzberg, H., Raisinghani, D., & Théorêt, A. (1976). The Structure of “Unstructured” Decision Processes. *Administrative Science Quarterly*, 21(2), 246–275.
- Munich Re Group (2011). *2011 Annual Report*. [Em linha]. Disponível em: http://www.munichre.com/publications/302-07342_en.pdf. [Acesso em: 2013-09-27].
- Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and practice. *Journal of Applied Corporate Finance*, 18(4), 8–20.
- Pagach, D. P., & Warr, R. S. (2010). *The Effects of Enterprise Risk Management on Firm Performance*. [Em linha]. Disponível em: <http://ssrn.com/abstract=1155218>. [Acesso em: 2013-09-27].
- Palermo, T. (2011) *Integrating risk and performance in management reporting*. [Em linha]. Disponível em: http://www.cimaglobal.com/Documents/Thought_leadership_docs/6307_R269_Integrating%20risk_FINAL.pdf. [Acesso em: 2013-09-27].
- Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos.
- Power, M. (2007). *Organized uncertainty: designing a world of risk management*. Oxford: Oxford Univ. Press.
- Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6–7), 849–855.
- Preble, J. F. (1992). Towards a Comprehensive System of Strategic Control. *Journal of Management Studies*, 29(4), 391–408.
- Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge: PMBOK Guide* (4th ed.). Newton Square, PA: Project Management Institute.

- Purdy, G. (2010). ISO 31000:2009 – Setting a new standard for risk management. *Risk Analysis*, 30(6), 881–886.
- PwC (2012). *Black swans turn grey – The transformation of risk*. [Em linha]. Disponível em: <http://www.pwc.co.uk/governance-risk-compliance/issues/risk-practices-black-swans-turn-grey-the-transformation-of-the-risk-landscape.jhtml>. [Acesso em: 2013-09-27].
- Rittenberg, L. & Martens, F. (2012). *Understanding and Communicating Risk Appetite*. [Em linha]. Disponível em: http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf. [Acesso em: 2013-09-27].
- Rumelt, R. P. (2011). *Good Strategy, Bad Strategy: The Difference and Why it Matters*. New York: Crown Business.
- Schreyögg, G., & Steinmann, H. (1987). Strategic control: A new perspective. *The Academy of Management Review*, 12(1), 91–103.
- Shapira, Z. (1994). *Risk Taking: A Managerial Perspective*. New York: Russell Sage Foundation.
- Sharpe, W. F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance*, 19(3), 425–442.
- Simon, H. A. (1955). A behavioral model of rational choice. *Quarterly Journal of Economics*, 69(1), 99–118.
- Simons, R. (1995). *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Boston, Mass.: Harvard Business School Press.
- Simons, R. (2000). *Performance Measurement & Control Systems for Implementing Strategy*. Upper Saddle River, N.J.: Prentice Hall.
- SINFIC, SA (2012). *Relatório e Contas 2012*. [Em linha]. Disponível em: <http://www.sinfic.pt/SinficWeb/docs/73480.pdf>. [Acesso em: 2013-09-27].

- Slywotzky, A. J., & Drzik, J. (2005). Countering the biggest risk of all. *Harvard Business Review*, 83(4), 78–88.
- Society of Actuaries (2006). *Enterprise Risk Management Specialty Guide*. [Em linha]. Disponível em: <http://www.soa.org/library/professional-actuarial-specialty-guides/enterprise-risk-management/2005/august/spg0605erm.pdf>. [Acesso em: 2013-09-27].
- Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640–661.
- Standard & Poor's (2008). *Standard & Poor's To Apply Enterprise Risk Analysis To Corporate Ratings*. [Em linha]. Disponível em: <http://www.standardandpoors.com/ratings/articles/en/us/?articleType=PDF&assetID=1245200609007>. [Acesso em: 2013-09-27].
- Sull, D. (2006). *Difficult decisions for an uncertain world*. [Em linha]. Disponível em: <http://www.ft.com/cms/s/2/84c40126-b44a-11da-bd61-0000779e2340.html#axzz2g8vJUYSV>. [Acesso em: 2013-09-27].
- Teece, D. J. (2009). *Dynamic Capabilities and Strategic Management*. Oxford: Oxford University Press.
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.
- Telford, T. (2005). *Strategic Risk – A Guide for Directors*. London: Telford Publishing.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124–1131.
- Van der Stede, W. A. (2009). Enterprise governance: Risk and performance management through the business cycle. *CMA Management*, 83(3), 24

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations and Society*, 32(7–8), 757–788.

Woods, M. (2008). Linking risk management to strategic controls: a case study of Tesco plc. *International Journal of Risk Assessment and Management*, 7(8), 1074-1088.

Anexos

Anexo I – ISO 31000:2009 – Princípios, estrutura e processo

Princípios da ISO 31000:2009:

- a) A gestão do risco cria e protege o valor.
- b) A gestão do risco é parte integrante de todos os processos organizacionais.
- c) A gestão do risco é parte da tomada de decisão.
- d) A gestão do risco considera explicitamente a incerteza.
- e) A gestão do risco é sistemática, estruturada e atempada.
- f) A gestão do risco baseia-se na melhor informação disponível.
- g) A gestão do risco é feita à medida.
- h) A gestão do risco tem em conta fatores humanos e culturais.
- i) A gestão do risco é transparente e participada.
- j) A gestão do risco é dinâmica, iterativa e reativa à mudança.
- k) A gestão do risco facilita a melhoria contínua da organização.

Estrutura da GR da ISO 31000:2009:

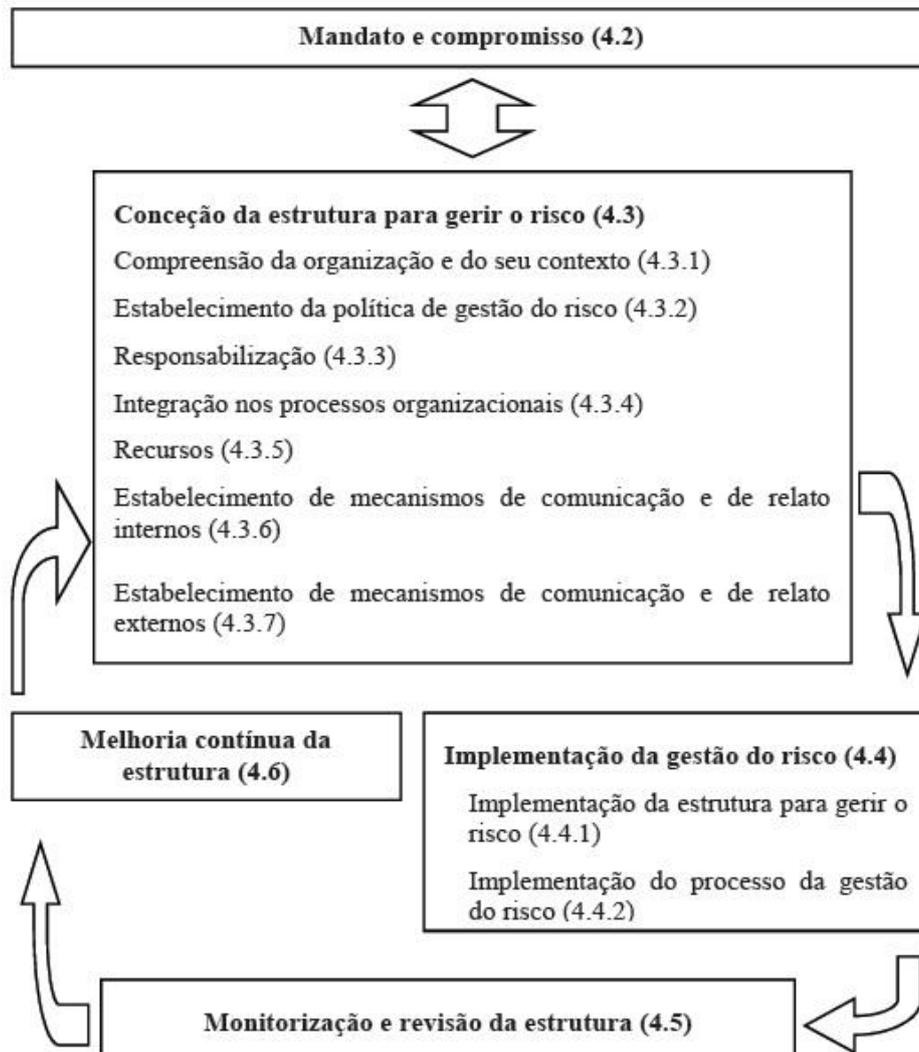


Figura 7: ISO 31000:2009 - Estrutura da gestão de risco (ISO, 2009)

Processo de GR da ISO 31000:2009:

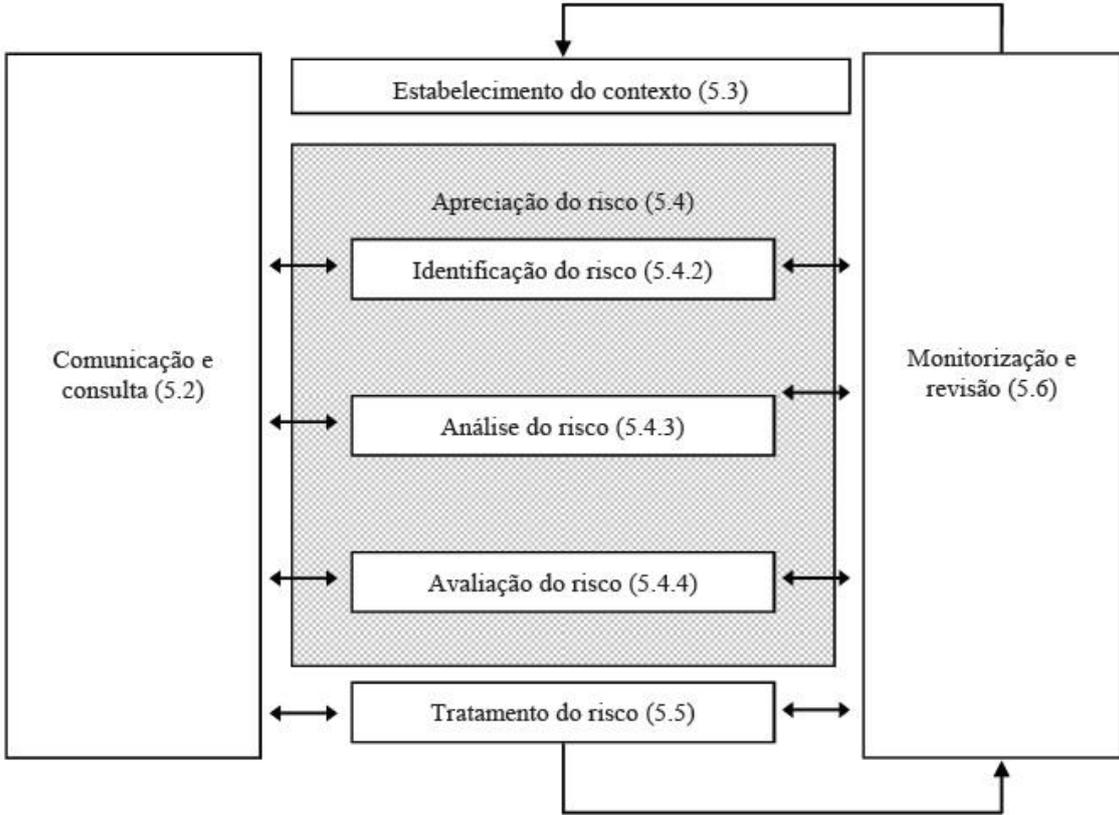


Figura 8: ISO 31000:2009 - Processo de gestão de risco (ISO, 2009)

Anexo II - Business Risk Model™

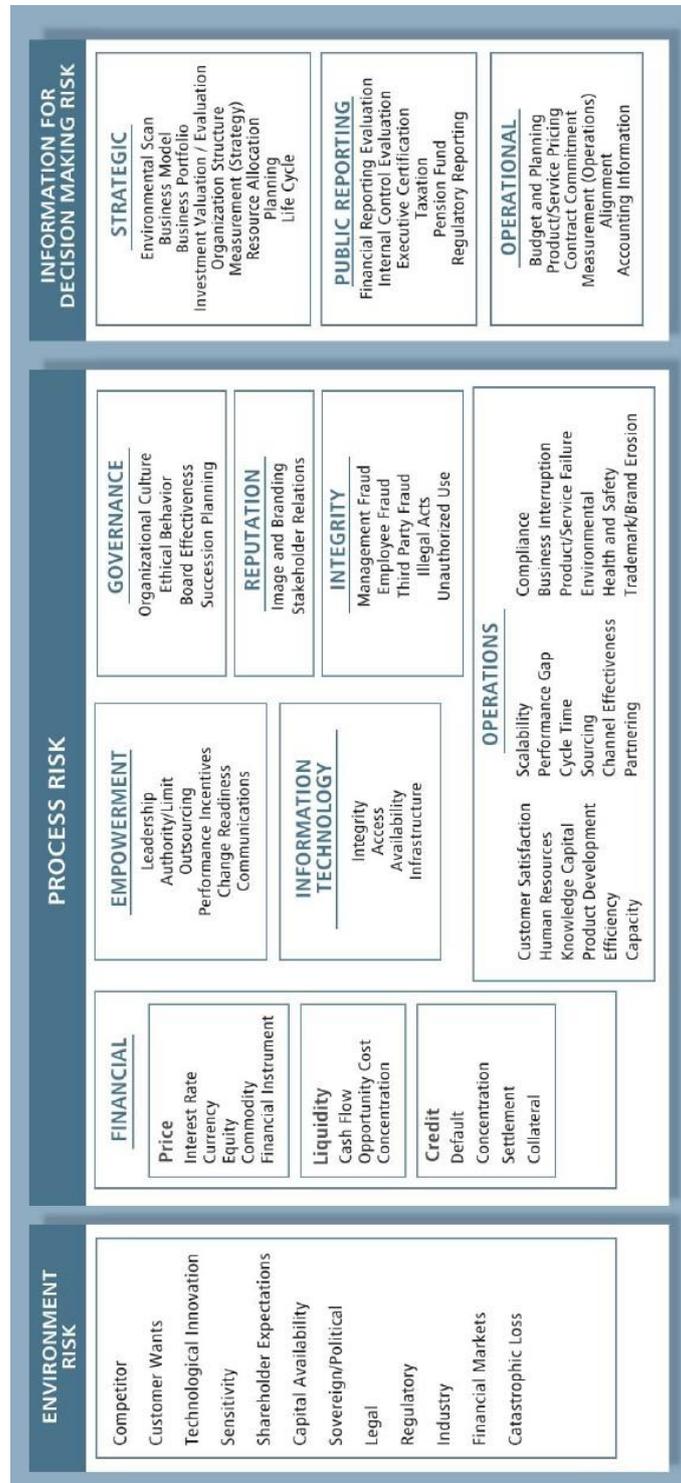


Figura 9: Taxonomia de riscos do Business Risk Model™ (DeLoach, 2000)

A descrição detalhada dos riscos pode ser encontrada em DeLoach (2000).

Anexo III – Definições de risco estratégico

“[...] Corporate strategic moves that cause returns to vary, that involve venturing into the unknown, and that may result in corporate ruin.” (Baird & Thomas, 1985)

“[...] The risk of not having a clear strategy; having a clear but nonviable strategy; having a clear, viable strategy but failing to implement it effectively; or having a clear, viable strategy that is derailed by an unforeseen circumstance.” (Glassman, 2000)

“[...] An unexpected event or set of conditions that significantly reduces the ability of managers to implement their intended business strategy.” (Simons, 2000)

“[...] Risks that arise in pursuit of business objectives”. São difusos, não específicos, ambíguos, não-probabilísticos e não mutuamente exclusivos, com potencial para constituírem tanto uma ameaça como uma oportunidade. Apesar de grande parte destes riscos ter origem no ambiente externo, as características e competências internas da organização determinam a forma como são geridos (Emblemsvåg & Kjølstad, 2002).

“[...] The array of external events and trends that can devastate a company's growth trajectory and shareholder value.” (Slywotzky & Drzik, 2005)

“Strategic risk consists of the most important risks that an organization faces, i.e. the possible future scenarios that would make a material difference (for better or worse) to its ability to achieve its main objectives or even to survive.” (Telford, 2005)

“Strategic risk is generally defined as being any risk (threat or opportunity) that materially affects the ability of an organization to survive.” (Allan & Beer, 2006)

“Strategic risk [...] may be defined as the risk associated with initial strategy selection, execution or modification over time, resulting in a lack of achievement of overall objectives.”

(Chapman, 2006)

“Strategic risk refers to the risk of significant investments for which there is a high uncertainty about success and profitability. If the venture is not successful, then the firm will usually suffer a major write-off, and its reputation among investors will be damaged.” (Crouhy *et al.*, 2006)

“Business risk refers to the classic risks of the world of business, such as uncertainty about the demand for products, the price that can be charged for those products, or the cost of producing and delivering products.” (Crouhy *et al.*, 2006)

“[...] Risks that threaten a firm’s long-term competitive success and survival: risks to its market position, critical resources, and ability to innovate and grow.” (Drew *et al.*, 2006)

“Strategic risks are [those that] have the greatest effects on a company’s market value, [and] the most difficult to quantify.” (Gates, 2006)

Muitos autores definem os riscos estratégicos através de exemplos: “Risks from damage to reputation, competition, demographic trends, technological innovation, capital availability and regulatory trends.” (SOA, 2006)

"[...] All external risks to the viability of the business arising from unexpected adverse changes in the business environment with respect to: the economy (business cycle); the political landscape; law and regulation; technology; social mores; and the actions of competitors." (Allen, 2007)

"[...] A risk that could cause severe financial loss or which could undermine the competitive position of a particular company [...]: macro threats emerging from the geopolitical and macroeconomic environment in which all businesses operate; sector threats which reshape specific industries; and operational threats that impact the performance of leading businesses in an industry". (Collier 2009)

"Strategic risks are those risks that are most consequential to the organization's ability to execute its strategies and achieve its business objectives. Strategic risk management is the process of identifying, assessing and managing the risk in the organization's business strategy – including taking swift action when risk is actually realized. Strategic risk management, then, is focused at the most consequential and significant risks to shareholder value – clearly an area deserving of the time and attention of executive management and the directors." (Frigo & Anderson, 2011)

"[...] The risk of making wrong business decisions, implementing decisions poorly, or being unable to adapt to changes in the operating environment. The existing and new potential for success in the Group and the segments in which it operates create strategic risks, which can lead to a significant long-term reduction in corporate value." (Munich Re Group, 2011)

"[...] Risks that can make or break a company." (Frigo & Laessoe, 2012)