POLITÉCNICO DO PORTO

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

Mestrado em Auditoria

O Processo de Gestão de Risco nas Organizações

Ana Jorge Neves de Barros

Dissertação apresentada ao Instituto Superior de Contabilidade e Administração do Porto para obtenção do Grau de Mestre em Auditoria

Orientada por Mestre Carlos Manuel Antunes Mendes

Porto, Novembro 2012

POLITÉCNICO DO PORTO

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

Mestrado em Auditoria

O Processo de Gestão de Risco nas Organizações

Ana Jorge Neves de Barros

Orientada por Mestre Carlos Manuel Antunes Mendes

Porto, Novembro 2012

Resumo

Palavras-chave: Riscos, Negócio, Supervisão e Regulação.

No final da década de 90 a crise económica e a desconfiança dos investidores que se instalou nos Estados Unidos na sequência dos escândalos financeiros que afectaram grandes empresas e consequentemente o mercado de capitais norte-americano, espalhando-se a todo o mundo, levou à aprovação de uma nova legislação que ficou conhecida por Lei *Sarbanes-Oxley* (SOX), com o objectivo de recuperar a credibilidade dos negócios.

Neste trabalho expõe-se a evolução que a Gestão de Riscos de Negócio teve desde então e as ferramentas que têm vindo a ser criadas para esse efeito e discute-se a relação entre a aprovação dessa Lei e o comportamento das organizações no pós-SOX, no que diz respeito à sua apetência para a Gestão de Riscos de Negócio a que ficam expostas, através da revisão de literatura sobre o assunto.

É parte integrante deste trabalho o inquérito realizado a várias organizações com o objectivo de apurar de que forma estão dispostas a preparar-se para monitorar os riscos de forma a criarem valor para os *stakeholders.* Contudo, a falta de respostas ao mesmo não permitiu concluir se estão abertas à utilização de mais esta ferramenta de gestão, ou se, pelo contrário, vão reagir com uma atitude hostil como o fizeram relativamente à Lei S*arbanes-Oxley,* classificando-a como mais uma forma de desviar recursos que poderiam estar ao serviço da criação de novos produtos para competir no mundo globalizado, o que na prática equivale a uma diminuição da apetência para a tomada de riscos por parte das organizações.

De todas as opiniões consultadas sobressai contudo a ideia de que as organizações têm hoje a consciência de que não podem passar sem melhor regulação, e melhorias do seu controlo interno que a auditoria interna tem uma palavra a dizer na gestão dos riscos de negócio.

Abstract

Keywords: Risk, Business, Supervision and Regulation.

In the late 90's economic crisis and distrust of investors who settled in the United States in the wake of financial scandals that have affected large companies and consequently the market for U.S. capital, spreading throughout the world, led to the approval of new legislation that became known as the Sarbanes-Oxley (SOX), with the aim of restoring the credibility of the business.

In this work we present the evolution of the Risk Management Business and since then had the tools that have been created for this purpose and discusses the relationship between the passage of this Act and the behavior of organizations in the post-SOX, the respect to its readiness for Risk Management Business which are exposed through the review of the literature on the subject.

It is an integral part of this work, the survey of various organizations in order to determine how they are willing to prepare to monitor risks in order to create value for stakeholders. However, the lack of responses to it not possible to conclude whether they are more open to using this management tool, or if, by contrast, will react with hostility as they did in relation to the Sarbanes-Oxley Act, classifying it as more a way of diverting resources that could be at the service of creating new products to compete in the globalize world, which in practice amounts to a decrease in appetite for risk taking by both organizations.

Of all the reviews but found the idea emerges that organizations today have an awareness that can not do without better regulation, and improvement of its internal control that internal audit has a say in the management of business risks.

À minha querida e doce Sara.

A tua partida inesperada deixou um vazio que aumenta a cada dia que passa!

Agradecimentos

Ao Dr. Rodrigo de Carvalho por todo o apoio numa altura muito difícil da minha vida.

Aos restantes professores do ISCAP por tudo o que me ensinaram, ao António Moreira pela ajuda, à Juju pelo incentivo, à minha querida mãe pela paciência.

Ao meu querido professor e orientador Mestre Carlos Mendes pelo que com ele aprendi ao longo destes anos e por toda a disponibilidade para chegar até aqui.

Lista de Abreviaturas e Siglas

- AAA - *Agricultural Adjustment Act*
- ABNT - Associação Brasileira de Normas Técnicas
- ABR - Auditoria Baseada em Riscos
- AI - Auditoria Interna
- ALCO - Assets and Liabilities Committee
- ASNZ - *Australia Standards New Zealand*
- BANIF – Banco Internacional do Funchal
- BCP – Banco Comercial Português
- BCSD Portugal - Conselho Empresarial para o Desenvolvimento Sustentável
- BES – Banco Espírito Santo
- BFA – Banco Fomento Angola
- BP- *British Petroleum*
- BPI – Banco Português de Investimento
- BPN - Banco Português de Negócios
- BPP - Banco Privado Português
- BSI - *British Standards Institution*
- CAE - *Certified Association Executive*
- CCC - *Civilian Conservation Corps*
- CEO - *Chief Executive Officer*
- CI - Controlo Interno
- CMF – Comissão para as Matérias Financeiras
- COBIT - *Control Objectives for Information and related Technology*
- COSO - *Committee of Sponsoring Organizations of the Treadway Commission*
- CSR Europe - *The Business Network for Corporate Social Responsibility*
- DRG - Departamento de Risco Global
- EDPR – EDP Renováveis

- EQUAL - Iniciativa Comunitária EQUAL
- ERM - *Enterprise Risk Management*
- ERP - *Enterprise Resource Planning*
- ERSE – Entidade Reguladora dos Serviços Energéticos
- EUA - Estados Unidos da América
- FDIC - *Federal Deposit Insurance Corporation*
- FDIS - *Final Draft International Standard*
- FED - *Federal Reserve System*
- FERA - *Federal Emergency Relief Administration*
- FERMA - *Federation of European Risk Management Associations*
- FLSA - *Federal Fair Labor Standards Act*
- FRC - *Financial Reporting Council*
- FTSE100 Index - índice de acções das 100 empresas mais altamente capitalizadas do Reino Unido na Bolsa de Londres (*London Stock Exchange*)
- GAI – Gabinete de Auditoria Interna
- GL - *Germanische Lloyd*
- GR – Gestão de Risco
- GRACE - Grupo de Reflexão e Apoio à Cidadania Empresarial
- GRI - *Global Reporting Initiative*
- GRN - Gestão de Riscos do Negócio
- I&D - Investigação e Desenvolvimento
- IAPMEI - Instituto de Apoio às Pequenas e Médias Empresas e à Inovação
- IBM - *International Business Machines*
- IIA - *The Institute of Internal Auditors*
- IPO - *Initial Public Offerings*
- IPPF - *International Professional Practices Framework*
- IPQ – Instituto Português de Qualidade
- ISMS - *IS Management System*
- ISO - Organização Internacional de Normalização
- ISO 26M - ISO 26000

- ISO/IEC - *International Organization for Standardization / International Electrotechnical Commission*
- KPI - *Key Performance Indicator*
- KRI - *Key Risk Indicator*
- NASDAQ - *National Association of Securities Dealers Automated Quotations*
- NIAHO[sm] - *The National Integrated Accreditation for Healthcare Organizations*
- NIRA - *National Industrial Recovery Act*
- NLRA - *National Labor Relations Act*
- NYSE - *New York Stock Exchange*
- OHSAS - *Occupational Health and Safety Assessment Services*
- ONA - Organização Nacional de Acreditação
- PCCL - Plano de Contingência de Capital e Liquidez
- PDCA - *Plan, Do, Check, Act*
- PME - Pequenas e Médias Empresas
- PSI20 – *Portuguese Stock Index* - 20
- PT Comunicações - Portugal Telecom
- PWA - *Public Works Administration*
- QSP - Centro de Qualidade, Segurança e Produtividade para o Brasil e América Latina.
- RPECS - Rede Portuguesa de Empresas para a Coesão Social
- RS – Responsabilidade Social
- RSE - Responsabilidade Social Empresarial
- RSE Portugal - Associação Portuguesa para a Responsabilidade Social das Empresas
- RU – Reino Unido
- S&P - *Standard & Poor's*
- S&P500 Index - *índice Standard & Poors* das 500 acções mais importantes do mercado
- SCIRF - Sistema de Controlo Interno do Relato Financeiro
- SEC - *Securities and Exchange Commission*
- SGSI - Sistema de Gestão de Segurança da Informação
- SI - Sistema de Informação

- SIS - *Swedish Standards Institute*
- SOX - Lei *SOX* ou Lei *Sarbanes-Oxley*
- SSI - *Software* e Sistemas de Informação
- TI - Tecnologias da Informação
- TIC - Tecnologias da Informação e da Comunicação
- TVA - *Tennessee Valley Authority*
- UE - União Europeia
- WBCSD - *World Business Council for Sustainable Development*
- WPA - *Works Progress Administration*

Índice geral

Índice de Figuras

Introdução

Este trabalho é realizado no âmbito do Mestrado de Auditoria e pretende responder à seguinte questão:

- Será a Gestão de Riscos de Negócio imprescindível para as Organizações criarem valor na actualidade?

Esta problemática foi escolhida por ser um tema muito actual no panorama pós escândalos financeiros e ser também muito importante para todas as organizações, dado que estamos num mundo globalizado, em que a uniformização tem sido a palavra-chave.

Com esse objectivo foi estruturado o trabalho que aqui se apresenta, dividido em seis capítulos, e realizado um inquérito a empresas portuguesas e brasileiras para daí retirar as devidas conclusões.

No **primeiro capítulo** é feita uma síntese introdutória a este trabalho dos principais acontecimentos históricos como o *Crash* de 1929 da Bolsa de Nova Iorque, e mais recentemente os escândalos financeiros, as bolhas informática e imobiliária e a Lei *Sarbanes-Oxley*, uma das últimas tentativas de obviar a estes problemas.

O **segundo capítulo** centra-se nos problemas que as organizações inseridas num mundo globalizado enfrentam na sua gestão diária, como sejam a necessidade de assumirem a sua Responsabilidade Social Empresarial, de respeitar o ambiente em que operam, o domínio das tecnologias da informação e de não serem por elas dominadas nomeadamente através da implementação de um sistema de segurança informática. Aborda-se também a evolução que o *COSO* tem sofrido no sentido de acompanhar as necessidades organizacionais, uma vez que a gestão não pode ser apenas o espelho da imposição do ponto de vista do gestor, mas tem de monitorar todo um conjunto de riscos, tirando daí vantagens adicionais para a organização e para o meio envolvente em que esta opera.

No **terceiro capítulo**, e na sequência de uma nova gestão tendo em conta os riscos, analisa-se um novo paradigma da auditoria, baseada em riscos, a implementação dos processos de gestão pró-activa de riscos, para introduzir a nova norma de Gestão de Risco de Negócio – a *ISO* 31000 e o seu *Guide* 73 de apoio aos seus termos e definições.

No **quarto capítulo** é feita a revisão de literatura sobre o tema, sendo apresentadas várias opiniões credenciadas de especialistas nestas matérias que falam sobre a aplicabilidade das ferramentas de gestão anteriormente analisadas e de como as organizações estão mais alerta para a Gestão de Risco e com maior ou menor apetência para a tomada de riscos.

O **quinto capítulo** trata a metodologia pensada para dar resposta à pergunta colocada e que consistiu num inquérito, apresentado no anexo II, realizado às empresas do *PSI*20 da EuroNext Lisboa em Portugal e às organizações ligadas ao QSP do Brasil sobre a apetência para a implementação da norma *ISO* 31000, mas que não possibilitou tirar conclusões por falta de respostas conclusivas sobre o tema.
Em alternativa a esta metodologia são apresentados três estudos (anexos III, IV e V) que, com o apoio do que foi pesquisado na revisão da literatura, irão permitir tirar algumas conclusões que darão a resposta à questão inicialmente colocada.

Finalmente o **sexto capítulo** apresenta como análise empírica um quadro resumo dos riscos tratados pelas empresas do *PSI*20. Começa por apresentar as diversas empresas que actualmente constituem este índice para um melhor conhecimento da actividade de cada uma. Seguidamente são feitas considerações sobre o tipo de riscos tratados por esta amostra bastante significativa de organizações portuguesas e que permitirá reforçar as conclusões anteriormente obtidas.

Toda esta pesquisa e análise permitiu chegar à conclusão de que, embora a gestão de riscos esteja presente nas organizações como uma ferramenta a ter em conta, as organizações ainda se mostram pouco predispostas a torná-la como algo fundamental no seu dia-a-dia, preferindo dar mais importância a outros factores que possam criar valor directamente, ao invés de a interiorizar como uma boa prática de gestão, que para além de as ajudar a prevenir os riscos representam também uma forma de criar valor para a organização.

1. Enquadramento Histórico

Neste primeiro capítulo é feita uma síntese introdutória a este trabalho dos principais acontecimentos históricos como o *Crash* de 1929 da Bolsa de Nova Iorque, os escândalos financeiros, as bolhas informática e imobiliária e a Lei *Sarbanes-Oxley*, uma tentativa recente de travar todos estes problemas.

1.1 O *Crash* de 1929 da Bolsa de Nova Iorque

Um *crash*[1] é geralmente provocado por pânico, associado a factores económicos subjacentes, e ocorre após uma "bolha" especulativa no mercado, quando grandes volumes de acções são negociados a preços consideravelmente desnivelados do seu valor intrínseco[2], sendo muito receado pelos investidores e pelas autoridades monetárias[3].

Com o término da Primeira Guerra Mundial, os EUA passaram a ser o grande nome do capitalismo mundial[4], mas a partir de 1925 começam a enfrentar graves problemas[5] como o aumento do desemprego, as grandes quantidades de produtos que não se escoavam e a crise da Bolsa de Nova Iorque. Como resultado da deflação[6] entretanto registada, milhares de empresas foram à falência.

Em 1933 o democrata *Franklin D. Roosevelt* foi eleito presidente dos EUA e elaborou um programa nacional de medidas reformistas para solucionar a crise e relançar a economia[7] que ficou conhecido por New *Deal*[8], baseando nas teorias do economista inglês *John Keynes.*

Com o *Emergency Banking Act*[9] restabeleceu-se a confiança nas instituições bancárias, tendo sido constituído o *FDIC*[10] e a *SEC* para regulamentar o mercado bolsista.

[1] http://pt.wikipedia.org/wiki/Crash_da_bolsa, consultado em 10.Nov.2009.
[2] http://pt.wikipedia.org/wiki/Crash_da_bolsa, consultado em 10.Nov.2009.
[3] http://www.clubeinvest.com/_technical_analysis/forex/1987crash_bolsa1929/1987crash_bolsa1929.php, consultado em 12 Nov.2009.
[4] http://www.brasilescola.com/historiag/crise29.htm, consultado em 10.Nov.2009.
[5] http://dandelife.com/story/25779, consultado em 15.Nov.2009.
[6] http://pt.wikipedia.org/wiki/Defla%C3%A7%C3%A3o_(economia), consultado em 4.Nov.2009.
[7] http://www.infopedia.pt/$new-deal, consultado em 10.Nov.2009.
[8] http://www.brasiles, consultado em 4.Nov.2009.
[9] Traduzido de http://wiki.answers.com/Q/Why_was_the_Emergency_Banking_Act_during_FDR's_presidency_the_first_legislation_passed_by_Roosevelt_and_Congress, consultado em 16.Dez.2009.
[10] Traduzido de http://www.answers.com/topic/federal-deposit-insurance-corporation, consultado em 17.Dez.2009.

A *FERA*[11] alargou as ajudas aos necessitados dos vários estados, em conjunto com o *CCC*[12], e foi criado o *TVA*[13] para desenvolver o rio Tennessee, bem como o *AAA*[14], o *NIRA*[15], o *PWA*[16] e um programa para regular os negócios e assegurar uma saudável concorrência.

Em 1935 é preparado um segundo *New Deal*, tendo sido lançado o *NLRA*, programa que seria continuado em 1938 pelo *FLSA*[17] e um novo programa, o *WPA*[18]. Na mesma data o Governo patrocinou o *Social Security Act*[19].

Este período de 1929 a 1933 deixou uma lição: a de que os mercados vivem crises periódicas e se não se dão respostas rápidas para os problemas, essas crises tendem a alastrar, afectando vários sectores da economia e podendo alcançar um poder de destruição em massa[20].

Mais recentemente, o *crash* de 1987 não teve consequências económicas assinaláveis, devido à rápida intervenção da Reserva Federal que disponibilizou liquidez ao mercado para acalmar os ânimos e não permitir que houvesse instituições financeiras em perigo de falência[21]. Foi a maior queda da história registada num só dia! O medo estendeu-se aos mercados de todo o mundo[22].

1.2 Os Escândalos Financeiros

"*Vivemos num mundo novo, mas não existe nem uma nova ordem mundial, nem uma nova desordem mundial. Em seu lugar, existe uma zona de segurança na Europa, e fora dela, uma zona de perigo e de caos*[23]".

É aqui que temos de reagir, nesta "*nova ordem europeia: nova no sentido em que historicamente não tem precedentes e também assenta em conceitos novos*[24]".

[11] Traduzido de http://www.novelguide.com/a/discover/egd_01/egd_01_00189.html, consultado em 17.Dez.2009.
[12] Traduzido de http://en.wikipedia.org/wiki/Civilian_Conservation_Corp, consultado em 17.Dez.2009.
[13] Traduzido de http://en.wikipedia.org/wiki/Tennessee_Valley_Authority, consultado em 17.Dez.2009.
[14] Traduzido de http://www.spartacus.schoolnet.co.uk/USARagriculture.htm, consultado em 16.Dez.2009.
[15] Traduzido de http://www.ourdocuments.gov/doc.php?flash=old&doc=66, consultado em 17.Dez.2009.
[16] Traduzido de http://en.wikipedia.org/wiki/Public_Works_Administration, consultado em 16.Dez.2009.
[17] Traduzido de http://careerplanning.aboutcom/cs/legalissues/a/fair_labor.htm, consultado em 16.Dez.2009.
[18] Traduzido de http://www.indiana.edu/~liblilly/wpa/wpa_info.html, consultado em 17.Dez.2009.
[19]Traduzido de http://en.wikipedia.org/wiki/Social_Security_(United_States)#Creation:_The_Social_Security_Act, consultado em 16.Dez.2009.
[20] http://vestibular.uol.com.br/ultnot/resumos/crise-economica-1929.jhtm, consultado em 4.Nov.2009.
[21] http://www.clubeinvest.com/_technical_analysis/forex/1987crash_bolsa1929/1987crash_bolsa1929.php, consultado em 12.Nov.2009.
[22] http://pt.euronews.net/2007/10/19/crash-de-1987-faz-20-anos/, consultado em 11.Nov.2009.
[23] Cooper, Robert, Ordem e Caos no século XXI, Editorial Presença, Fevereiro 2006, página 67.
[24] Cooper, Robert, Ordem e Caos no século XXI, Editorial Presença, Fevereiro 2006, página 86.

"*A ordem europeia pós-moderna enfrenta os mesmos perigos que os EUA*[25]*", porém a tentativa será fazer funcionar o sistema em que todos cooperam sem a ambição do controlo pois as "velhas soluções para os problemas da ordem internacional – equilíbrio e hegemonia – não parecem interessantes*[26]".

A 11 de Setembro de 2001 o mundo assiste à destruição das chamadas torres gémeas dos EUA no *World Trade Center* e logo de seguida à maior fraude corporativa protagonizada pela *Enron*, cujo escândalo financeiro culminou com milhares de pessoas desempregadas e arrastou consigo uma das *Big Five* da auditoria mundial[27].

Seguiram-se outras grandes empresas como a *WorldCom, Xerox, Tyco, Global Crossing, Qwest, Merck e Bristol-Myers, ImClone* e *Adelphia*, etc., que abalaram a confiança nos mercados e trouxeram a necessidade de se começar a pensar numa mais forte regulação dos mesmos.

Verificou-se que as suas demonstrações financeiras que até então eram o espelho de modelos de gestão bem sucedidos em revistas da especialidade, afinal tinham sido manipuladas. As fraudes levaram o índice *Dow Jones*[28] a patamares de 1997[29].

***Enron* – 2 de Dezembro de 2001 -** Estabelecida em *Houston* no *Texas*, chegou a ser a sétima maior companhia dos EUA e uma das maiores do mundo na distribuição de energia, gás natural e comunicações, antes de falir[30].

A empresa era uma das maiores beneficiárias dos subsídios do *Export-Import Bank*[31], que subsidiava a descoberto certas empresas americanas em troca de favores políticos[32].

***Global Crossing* – 28 de Janeiro de 2002 -** A companhia de redes de fibras ópticas

[25] Cooper, Robert, Ordem e Caos no século XXI, Editorial Presença, Fevereiro 2006, página 90.
[26] Cooper, Robert, Ordem e Caos no século XXI, Editorial Presença, Fevereiro 2006, página 93.
[27] http://www.vidabrasil.com.br/exibe_noticias.asp?cod_noticia=515&edicao=316&data=15/10/2002, consultado em 14.Nov.2009.
[28] http://www.constelar.com.br/revista/edicao23/bolsany1.htm, consultado em 10.Nov.2009.
[29] http://revistaepoca.globo.com/Epoca/0,6993,EPT341656-1662,00.html, consultado em 14.Nov.2009.
[30] http://www.scribd.com/doc/6841023/O-caso-Enron, consultado em 4.Nov.2009.
[31] Traduzido de http://en.wikipedia.org/wiki/Export-Import_Bank_of_the_United_States, consultado em 16.Dez.2009.
[32] http://www.google.pt/imgres?imgurl=http://www.mises.org.br/images/articles/enron.jpg&imgrefurl=http://http://www.google.pt/imgres?imgurl=http://www.mises.org.br/images/articles/enron.jpg&imgrefurl=http://www.mises.org.br/Article.aspx%3Fid%3D28&h=311&w=401&sz=27&tbnid=F3dpJHCWP2cwoM:&tbnh=96&tbnw=124&prev=/images%3Fq%3Denron&hl=pt-PT&usg=__aGeWsijWV6i0v1L5CNdsc35Ve-I=&ei=mLcfS7i-Et_OjAeqpsmmCw&sa=X&oi=image_result&resnum=4&ct=image&ved=0CBkQ9QEwAw, consultado em 14.Nov.2009.

de telecomunicações teve de entrar com um pedido de falência. O governo americano suspeita que as suas receitas foram inflacionadas por contratos de longo prazo fictícios[33].

 ***Xerox* – 1º de Abril de 2002 -** A fabricante de materiais para escritório *Xerox Corporation* admitiu ter sobrestimado os seus lucros nos últimos cinco anos[34].

A empresa foi multada e hoje ainda se mantém como uma das maiores empresas de fotocopiadoras, tendo recuperado do escândalo.

 ***Tyco* Internacional – 4 de Junho de 2002 -** Outra gigante norte americana, um conglomerado industrial com negócios nas áreas de saúde, electrónica e segurança, com sede nas ilhas Bermudas[35].

A *Tyco* concordou pagar uma multa para encerrar o caso que vinha a ser investigado pela *SEC*[36], mas nunca se chegaram a conhecer publicamente as fraudes. A *Tyco* informou que estabeleceu um fundo de 2,975 biliões de dólares para compensar os seus investidores[37].

 ***WorldCom* – 26 de Junho de 2002 -** A segunda maior empresa de serviços de telecomunicações de longa distância norte-americana registou como investimentos montantes que na verdade eram despesas, transformou em lucro prejuízos, durante cinco trimestres[38].

 ***Merck* – 8 de Julho de 2002 -** Depois de auditar as contas do terceiro maior fabricante de medicamentos do mundo, o governo americano revelou que haviam sido escrituradas como receitas US$ 14 bilhões, contabilizadas pela empresa desde 1999, que na realidade nunca existiram[39], pois tratava-se de valores provenientes da concessão de descontos na compra de medicamentos através da subsidiária *Medco*, que geria os planos de saúde desta empresa.

[33] http://www.terra.com.br/istoedinheiro/253/negocios/253_herois_capitalismo.htm, consultado em 14.Nov.2009.
[34] http://www.bbc.co.uk/portuguese/economia/020628_xeroxcg.shtml, consultado em 14.Nov.2009.
[35] http://www.miradaglobal.com/index.php?option=com_content&view=article&id=80:la-crisis-moral-del-capitalismo&catid=28:economia&Itemid=32&lang=pt, consultado em 14.Nov.2009.
[36] http://www.engenhariadigital.com.br/engenhariadigital/noticias.asp?arquivo=dinheiro/ult91u108013.shtml, consultado em 14.Nov.2009.
[37] http://g1.globo.com/Noticias/Economia_Negocios/0,,AA1540117-9356,00.html, consultado em 14.Nov.2009.
[38] http://revistaepoca.globo.com/Epoca/0,6993,EPT344659-1663-1,00.html, consultado em 14.Nov.2009.
[39] http://www.jacoby.pro.br/fraudes.doc, consultado em 14.Nov.2009.

Na Europa, há casos como a da cadeia de supermercados *Ahold*, que manipulou as contas de sua filial argentina *Disco* e da americana *US Foodservice* e as contas secretas do *Banco Bilbao Vizcaya* em paraísos fiscais[40].

A *Parmalat* foi acusada de fraude pela *SEC*, que afirmou que a empresa italiana enganou investidores ao vender-lhes títulos de dívida para captar dinheiro enquanto disfarçava a sua verdadeira situação financeira[41].

Para evitar este tipo de comportamentos e recuperar a confiança dos accionistas, o governo dos EUA decidiu mais uma vez intervir.

1.3 A Era pós Lei *Sarbanes-Oxley*

Em 30 Julho de 2002 é assinada a conhecida Lei *SOX* ou Lei *Sarbanes-Oxley*, considerada a maior reforma do mercado de capitais após a crise financeira de 1929[42], pelo senador *Paul Sarbanes* (Democrata de *Maryland*) e pelo deputado *Michael Oxley* (Republicano de *Ohio*). Esta lei, de aplicação a todas as empresas americanas ou estrangeiras que tivessem acções cotadas na NYSE e NASDAQ, pretendia evitar a ocorrência de fraudes, como as que haviam acontecido recentemente, criar meios de as identificar caso ocorressem, tornando deste modo os negócios muito mais seguros e a gestão mais transparente.

Quando o papel do auditor e do consultor se misturam podemos estar perante um problema muito grave, o que já aconteceu. O consultor vai tentar aconselhar a contornar a lei e muitas vezes a própria ética empresarial, para agradar e ajudar a obter resultados muito satisfatórios, a fronteira entre uma e outra tende a desaparecer e foi isso mesmo que se verificou na gigante norte-americana *Enron*[43].

Os principais benefícios da *SOX* para as empresas[44] são permitir a viabilização dos controlos internos e a avaliação de fluxo de informação, o mapeamento de processos críticos das empresas, a gestão de riscos de negócio (adiante designada por GRN) associados a estes processos, a alocação de responsabilidades aos responsáveis internos, a identificação de não conformidades e rapidez na gestão de GRN.

[40] http://www.wharton.universia.net/index.cfm?fa=viewfeature&id=1118&language=portuguese, consultado em 14.Nov.2009.
[41] http://www.bbc.co.uk/portuguese/economia/story/2003/12/031230_parmalatml.shtml, consultado em 4.Nov.2009.
[42] http://www.fraudes.org/showpage1, consultado em 22.Nov.2009.
[43] http://www.webartigos.com/articles/24670/1/o-caso-enron/pagina1.html, consultado em 14.Dez.2009.
[44] http://www.softexpert.com.br/norma-sox.php, consultado em 14.Dez.2009.

O objectivo desta lei visou fundamentalmente criar um novo ambiente de controlo no governo das sociedades, apoiado por um conjunto de novas responsabilidades e sanções aos administradores para coibir as práticas lesivas que expõem as sociedades de capital aberto a elevados níveis de risco e que fazem com que os *stakeholders* se retraiam em participar no capital dessas empresas.

1.4 As novas crises – Bolha Informática e Bolha Imobiliária

A publicação da referida Lei *SOX* assinada em 30 de Julho de 2002 pareceu acalmar os mercados e tudo aparentemente começava a caminhar para a normalidade quando em 2008 rebenta a crise do *subprime* que arrasta para uma nova crise mundial, e que já tinha sido revelada ao público a partir de Fevereiro de 2007, como uma crise financeira.

No final dos anos 90, a internet ganhou reconhecimento a nível mundial como um novo meio de comunicação muito eficiente e que traria enormes vantagens competitivas às organizações, nomeadamente com a criação de *websites* que as iria posicionar como muito modernas no novo milénio, para o *e-commerce*[45]com lucros nunca antes conseguidos.

Foi até criada a *NASDAQ*, uma nova bolsa de valores para os negócios da electrónica, operando exclusivamente para empresas da área da alta tecnologia em electrónica, informática, telecomunicações, biotecnologia, etc.[46].

Nascia assim a questão da **bolha informática** ou tecnológica do ano 2000, quando as empresas que actuavam na internet chamadas ".*com*" e que estavam muito sobrevalorizadas, viram as suas acções caírem vertiginosamente, provocando falências nalguns casos ou reduções drásticas do seu valor noutros casos, quando foram reavaliadas. Apesar disso, a internet ficou instalada de vez nas relações entre empresas, pela facilidade de comunicação num mundo globalizado[47].

[45] http://pt.wikipedia.org/wiki/Com%C3%A9rcio_eletr%C3%B4nico, consultado em 16.Dez.2009.
[46] http://pt.wikipedia.org/wiki/NASDAQ, consultado em 29.Nov.2009.
[47] http://www.brasilescola.com/informatica/bolha-dos-anos-2000.htm, consultado em 18.Nov.2009.

A **bolha imobiliária** americana (2005) surge em analogia com a anterior e pela mesma razão, ou seja, pelo facto dos preços dos imóveis nos EUA estarem muito inflacionados, não correspondendo ao seu valor real[48] criando uma situação insustentável.

Os problemas começam em 2006, quando o presidente do *FED*, *Ben Bernanke*, falou da existência de um risco inflacionário no país, em função do excesso de dinheiro no mercado, o que viria a provocar o aumento das taxas de juro.

Assim, a classe média começou a preferir aplicar o seu dinheiro em títulos do governo, o que provocou a descida do preço dos imóveis, face à diminuição da procura[49].

Anunciada em 2005 acabou por rebentar em 2006 a crise do *subprime* e a insolvência de várias instituições de crédito dos EUA, que concediam empréstimos hipotecários de alto risco, que em inglês se designam por *subprime loan* ou *subprime mortgage*, com repercussões nas bolsas de valores de todo o mundo. Os *subprimes* incluíam empréstimos hipotecários, cartões de crédito e aluguer de carros, e eram concedidos, nos EUA, a clientes sem rendimentos e com um histórico de crédito muito mau a que se convencionou chamar os *ninja's* (*no income, no job, no assets*: sem rendimentos, sem emprego, sem património)[50].

Como foi possível chegar a esse estado de coisas, já que esses títulos obtiveram o aval das agências internacionais de classificação de risco - de renome até então inquestionável -, que lhes deram a sua chancela máxima - AAA - normalmente dada a títulos tão sólidos quanto os do Tesouro dos EUA[51]?

A partir de 18 de Julho de 2007, a crise do crédito hipotecário provocou uma crise de confiança geral no sistema financeiro e falta de liquidez bancária e mesmo os bancos que não trabalhavam com os chamados activos tóxicos foram atingidos.

Foi o que aconteceu por exemplo com o banco britânico *Northern Rock*, que não tendo hipotecas "lixo" adoptava uma estratégia arriscada ao receber dinheiro emprestado a curto prazo das instituições financeiras, para emprestá-lo a longo prazo aos compradores de imóveis.

[48] http://pt.shvoong.com/exact-sciences/1740108-entendendo-bolha-imobili%C3%A1ria-americana/, consultado em 22.Nov.2009.
[49] http://pt.shvoong.com/exact-sciences/1740108-entendendo-bolha-imobili%C3%A1ria-americana/, consultado em 22.Nov.2009.
[50].http://pt.wikipedia.org/wiki/Crise_do_subprime, consultado em 3.Nov.2009.
[51] http://pt.wikipedia.org/wiki/Crise_do_subprime, consultado em 3.Nov.2009.

Repentinamente as instituições financeiras deixaram de emprestar dinheiro, o que fez com que se tornasse o primeiro banco britânico a sofrer intervenção governamental, desde 1860[52].

No nosso país os recentes escândalos do BPP e BPN foram o culminar de toda a crise económica e social que já se vivia no resto do mundo, embora por razões diversas.

[52] http://pt.wikipedia.org/wiki/Crise_do_subprime#cite_note-3, consultado em 14.Nov.2009.

2. A Necessidade da Gestão de Riscos de Negócio

Este segundo capítulo centra-se nos problemas que as organizações inseridas num mundo globalizado enfrentam na sua gestão corrente, como sejam, a necessidade de assumirem a sua responsabilidade social empresarial, de agora em diante designada por RSE, de respeitar o ambiente em que operam, a questão de dominarem as tecnologias da informação e de não serem por elas dominadas, nomeadamente através da implementação de um sistema de segurança informática. Fala-se também de toda a evolução que o *COSO* tem sofrido no sentido de acompanhar as necessidades organizacionais em matéria do seu controlo interno, a partir de agora designado por CI, pois a gestão tem de monitorar todo um conjunto de riscos, tirando daí vantagens adicionais para a organização e o meio envolvente onde esta opera.

2.1 A Responsabilidade Social Empresarial

No Livro Verde da Comissão Europeia publicado em Julho de 2001 sobre RSE, pode ler-se que é *"um conceito, segundo o qual, as empresas decidem, numa base voluntária, contribuir para uma sociedade mais justa e para um ambiente mais limpo"*[53].

A adopção dum conceito de RSE veio contribuir para atingir o objectivo definido pelo Conselho Europeu de Lisboa de tornar a UE *"a economia baseada no conhecimento mais dinâmica e competitiva do mundo, capaz de garantir um crescimento económico sustentável, com mais e melhores empregos, e com maior coesão social"*, como pode ler-se no site Europa de sínteses da legislação europeia[54].

Por RSE entende-se a integração voluntária das preocupações sociais e ambientais nas operações quotidianas das organizações através da interacção de todas as partes interessadas - trabalhadores, comunidades locais, clientes, fornecedores, autoridades públicas, concorrentes e a sociedade em geral, com o propósito de garantir uma maior competitividade, o que representa um corte com o anterior conceito de gestão que se reduzia ao exclusivo cumprimento de interesses dos proprietários.

[53] http://eur-lex.europa.eu/LexUriServ/site/pt/com/2001/com2001_0366pt01.pdf/, consultado em 6.Jan.2010.

[54] http://europa.eu/legislation_summaries/employment_and_social_policy/employment_rights_and_work_organisation/n26034_pt.htm , consultado em 19.Ago.2010.

"*A organização socialmente responsável tem em consideração a comunidade em que se insere e o ambiente em que opera antes de tomar as suas decisões. Cada vez mais as organizações, como motor de desenvolvimento económico, tecnológico e humano, só se realizam plenamente quando consideram na sua actividade o respeito pelos direitos humanos, o investimento na valorização pessoal, a protecção do ambiente, o combate à corrupção, o cumprimento das normas sociais e o respeito pelos valores e princípios éticos da sociedade em que se inserem*[55]".

A globalização e a transformação industrial dos últimos tempos trouxeram preocupações acrescidas às organizações, os consumidores tornaram-se mais exigentes social e ecologicamente e o impacto dos danos causados ao ambiente (p.e., fugas radioactivas e marés negras) fizeram surgir a necessidade da existência de legislação específica e entidades reguladoras/fiscalizadoras, para as quais as modernas TIC muito têm contribuído.

No site do IAPMEI[56] pode ler-se sobre o significado prático da RSE do projecto SER PME Responsável, enquadrado no âmbito da Iniciativa Comunitária EQUAL, que visou promover a adopção e valorização dessas práticas de gestão.

É neste contexto de procura de uma conduta social, ética e ambientalmente responsável e de respeito ao próximo que têm surgido as associações de RSE.

A *IBM* é pioneira na associação a diversas organizações que desenvolvem projectos neste âmbito, desde acções de sensibilização para a prática da RSE, à contribuição ao desenvolvimento de manuais informativos e formativos sobre o tema, divulgação de boas práticas individuais e associativas, acções de voluntariado, etc., para uma maior consciencialização sobre as vantagens desta prática.

A *IBM* é actualmente membro da

grace Grupo de Reflexão e Apoio à Cidadania Empresarial A associação GRACE foi formada em Fevereiro de 2000 por um conjunto de empresas, maioritariamente multinacionais, tendo sido a primeira associação portuguesa sem fins lucrativos dedicada à problemática da RSE. O seu principal objectivo é fomentar a

[55] http://www.portaldaempresa.pt/CVE/pt/Gestao/ResponsabilidadeSocial/, consultado em 6.Jan.2010.
[56] http://www.iapmei.pt/iapmei-art-03.php?id=1860/, consultado em 19.Ago.2010.

participação das empresas no contexto social em que se inserem, procurando disseminar práticas de gestão empresarial socialmente responsáveis.

Criado em 2001, por iniciativa da PT Comunicações, o Projecto Mão-na-Mão foi na altura uma iniciativa pioneira em Portugal, ao reunir pela primeira vez sob um projecto de características empresariais, diferentes entidades apostadas em concretizar o objectivo comum de levar solidariedade e apoio a segmentos mais desfavorecidos da população.

A RSE Portugal, como membro nacional da CRS *Europe, The Business Network* for *Corporate Social Responsibility*, instituição apoiada pela D.G. para o Emprego e Assuntos Sociais da Comissão Europeia, veio ampliar a acção da RPECS. A Associação tem como objectivo social a concepção, a execução e o apoio a programas e projectos nas áreas do emprego e formação profissional, e de cariz educacional, social, cultural, científico, ambiental, cívico e económico, fundamentalmente nos âmbitos da cooperação para o desenvolvimento, da protecção e promoção dos direitos humanos e da coesão social.

O BCSD Portugal é uma associação sem fins lucrativos, criada em Outubro de 2001 pela iniciativa das empresas Sonae, Cimpor e Soporcel, associadas ao WBCSD. A sua missão principal é fazer com que a liderança empresarial seja catalisadora de uma mudança rumo ao Desenvolvimento Sustentável e promover nas empresas a eco-eficiência, a inovação e a responsabilidade social[57].

Este relacionamento ético e transparente da organização com todas as partes interessadas, visando o desenvolvimento sustentável da sociedade e preservando recursos ambientais e culturais para gerações futuras, respeita a diversidade e promove a redução das desigualdades sociais.

A RSE torna-se assim uma forma de gestão estratégica, não por força da obrigatoriedade legal ou do marketing social, mas mais como um comprometimento permanente da organização, em adoptar comportamentos éticos que contribuam para o desenvolvimento global da sociedade, de forma responsável e sustentável.

[57] http://www-05.ibm.com/pt/ibm/ccr/ars.html, consultado em 17.Ago.2010.

2.2 A Nova *ISO* 26000 e a Questão Ambiental

As questões ambientais cada vez mais não passam despercebidas e todas as organizações têm procurado mostrar nos seus relatórios alguma preocupação sobre o tema.

O desastre ecológico que recentemente ocorreu na plataforma *Deepwater Horizon* do Golfo do México e propriedade da BP, apesar de já controlado, vai continuar a ter efeitos económicos globais durante muito tempo o que irá fazer os prémios de seguro da exploração do petróleo *offshore* subir exponencialmente, podendo chegar a 50%, sendo que as apólices verão reduzido o seu tempo de duração com a exigência acrescida de planos adequados de prevenção de acidentes que vão ser exigidos na contratação de apólices ambientais[58].

A questão ambiental é um dos temas centrais da ***ISO* 26000**, sendo a responsabilidade ambiental um pré-requisito para a sobrevivência e prosperidade dos seres humanos, mas não será mais uma certificação[59]!

"A ISO 26M foi construída com um formato aberto e provocador e não será certificável - apenas trará orientações para todas as organizações sobre como devem assumir responsabilidades sobre os impactos de suas actividades que incluem produtos, serviços e processos e os seus relacionamentos ou actividades da organização dentro da sua esfera de influência. Encontra-se na versão quase definitiva - FDIS e será publicada em finais de 2010 a sua versão final[60]".

"Tem carácter multistakeholder, o que é inovador na ISO, pois foram convidadas a participar diversas categorias de stakeholders – consumidores, empresas, governos, trabalhadores e outros e para além disso, também pela primeira vez, a liderança de um processo desta natureza é compartilhada entre um país em desenvolvimento (Brasil) através da ABNT, e um país desenvolvido (Suécia) pela SIS[61]".

Segundo *Cajazeiras*, Jorge presidente do Grupo de Trabalho de RSE da *ISO* 26M do Brasil, numa entrevista dada em 2007 ao Instituto *Ethos*, trata-se de uma norma de directrizes e não certificadora pois *"a certificação é susceptível de ser manipulável. É uma relação entre clientes e fornecedores. Essa é uma discussão complexa, pois como você pode certificar a*

[58] http://www.iso31000qsp.org/, consultado em 17.Ago.2010.
[59] http://construcoesverdes.blogspot.com/2010/03/norma-iso-26000-e-aprovada-para.html,consultado em 17.Ago.2010.
[60] http://www.qsp.org.br/GI_26000.shtml, consultado em 17.Ago.2010.
[61] http://uniethos.tempsite.ws/iso26000/iso-26000-o-que-e/a-norma-iso-26000/, consultado em 18.Ago.2010.

responsabilidade social de uma empresa, sendo que nenhuma empresa é totalmente responsável[62]*"*?

A *ISO* 26M define RSE como: *"**A responsabilidade de uma organização pelos impactos de suas decisões e actividades na sociedade e no meio ambiente, por meio de um comportamento ético e transparente, que**:*

- ✓ *Contribua para o desenvolvimento sustentável, incluindo a saúde e bem-estar da sociedade;*
- ✓ *Leve em consideração as expectativas dos stakeholders;*
- ✓ *Esteja em conformidade com a legislação aplicável e seja consistente com normas internacionais de comportamento;*
- ✓ *Esteja integrada em toda a organização e praticada por todos."*

"Todos os interessados numa sociedade mais justa encontram dificuldade em termos e conceitos como - responsabilidade social, RSE, responsabilidade sócio-ambiental, responsabilidade corporativa, sustentabilidade, desenvolvimento sustentável, etc., que esta norma tentará tornar uniformes. A norma 26M recomenda também que as organizações respeitem e promovam os seguintes princípios ambientais:

- ✓ ***Responsabilidade ambiental** - além da obediência a leis e regulamentos, uma organização deveria assumir a responsabilidade pelo impacto ambiental causado pelas suas actividades, produtos e serviços em áreas rurais ou urbanas e no meio ambiente como um todo.*
- ✓ ***Abordagem preventiva** - originária da Declaração do Rio sobre Meio Ambiente e Desenvolvimento e subsequentes declarações e acordos, segundo as quais, onde há ameaças de danos graves ou irreversíveis ao meio ambiente ou à saúde humana, falta de total certeza científica ou falta de certeza total quanto à gravidade da ameaça ao meio ambiente, a falta de total certeza científica não deveria ser usada como motivo para adiar medidas com boa relação custo-benefício para evitar a degradação ambiental ou os danos à saúde humana.*
- ✓ ***Gestão de riscos ambientais** - a ISO 26M recomenda que as organizações implementem programas usando uma abordagem baseada em riscos e em*

[62] http://uniethos.tempsite.ws/iso26000/iso-26000-o-que-e/a-norma-iso-26000/, consultado em 18.Ago.2010.

sustentabilidade, para avaliar, evitar, reduzir riscos e impactos ambientais gerados pelas suas actividades, produtos e serviços.

- ✓ ***O poluidor paga*** *- as organizações que arquem com os custos da poluição causada pelas suas actividades, produtos e serviços, de acordo com a extensão do impacto ambiental para a sociedade e com a acção correctiva exigida, ou na medida em que a poluição ultrapasse um nível considerado aceitável*[63]*".*

"A intenção é que a ISO 26M se torne um documento-guia de RS, orientador das organizações em diferentes culturas, sociedades e contextos e estimulador da melhoria de desempenho e resultados, tendo em atenção os seguintes pontos:

- ✓ ***Foco no ciclo de vida*** *- para reduzir os impactos ambientais de produtos e serviços e aumentar o seu desempenho socioeconómico;*
- ✓ ***A avaliação dos impactos ambientais*** *- para ser realizada antes da organização iniciar uma nova actividade ou projecto, e para que os resultados dessa avaliação sejam utilizados no processo decisório;*
- ✓ ***Produção mais limpa e eco-eficiência*** *- para o uso mais eficiente de recursos e menor geração de poluição e resíduos;*
- ✓ ***Abordagem de sistema de produto-serviço*** *- para a mudança de foco - de um mercado de venda de produtos para um sistema de produtos e serviços que satisfaçam as necessidades do consumidor, reduzam o uso de materiais e envolvam os stakeholders na promoção de uma maior responsabilidade do fabricante ao longo do ciclo de vida do produto;*
- ✓ ***Uso de tecnologias e práticas ambientalmente sólidas*** *para a adopção e divulgação de tecnologias e serviços ambientalmente seguros*[64]*".*

Fundamentalmente trata-se de uma norma que recomenda às organizações avaliarem a sua gestão, de forma consciente e metódica, em intervalos tidos como adequados, em termos do impacto social e ambiental, aumentando as decisões benéficas e reduzindo as negativas na cadeia de procedimentos e processos.

[63] http://aeiou.expressoemprego.pt/PageTree.aspx?PageTreeId=4983, consultado em 17.Ago.2010.
[64] http://www.iso26000qsp.org/search/label/A%20quest%C3%A3o%20ambiental%20na%20ISO%2026000, consultado em 17.Ago.2010.

2.3 O *COSO ERM* – A Nova Era da Gestão de Riscos

A auditoria tem vindo a evoluir para acompanhar as novas metodologias de gestão nas organizações. Inicialmente a Auditoria era baseada nos controlos - *Control-based Audit*, depois a Auditoria baseada nos processos - *Process-based Audit*, a Auditoria baseada no risco - *Risk-based Audit* e mais recentemente a Auditoria e os conceitos de Gestão do Risco Empresarial - *Enterprise Risk Management*.

Nos anos oitenta o trabalho do auditor consistia fundamentalmente na análise documental para validar e suportar os saldos das principais rubricas do balanço e das transacções, sem descurar os aspectos legais e regulamentares.

A complexidade das operações aliadas aos novos sistemas de TI's veio colocar a ênfase nos processos críticos de negócio.

O relatório publicado em 1987 denominado *Treadway Report*[65] chama a atenção para a adopção de um referencial comum sobre o CI, alertando os responsáveis da gestão para reportarem sobre o funcionamento do sistema de CI, da sua eficácia e da existência ou não de um código de conduta e de uma comissão de auditoria formada por profissionais competentes.

Em 1992, o *COSO* através do *Internal Control-Integrated Framework*, propôs um referencial comum para a definição de CI e os procedimentos para a sua avaliação – O CI consiste num processo concebido e desenhado pelos responsáveis da gestão, assim como outros colaboradores, que visa fornecer garantias relativamente à capacidade da entidade de prosseguir os seus objectivos nas seguintes áreas:

- ✓ Eficiência e eficácia operacional;
- ✓ Fiabilidade do relato financeiro;
- ✓ Cumprimento da legislação e regulamentos aplicáveis.

De acordo com este conceito da auditoria baseada no risco e tendo em linha de conta aquele referencial, o auditor apenas deveria possuir conhecimento da entidade, do seu negócio e do seu sistema de CI de modo a poder planear o seu trabalho. De salientar que a atitude do

[65]Este relatório apresenta os resultados, conclusões e recomendações da Comissão Nacional de Fraude e de Relato Financeiro, de Outubro 1985 a Setembro de 1987, relativos ao estudo levado a cabo sobre o sistema de informação financeira nos EUA, traduzido de http://www.coso.org/Publications/NCFFR.pdf, consultado em 23.Ago.2010.

auditor em face de possíveis fraudes deveria ser a de comunicar essas situações sempre que as detectasse, embora não estando vocacionado para a sua detecção.

"O conluio entre empregados é muitas vezes utilizado para ultrapassar controlos internos bem concebidos de uma empresa lesada[66]*"*. Em empresas com um complexo grau de segregação de funções torna-se quase impossível um único funcionário de forma isolada praticar fraudes. Ele tem de ter o apoio de outros elementos da cadeia, o que pode dificultar e muito a tarefa do auditor.

Como também esta abordagem da ABR se veio a revelar insuficiente no final da década de noventa do último século, o *COSO* desenvolveu e apresentou em 2004 a estrutura conceptual do processo de gestão do risco empresarial *ERM*, que consiste num processo, concebido pelos responsáveis da gestão e outros colaboradores, aplicado com objectivos estratégicos a toda a organização, e utilizado para identificar potenciais riscos que possam afectar a entidade, e a geri-los na lógica da garantia da prossecução dos objectivos da entidade.

Trata-se no fundo de uma metodologia que visa abordar quatro principais categorias de risco:

- ✓ Risco estratégico;
- ✓ Risco operacional;
- ✓ Risco de relato;
- ✓ Riscos legais e regulamentares.

Segundo esta visão *ERM* a GRN deve partir de um entendimento holístico, avaliando a contribuição de cada área, processo, sistema, independente dos limites funcionais da organização no seu organograma, para que a interacção entre riscos possa ser modelada para a prioritização das vulnerabilidades críticas a serem controladas, o que vai permitir encontrar e gerir riscos positivos que podem trazer valor acrescentado e sucesso às organizações interessadas em actuar proactivamente nas fontes de incerteza, alavancando assim oportunidades lucrativas para os seus *stakeholders* e clientes e identificando, para manter dentro de níveis mínimos as suas deficiências e vulnerabilidades em termos de pessoas, processos e sistemas que muitas vezes os impedem de alcançar os objectivos previamente determinados.

De acordo com a *COSO ERM Framework*, a GRN envolve:

[66] Wells, Joseph T., (2009), Manual da Fraude na Empresa – prevenção e detecção – Almedina, página 237.

- ✓ O alinhamento do apetite pelo risco;
- ✓ A melhoria da resposta ao risco;
- ✓ A redução das surpresas operacionais;
- ✓ A identificação e gestão de múltiplos riscos e riscos transversais a toda a empresa;
- ✓ Dimensionamento das oportunidades;
- ✓ A melhoria da utilização do capital.

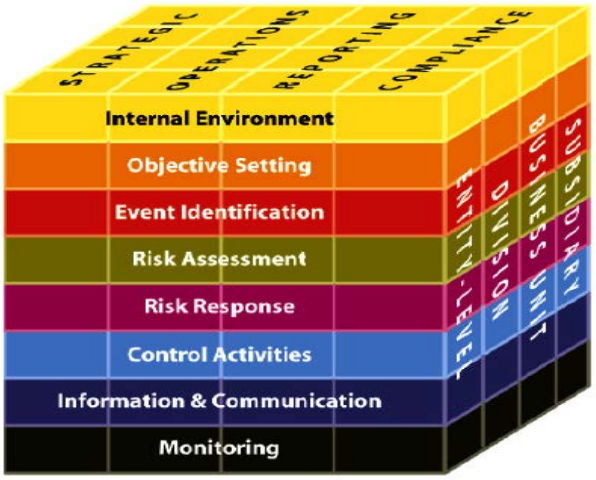


Figura 1 - Cubo *COSO ERM*

Fonte: http://www.nirf.org/_upl/presentasjon_vedr_coso_erm_av_martin_stevens_paa_nfrfs_aarskonferanse_i_stockholm_april_2004.pdf.

A GRN - *ERM* ajuda a gestão a atingir os objectivos de desempenho e de rentabilidade definidos, a evitar a perda de recursos, a reportar em conformidade com a legislação e os regulamentos e a reduzir danos para a reputação da organização e consequências associadas.

A actual redacção das Normas Internacionais de Auditoria **300** - Planear uma Auditoria de Demonstrações Financeiras e **315** - Compreensão da Entidade e do seu Ambiente e Avaliar os Riscos de Distorção Material, são o reflexo claro desta nova perspectiva.

Uma vez fixados os objectivos de CI, é possível identificar e avaliar os eventuais potenciais riscos que possam comprometer a prossecução desses objectivos previamente fixados e assim

a gestão pode desenvolver respostas adequadas, nomeadamente a concepção de um sistema de CI eficaz, cujos objectivos para a entidade podem ser agrupados em quatro categorias:

- ✓ Estratégicos;
- ✓ Relato financeiro;
- ✓ Operacionais;
- ✓ Cumprimento de leis e regulamentos.

Os conceitos desenvolvidos pelo *COSO* relativos à gestão do risco empresarial levarão à ABR, cujo foco principal é determinar quais os objectivos primários do negócio da entidade, os riscos associados e as métricas definidas, avaliando o grau de eficácia das actividades de GRN - *ERM* e garantindo a prossecução da missão da entidade, gerindo os riscos a um nível adequado. Trata-se de uma nova abordagem, que visa alinhar os objectivos estratégicos com os mecanismos de identificação dos riscos, a sua avaliação, gestão e acompanhamento quer pelos auditores internos, quer por auditores externos e membros das comissões de auditoria.

A recente crise mundial de 2008 chamou a atenção sobre a necessidade de se controlar, regular e atenuar os factores de risco, em todos os aspectos da gestão das organizações.

Claro está que essa nova e revigorada cultura de GRN afecta o dia-a-dia da avaliação de riscos para um auditor de TI's, sendo que uma criteriosa avaliação de riscos nesta área é essencial para o contínuo desenvolvimento de um ambiente desse tipo que trabalhe baseado na relação custo/benefício.

Os riscos relacionados com as TI's são cada vez mais um problema da gestão de topo, na medida em que o impacto no negócio de uma falha desse tipo - por exemplo, um *crash* operacional, um problema de segurança, ou um projecto fracassado - pode ter consequências devastadoras. A GRN, em si mesma, não é nada de novo, e a necessidade de correr riscos é parte integrante do dia-a-dia da gestão de qualquer empresa.

Em resumo, a *ERM* ajuda as organizações a chegarem onde querem e a evitar dificuldades e surpresas ao longo do caminho. Dado que as TI's desempenham um papel significativo nas estratégias e operações de muitas organizações, os riscos inerentes deverão ter um grande significado numa abordagem global de *ERM*.

2.4 A *ISO* 27003 – Gestão de Segurança Informática

"Um sistema de informação deve produzir indicadores que possibilitem a análise dos resultados da organização quanto à satisfação dos clientes e do mercado, resultados financeiros, pessoas, fornecedores/produtos e processos organizacionais[67]*".*

"O sistema de informações competitivo deve ser definido a partir da vantagem competitiva que a empresa possui, pretende conquistar ou manter. Será fonte de vantagem competitiva se contribuir para aprimorar as características da vantagem competitiva que a empresa busca[68]*".*

"A informação deve ser usada para aperfeiçoar e não para julgar nem controlar as pessoas[69]*",* mas dada a sua actual complexidade as organizações confrontam-se com muitos problemas para conseguir manter uma segurança da informação capaz de por um lado disponibilizar o que tem de ser disponibilizado, mas apenas às pessoas certas e por outro de controlar os acessos e os ataques de elementos nocivos à organização.

As necessidades da organização em termos da utilização da informação, de segurança da informação e do envolvimento das pessoas no que concerne à informação, à segurança dessa mesma informação, bem como os impactos, em termos de segurança, da utilização dos sistemas de informação que permitem a partilha da informação e das tecnologias de informação e comunicação que suportam esses mesmos sistemas, estão hoje entre as principais preocupações da gestão.

"A necessidade de determinar a documentação crítica para o negócio, garantindo o acesso imediato à informação e a consciência dos benefícios da implementação de sistemas de gestão documental, está a tornar-se cada vez mais procurada pelas organizações das mais diversas dimensões, dado que a vulnerabilidade das redes cresce a um ritmo mais acelerado do que o tempo de resposta para actualizações e correcções nos sistemas e apesar de ferramentas antivírus e firewall isso não é suficiente para que o sistema esteja livre de vírus, ataques, acesso a informação classificada ou mesmo fraudes.

[67] Meireles, Manuel, Sistemas de Informação, Volume I, Primeira Edição 2001, página 132, Editora Arte & Ciencia, Coleção Sapientia.
[68] Meireles, Manuel, Sistemas de Informação, Volume I, Primeira Edição 2001, página 41, Editora Arte & Ciencia, Coleção Sapientia.
[69] Meireles, Manuel, Sistemas de Informação, Volume I, Primeira Edição 2001, página 25, Editora Arte & Ciencia, Coleção Sapientia.

Para ajudar têm surgido várias ferramentas como a série de normas ISO 27000 que foi reservada pela ISO exclusivamente para assuntos de Segurança da Informação, relacionadas com outras áreas, como as séries ISO 9000 da Gestão da Qualidade e a ISO 14000 da Gestão Ambiental, entre outras[70]".

A evolução das TIC, em vez de simplificar o processo veio nalguns casos torná-lo muito complexo e fazer com que se tenha perdido a capacidade de controlo. Os fluxos de informação suscitaram dúvidas sobre a segurança dos dados utilizados pelas organizações, bem como sobre a vulnerabilidade dos mesmos face aos acessos por parte de agentes externos à entidade.

Daí a necessidade da nova **norma 27003** que será constituída por indicações para implementação, supervisão e melhoria contínua do sistema de controlos. Com um conteúdo idêntico ao da norma BS 7799-3:2005 – *Information Security Management Systems - Guidelines for Information Security Risk Management*[71], consistirá num guia de implementação de um *SGSI*, sendo um suporte da norma *ISO/IEC*/27001 e informações sobre como usar o modelo *PDCA* e as exigências nas suas diferentes fases.

O Modelo *PDCA* é o mesmo que é utilizado para qualquer sistema de gestão e estabelece os seguintes passos: *Plan – Do – Check – Act*[72].

"Tem a sua origem no Anexo B da norma BS7799-2 e da série de documentos publicados pela BSI ao longo dos anos, com recomendações e directrizes de implementação[73]".

"Já foi publicada em 01 de Fevereiro de 2010, mas não é certificável e irá ajudar as organizações a implementar um ISMS, nos seguintes pontos:

- ✓ *Aprovação e autorização para a gestão do projecto;*
- ✓ *Definição de limites e fronteiras;*
- ✓ *A avaliação de riscos e plano de tratamento de risco;*
- ✓ *Design do ISMS;*
- ✓ *Planeamento do projecto de execução[74]".*

[70] http://andrepitkowski.wordpress.com/tag/iso27001/, consultado em 15.Ago.2010.
[71] http://www.smartsec.com.br/iso_27000.html, consultado em 15.Ago.2010.
[72] http://latamnews.globalcrossing.com/2009/06-jun/Sec_DC_Out/Sec_DC_Out_10POR_jun.htm, consultado em 15.Ago.2010.
[73] http://iso27000.wik.is/Area_Normas, consultado em 15.Ago.2010 às 14 horas.
[74] http://www.seguridadinformatica.es/profiles/blogs/publicada-isoiec-270032010, consultado em 15.Ago.2010.

"Hoje as empresas precisam de gerir o SI de que dependem de modo a torná-lo o mais seguro possível e isso abrange pessoas, processos e sistemas de TI. A segurança vai tranquilizar clientes e fornecedores e mostra que a organização leva a sério as ameaças à sua informação, tornando-a assim mais atractiva aos olhos dos seus clientes e fornecedores, e de todos os interessados[75]*"*.

A Gestão dos SI alia credibilidade comercial à redução dos custos com possíveis incidentes de segurança, claramente mais dispendiosos do que investir em sistemas de protecção contra riscos de negócio, vulnerabilidades e a forma de as evitar. As organizações globais têm tentado tornar a sua gestão mais responsável social e ambientalmente, e procurado dominar as novas TI's através das várias ferramentas que ajudem a criar valor acrescentado à organização e a trazer vantagens competitivas que lhes permitam conquistar e manter todos os terceiros que com ela interagem, interessados e confiantes.

[75] Traduzido de http://www.iso.org/iso/pressrelease.htm?refid=Ref1302, consultado a 15.Ago.2010.

3. *ISO* 31000:2009

Este terceiro capítulo, e na sequência da nova gestão tendo em conta os riscos, analisa o novo paradigma da auditoria, baseada em riscos, a implementação dos processos de gestão pró-activa de riscos, para introduzir a nova norma de GRN – a *ISO* 31000 e o seu *Guide* 73 de apoio aos termos e definições.

3.1 A Auditoria Baseada em Riscos – ABR

O IIA define ABR como uma metodologia que associa a auditoria interna, doravante designada por AI à GRN de uma organização, possibilitando que esta dê garantias à gestão de topo que os processos de GRN os estão a tratar de maneira eficaz em relação ao seu nível de apetência por riscos[76].

Para implementar uma auditoria deste tipo é conveniente avaliar a maturidade dos riscos da organização, em cadastro próprio a cada organização, elaborando um plano de auditorias periódicas e documentando a ligação da GRN com a ABR.

A AI, como actividade independente e objectiva de garantia e aconselhamento, é concebida para agregar valor e melhorar as operações de uma organização, podendo auxiliar esta a atingir os seus objectivos através da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de GRN e dos controlos. Esta abordagem a implementar pelos auditores deverá ser compatível com a escolhida pela organização para evitar duplicações dos processos, devendo a auditoria usar os seus esforços para fazer a sua correcta avaliação, com o objectivo de fornecer uma garantia independente para a gestão de que os processos de GRN, colocados em prática na organização, estão em conformidade com o planeado e dentro de um nível aceitável do chamado apetite pelo risco, conseguido através de uma estrutura sólida de controlos para os mitigar.

Cada organização deverá determinar como pretende implementar ou melhorar a GRN, preferencialmente adoptando como modelo de referência a nova norma internacional ***ISO* 31000:2009,** que ajudará a determinar o seu nível de apetite por riscos e maturidade da organização no que concerne à GRN. A ABR possibilita que a AI se ligue directamente a essa

[76] Traduzido de http://www.theiia.org/, consultado em 15.Jan.2010.

estrutura de GRN, alavancando dessa forma as sinergias, ao permitir que o auditor identifique os riscos para a prossecução do negócio e o grau de apetite por riscos aconselhável para a organização, que ela estará disposta a suportar.

Para isso deverá verificar se os processos de GRN são adequados e eficazes na identificação, análise, avaliação, tratamento e reporte dos riscos.

Em caso negativo cabe ao auditor propor a melhoria desse processo que determine as áreas a serem auditadas, sendo que para cada área deverá analisar a adequação dos processos de GRN para os identificar e gerir.

Em caso afirmativo avaliará esses processos, ou proporá formas de identificar e avaliar os riscos e respectivos controlos existentes. Se chegar à conclusão que há muitas falhas deverá realizar a sua própria avaliação de riscos.

As questões fundamentais da organização a abordar com a ABR são as finanças, a qualidade, a RSE, a *compliance*, garantindo o controlo e optimizando a GRN.

Se o auditor centrar a sua atenção sobre os riscos, a auditoria fica mais direccionada para apoiar a gestão, pois em vez de identificar e testar os controlos, o auditor irá identificar os riscos e testar as vias pelas quais a gestão mitiga e controla esses riscos.

Quando os auditores internos utilizam os componentes do método *COSO*, anteriormente referidos, ou seja - Ambiente de Controlo, Avaliação de Risco, Actividade de Controlo, Informação e Comunicação e Supervisão, é possível analisar se a organização possui um ambiente de CI eficiente - se os funcionários sabem o que deve ser feito, se sabem como fazê-lo e se querem e podem fazê-lo, se os riscos relacionados estão identificados, se possui normas e procedimentos específicos e se essas estão de acordo com os objectivos estratégicos traçados, se esses procedimentos são realizados através de comunicação formal ou informal, e verificar se a qualidade dos controlos utilizados efectivamente realizam a sua função de manter o grau de risco residual ao nível desejado.

Esta visão macro permite ao auditor emitir opiniões eficazes e pró-activas com relação ao risco, avaliar o impacto desta materialização frente aos objectivos da organização e fornecer informações para tomadas de decisões tempestivas por parte da alta administração.

3.2 Implementação de Processos de Gestão Pró-Activa de Riscos

"A administração deve avaliar se tem implementado controlos que tratem adequadamente o risco dos erros materiais não serem prevenidos ou detectados atempadamente e em seguida, centrar-se sobre a fixação ou o desenvolvimento de controlos para preencher eventuais lacunas. Tem de ter em atenção que o risco real reside nas pessoas por trás dos processos e controlos que compõem o ambiente da empresa como um elemento de controlo dinâmico e desafiador da consciência da organização.

As pessoas cometem erros e irregularidades e a avaliação do ambiente de uma empresa com base no risco torna-se cada vez mais necessária. É uma oportunidade para a gestão de identificar os elos fracos que poderão vir a resultar numa distorção, bem como para os departamentos de AI de fazerem a avaliação da gestão. Os auditores internos devem evitar confiar demasiado na documentação, especialmente quando se trata de quantificar e caracterizar o elemento humano do risco de adulteração, e precisam de ser capazes de desafiar a qualidade, integridade e motivação dos funcionários, em todos os níveis da organização"[77].

"A orientação da SEC vem de encontro aos princípios do tipo de risco baseado numa abordagem de auditoria holística que melhor servirá a organização.

Para implementar a GRN *com sucesso, as organizações devem abordar uma ampla gama de problemas na fase de planeamento em relação à gestão do pessoal e ao compromisso com o processo, bem como o processo de sustentabilidade de longo prazo.*

O desenvolvimento de uma ferramenta adaptada à forma como as abordagens de risco são executadas na organização não é tão rígida como muitos podem pensar[78]*".*

"A matriz de risco é uma ferramenta comummente usada para documentar a análise dos objectivos, riscos e respostas. Normalmente uma matriz de riscos concentra-se primeiro sobre os riscos inerentes - isto é, todos os eventos de risco que poderiam ter um impacto no alcance dos objectivos, sem levar em conta as respostas da administração. A matriz de riscos inerentes típicos lista esses eventos de risco, juntamente com uma classificação de risco - alto,

[77] Traduzido de The Human Side of Risk by Russell Jackson, artigo inserido na página 40 da Revista Internal Auditor de Out. 2007.

[78] Traduzido de The Model Approach by Imad A. Mouchayleh, artigo inserido na página 75 da Revista Internal Auditor de Out. 2007.

médio ou baixo do seu potencial impacto e probabilidade. Em seguida, a matriz identifica a resposta da administração ou seja os controlos para cada evento e determina a sua adequação global. A questão central desta avaliação é, considerando os riscos identificados, se a gestão tem respostas para mitigar ou controlar os eventos de risco. Com base nesta avaliação, os auditores prepararam um programa de auditoria para testar a eficácia operacional dos controlos[79]*".*

"Usando uma abordagem de análise de risco residual que começa por identificar os controlos, o processo da matriz de riscos pode ser tornado mais eficaz e eficiente, nomeadamente através da identificação dos riscos que não estão a ser tratados pelos controlos existentes, com o objectivo de os mitigar[80]*".*

Desta forma a avaliação de riscos e vulnerabilidades ajuda a compreender melhor as situações que constituem o risco mais elevado para que seja possível dar prioridade e implementar as técnicas de mitigação adequadas. É por essa razão que muitas organizações falham em atingir os resultados desejados nas suas iniciativas de gestão do desempenho, apesar de terem planos bem delineados.

A importância de tornar a gestão do risco pró-activa num elemento essencial em qualquer gestão do desempenho, visa reduzir a um nível aceitável, em antecipação, os riscos identificados pela organização, através da criação de uma cultura fundamentada na avaliação e na prevenção, em vez de acções reactivas e de correcção.

A GRN pró-activa é um elemento-chave na gestão do desempenho.

O problema está em que poucas organizações tendem a monitorar proactivamente e a gerir o risco como forma de definir e implementar as suas estratégias de gestão de desempenho, sendo o foco colocado nos resultados positivos que se pretendem alcançar e não nos factores negativos que podem surgir, mas que são ignorados.

A única forma da gestão obter um desempenho com real optimização, maximizando a rentabilidade e vantagens competitivas sustentadas é quando o risco potencial e as

[79] Traduzido de The Matrix Revisited by Larry Hubbard, artigo inserido na página 55 da Revista Internal Auditor de Abr.2009.

[80] Traduzido de The Matrix Revisited by Larry Hubbard, artigo inserido na página 55 da Revista Internal Auditor de Abr.2009.

consequências são devidamente avaliadas, geridas e enquadradas nas metas de desempenho visadas pela organização.

Talvez o maior obstáculo para o equilíbrio eficaz do desempenho e do risco é que ele requer mudanças inerentes à cultura da empresa, sendo necessário criar um ambiente onde o risco é considerado e avaliado em cada etapa durante o processo de planeamento estratégico, acompanhamento e, em seguida, de forma proactiva, com metas e objectivos a cumprir, exigindo mudanças culturais que permitam chegar a um equilíbrio adequado.

A organização deverá adoptar actividades eficazes de GRN, tais como a identificação de ameaças, análise, avaliação, e previsão, ou por outras palavras, deve ligar os indicadores chave de desempenho – KPI's[81], aos indicadores chave de risco – KRI's para ter uma visão completa do risco ajustado ao desempenho, de uma forma dinâmica que permita fácil modificação e seja personalizável para se adaptar de imediato à evolução dos riscos externos, como as novas exigências reguladoras ou às dinâmicas condições do mercado, bem como aos factores internos, tais como mudanças inesperadas nas estratégias ou mudanças na política da empresa.

A supervisão de riscos é considerada proactiva e não reactiva, quando se consegue uma gestão em tempo real dos indicadores KPI's e KRI's, permitindo ver não só o que aconteceu, mas também o que está a acontecer tanto em termos de desempenho como de perspectiva de risco. O sistema deve oferecer indicações dinâmicas, para de imediato, notificar as partes interessadas no momento do estado crítico ou quando um importante evento ocorra.

A GRN inclui quatro etapas que são a identificação, avaliação e hierarquização dos riscos, tratamento dos riscos, acompanhamento da evolução e finalmente a garantia do bom andamento do mecanismo através de fiscalizações independentes[82].

"A falta de supervisão pró-activa de riscos, detecção e prevenção significa que, mesmo quando as organizações estão conscientes das ameaças, são incapazes de controlá-las eficazmente, o que torna difícil evitar que os riscos tenham um impacto negativo ou mesmo manter o desempenho e o risco dentro de níveis considerados aceitáveis[83]".

[81] Medem o nível de desempenho do processo, focando no "como" e indicando quão bem os processos de tecnologia da informação permitem que o objectivo seja alcançado, em http://pt.wikipedia.org/wiki/KPI, consultado em 24.Ago.2010.
[82] Moreau, Franck (2003) Compreender e Gerir os Riscos, Bertrand Editora, página 189.
[83] Traduzido de http://www.computerworld.com.pt/media/2010/07/WP_9025.pdf, consultado em 20.Ago.2010.

Assim qualquer programa de GRN deve ter em atenção a cultura quanto à GRN, o pessoal, os controlos internos e a tecnologia de suporte, elementos que interagindo entre si são essenciais para o sucesso dentro da organização.

Essa cultura de GRN deverá ser orientada, com o comprometimento da alta direcção, de forma a ser flexível para mudar práticas existentes, admitir lacunas noutros casos e ser capaz de encontrar respostas qualificadas, para além de promover as responsabilidades individuais, educando todos os colaboradores.

Cada colaborador deve participar nesse processo de maneira efectiva, através do pleno conhecimento de suas responsabilidades e dos riscos a serem evitados.

A motivação é decisiva para o estabelecimento de um programa de GRN, complementada com controlos internos e utilizando a tecnologia como uma ferramenta de grande importância no treino e educação dos colaboradores para a tomada de decisões ao nível da gestão pró-activa de riscos.

"A auditoria posiciona-se, assim, claramente na cadeia de riscos: a auditoria define-se sempre como uma actividade independente e objectiva mas ultrapassa a aprovação da conformidade, "proporcionando aconselhamento" e, sobretudo, avaliando os processos de gestão de riscos[84]".

A GRN ou *Risk Management* tem como vantagens alinhar a apetência para o risco e estratégia, ligar crescimento, risco e retorno, identificar as decisões de resposta ao risco, minimizar surpresas operacionais e perdas, identificar e gerir riscos transversais inter-relacionados, proporcionar respostas integradas a riscos múltiplos, aproveitar oportunidades e racionalizar o capital[85].

"As organizações estão agora com uma mentalidade de supervisão do risco e da sua importância para o planeamento estratégico e para a criação de valor numa abordagem top-down[86]", não como um fim em si mesmo mas como um meio, um facilitador do processo de gestão, inter-relacionando-se com a governação da sociedade, com a performance de gestão e com o CI, parte integrante da GRN[87].

[84] Moreau, Franck (2003) Compreender e Gerir os Riscos, Bertrand Editora, página 217.
[85] Beja, Rui (2004) Risk Management – Gestão, Relato e Auditoria dos Riscos de Negócio, Áreas Editora, página 88.
[86] Traduzido de Time to teach ERM by Mark S. Beasley, artigo inserido na página 61 da Revista Internal Auditor de Fev. 2009.
[87] Beja, Rui (2004) Risk Management – Gestão, Relato e Auditoria dos Riscos de Negócio, Áreas Editora, página 89.

Relativamente ao enquadramento sistémico do *Risk Management*, há quatro componentes fundamentais que são o planeamento estratégico e a contabilidade de gestão, o CI e os instrumentos técnicos de *Risk Management*, constituído por um conjunto de metodologias próprias da organização, responsabilização e de execução que em articulação dão corpo a todo este processo[88].

"Ao risco da empresa inerente à tomada de decisão, à gestão corrente, às opções estratégicas, vem juntar-se e, muitas vezes, combinar-se, um ambiente de risco, ele próprio marcado pela importância do imaterial e da dificuldade crescente em definir fronteiras da empresa"[89]. Tudo isto devido aos novos problemas criados pela globalização, as novas tecnologias, pois além da responsabilidade do espaço existe a responsabilidade do tempo, que pode inclusive alterar a atitude dos dirigentes e colaboradores e modificar inclusive o seu comportamento[90].

3.3 As Directrizes da Nova Norma Internacional - *ISO* 31000:2009

"O texto em português da norma internacional ISO 31000:2009 e do ISO Guia 73:2009 traz a seguinte definição oficial de Risco – ***Risco é o efeito da incerteza nos objectivos****. Por efeito entende-se um desvio em relação ao esperado - positivo e/ou negativo.*

Os objectivos podem ter diferentes aspectos - metas financeiras, de segurança e ambientais e podem aplicar-se em diferentes níveis - estratégico, em toda a organização, de projecto, de produto e de processo.

O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma combinação destes e expresso em termos de uma combinação de consequências de um evento e a probabilidade de ocorrência associada.

A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, conhecimento, a sua consequência ou a sua probabilidade[91]*".*

"O processo de gestão de riscos auxilia a tomada de decisão, levando em consideração as incertezas e a possibilidade de circunstâncias ou eventos futuros.

[88] Beja, Rui (2004) Risk Management – Gestão, Relato e Auditoria dos Riscos de Negócio, Áreas Editora, página 90 e 91.
[89] Moreau, Franck (2003) Compreender e Gerir os Riscos, Bertrand Editora, página 227.
[90] Moreau, Franck (2003) Compreender e Gerir os Riscos, Bertrand Editora, página 227 e 228.
[91] http://www.blogger.com/feeds/5432916894862042050/posts/default, consultado em 22.Ago.2010.

O processo de avaliação de riscos é a parte da GRN que fornece um processo estruturado para identificar como os objectivos podem ser afectados, e analisa o risco em termos das consequências e suas probabilidades, antes de decidir se um tratamento adicional é requerido.

A ISO/IEC 31010:2009 auxilia as organizações na implementação dos princípios e directrizes de GRN fornecidas pela ISO 31000:2009 - GRN - princípios e directrizes, complementada pelo ISO Guia 73:2009 - GRN -vocabulário.

A aplicação de uma série de técnicas é introduzida na ISO/IEC 31010, com referências específicas a outras normas internacionais em que o conceito e a aplicação das técnicas são descritos mais detalhadamente. O processo de avaliação de riscos é uma actividade autónoma e deve ser plenamente integrado noutros componentes do processo de GRN.

Esta nova norma foi desenvolvida para aplicação tanto por principiantes na GRN como por profissionais experientes, ela é parte de uma estrutura integrada de normas de GRN, desenvolvidas com vista a proporcionar uma abordagem de melhores práticas para todas as organizações"[92].

Como objectivos desta norma podem-se destacar no *"**QSP 31000:2010** -* **Sistemas de Gestão de Riscos – Requisitos** os seguintes**:**

- ✓ *Demonstrar aos stakeholders a capacidade de gerir riscos - de todos os tipos - de maneira eficaz e eficiente;*
- ✓ *Demonstrar que estão à frente dos concorrentes na implementação das melhores práticas actuais - e internacionais - de GRN;*
- ✓ *Utilizar o Sistema de GRN para dar suporte a todos os seus programas de compliance;*
- ✓ *Ganhar vantagem competitiva no mercado;*
- ✓ *Reduzir custos e agregar valor aos demais sistemas de gestão existentes na empresa*[93]*".*

[92] http://www.blogger.com/feeds/5432916894862042050/posts/default, consultado em 22.Ago.2010.
[93] http://www.blogger.com/feeds/5432916894862042050/posts/default, consultado em 22.Ago.2010.

Na edição de *Inside Deloitte ISO* 31000: 2009[94] pode ler-se que esta norma fornece orientações sobre o estabelecimento e manutenção de um quadro de gestão formalizado de risco que podem ser adoptadas por qualquer organização - incluindo públicas, privadas, sem fins lucrativos e organizações governamentais.

No actual cenário de volatilidade financeira e dos negócios nenhuma organização está imune ao risco e como tal o mais acertado é geri-los de forma controlada, tentando estabelecer um quadro consistente de GRN que pode ser integrado em várias indústrias e regiões e adoptado por qualquer tipo de organização.

Novas definições	O que isso significa
Definição de risco	*Risk* é definido como o "efeito da incerteza sobre os objectivos". Esta definição é coerente com ASNZ 4360 *("a possibilidade de acontecer algo que terá impacto sobre os objectivos"*), mas difere da percepção de que muitas pessoas têm de que os riscos são *"riscos"* ou *"coisas que correm mal"*. Risco é um evento neutro, que pode ser positivo ou negativo.
A *Framework*	Ao invés de simplesmente articular um processo de gestão de risco que as organizações podem adoptar, a *ISO* 31000 trata especificamente as práticas necessárias relativas à gestão da estrutura (concepção, implementação, monitorização e melhoria contínua). Como resultado, a norma prevê um sistema completo de gestão de risco em toda a empresa.
Gestão da Qualidade	A *ISO* 31000 está alinhada com o Processo de Gestão da Qualidade (cláusula 4.6), de "*Plan, Do, Check, Act* ", reformulada como *"Framework Design, implementação, monitorização e revisão e melhoria contínua da Framework"*.
Responsabilidade	A *ISO* 31000 coloca a tónica na importância de fazer a organização, bem como gestores individualmente - responsáveis por riscos e controlos do risco. Empenho e responsabilização, gestão de risco, são considerados critérios fundamentais de avaliação de desempenho em toda a organização.
Definição de prioridades	Para ajudar as organizações a definir prioridades, a norma deixa claro que a gestão de risco em si deve criar valor. Como resultado, isso significa que os gestores devem garantir que os recursos consumidos pela gestão do risco não excedam o impacto potencial do risco.

Figura 2 – O que há de novo na *ISO* 31000?

Fonte: http://www.deloitte.com/view/en_CA/ca/services/enterpriserisk/risk-cnsulting/dd30be87be927210 VgnVCM100000ba42f00aRCRD.htm.

[94]Traduzido de http://www.deloitte.com/view/en_CA/ca/services/enterpriserisk/risk-consulting/dd30be87be927210VgnVCM100000ba42f00aRCRD.htm, consultado em 26.Jun.2010.

A *ISO* 31000 está dividida em três secções:

- ✓ Princípios e Directrizes;
- ✓ *Framework*
- ✓ Processo

Tratam especificamente as práticas necessárias relativas à gestão da estrutura - concepção, implementação, monitorização e melhoria contínua, alinhada com o processo de Gestão da Qualidade.

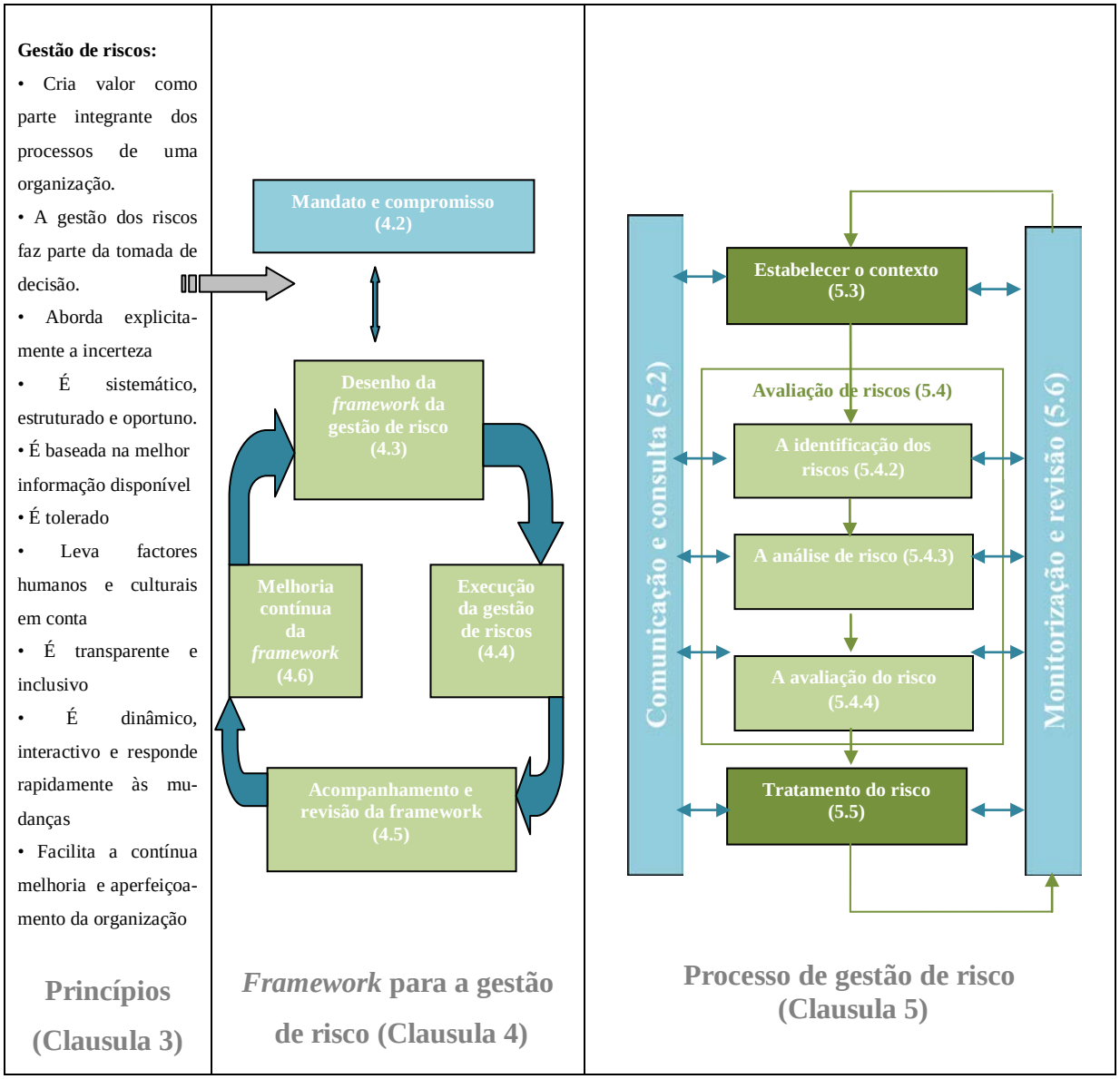


Figura 3 - Relationship *between the 3 key clauses of the ISO 31000:2009 standard*

Fonte: Traduzido de http://torquemanagement.newsweaver.co.uk/TorqueManagement/1dvfvtvm56c.

O empenho e responsabilização da GRN são considerados os critérios fundamentais de avaliação de desempenho em toda a organização.

Para ajudar as organizações a definir prioridades, a norma deixa claro que a GRN em si deve criar valor, o que significa que deve ser garantido que os recursos consumidos pela gestão do risco não excedem o impacto potencial do risco.

A S&P publicou um artigo[95] com as principais questões relacionadas com organizações não financeiras de todo o mundo e sobre a forma como estão a gerir os seus riscos. É dado destaque no artigo a esta nova norma, pela importância crescente que está a ser dado à GRN nos critérios de *rating* de crédito. A obtenção de crédito pelas empresas é mais um forte argumento que se irá somar aos benefícios e às justificativas para a adopção de um modelo de GR aprovado internacionalmente, como é o caso da *ISO* 31000.

Na classificação de risco *S&P Ratings Services* as empresas de crédito incluem avaliações das estratégias dos gestores, de eficácia e credibilidade, que vão ajudar a desenvolver no futuro pareceres sobre capacidade de crédito, completando a análise fundamental do negócio da empresa e o perfil de risco financeiro.

Iniciado em Setembro de 2008, alargou o âmbito a algumas empresas não financeiras para melhorar a revisão da capacidade dos gestores para identificar, monitorar e gerir os riscos - avaliação do risco empresarial *ERM*. Afinal a gestão e a avaliação de credibilidade sempre foram importantes na análise de crédito, tratando-se apenas de alargar o âmbito para verificar a credibilidade da gestão, isto é, se as suas acções são coerentes com os seus planos e objectivos, e de como ela afecta o crédito, o stress financeiro ou os desafios estratégicos, pois uma vez perdida a credibilidade torna-se difícil de a voltar a recuperar!

Existindo actualmente uma série de normas para GRN, qual será a necessidade de adoptar a norma *ISO* 31000?

Como já vimos a criação de padrões é um elemento fundamental para desenvolver uma linguagem comum, sistemas de gestão, normas e procedimentos para orientar as organizações como um todo e disseminar a cultura de GRN.

A ideia subjacente a esta norma é usá-la como referência de todos os padrões que envolvam a GRN, ou seja, ser a norma das normas para uma GRN integrada, tanto no que se refere a

[95] Traduzido de http://www.marsh.nl/documents/nieuwsenmedia/Rapport_SP_ERM.pdf, J Dreyer, Steven "Standard & Poor's Looks Further Into How Nonfinancial Companies Manage Risk", consultado em 24 Jun.2010.

riscos ambientais, operacionais ou financeiros, de segurança da informação, que qualquer tipo de organização em qualquer parte do mundo possa sentir e querer gerir.

A norma recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cuja finalidade é integrar o processo para gerir os riscos na governação, gestão, políticas, valores e cultura e em toda a organização.

Como não é certificável a forma como cada organização a vai moldar ao seu próprio caso pode ser demorada, mas espera-se que com resultados muito satisfatórios.

Já estão pensadas novas normas desta série para a complementarem, também sem o objectivo da certificação, como é o caso da norma *ISO* 31010: *Risk Management – Risk Assessment Techniques*, que se destina a fornecer orientações sobre a definição e aplicação de técnicas e métodos para avaliação de riscos, com periodicidade de revisão anual[96].

"A norma 31010 sugere que se utilize para questões de impacto não somente a componente financeira, mas também as de imagem, de recursos humanos, e as relativas à área operacional[97]".

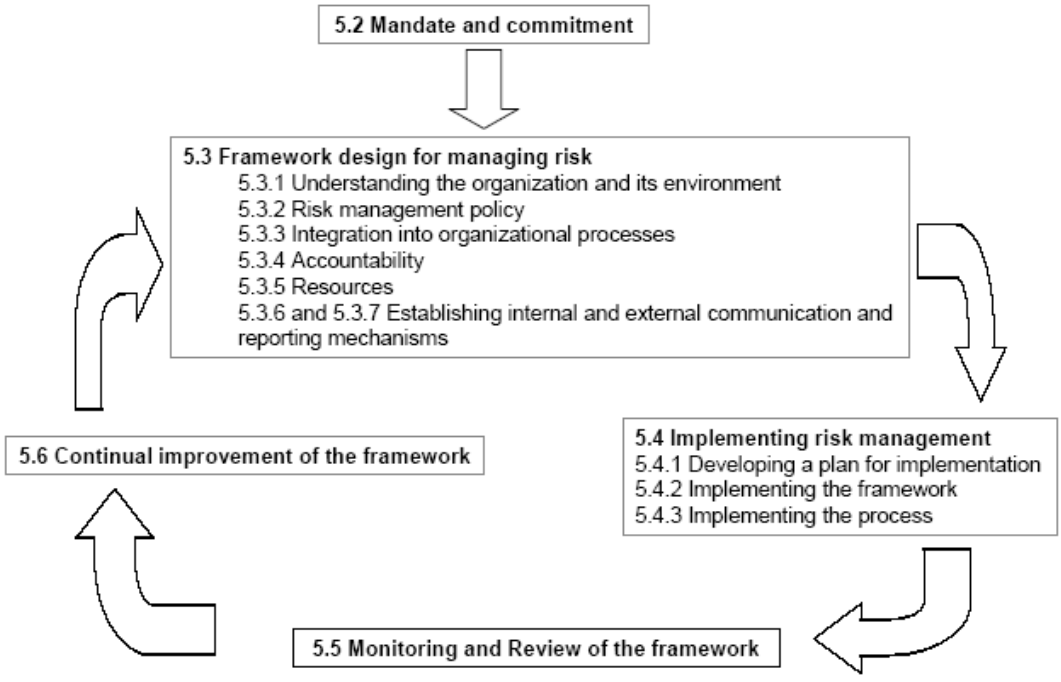


Figura 4 - ***ISO* 31000**

Fonte: http://www.elogroup.com.br/download/Apresenta%C3%A7ao%20IBRACON%20-%20Gestao%20de%20Risco%20e%20a%20ISO%2031000.pdf

[96] Edição 56 da revista Gestão de riscos da Brasiliano & Associados, Junho 2010, página 26.
[97] Edição 56 da revista Gestão de riscos da Brasiliano & Associados, Junho 2010, página 28.

Não é uma norma de substituição de nenhuma das existentes.

A *ISO*/*IEC* 27005 faz parte do conjunto de normas da série de 27M, sobre o sistema de gestão de SI, e apresenta as melhores práticas para SI.

A *ISO* 31000 é mais genérica contemplando todos os sectores, e a tendência é depois rever todas em conjunto para as alinhar.

Relativamente às orientações do *COSO ERM* no que se refere aos princípios de GRN e processos, a principal diferença com a norma *ISO* 31000 é que o seu conteúdo se apresenta de uma forma mais sucinta, oferecendo orientações genéricas para GRN, determinando princípios, uma *framework* de trabalho e um processo para gestão dos diversos tipos de risco.

A norma apresenta a seguinte estrutura:

Introdução

1. Âmbito

2. Termos e Definições

3. Princípios

4. Estrutura

5. Processo

6. Anexos: A Atributos de uma gestão de riscos avançada

"O processo de gestão de riscos contido na ISO 31000 *segue o padrão australiano e neozelandês AS/NZS 4360, que consiste em:*

- ✓ *Comunicação e consulta;*
- ✓ *Estabelecimento do contexto;*
- ✓ *Avaliação do risco contendo as etapas de identificação, análise e avaliação;*
- ✓ *Tratamento do risco;*
- ✓ *Supervisão e revisão;*
- ✓ *Benefícios."*

"Quando implementada e mantida em conformidade com a norma internacional ISO 31000, *a* ***GRN possibilita*** *à organização:*

- ✓ *Encorajar a gestão pró-activa ao invés da reactiva;*
- ✓ *Estar ciente da necessidade de identificar e tratar riscos em toda a organização;*

- ✓ *Aperfeiçoar a identificação de oportunidade e ameaças;*
- ✓ *Estar em conformidade com requerimentos legais e de regulação e normas internacionais;*
- ✓ *Aperfeiçoar os relatórios financeiros;*
- ✓ *Aperfeiçoar a governação;*
- ✓ *Melhorar a confiança dos stakeholders;*
- ✓ *Estabelecer uma base confiável para o planeamento e a tomada de decisão;*
- ✓ *Aperfeiçoar os controlos;*
- ✓ *Alocar e utilizar os recursos para o tratamento dos riscos de maneira eficaz;*
- ✓ *Melhorar a efectividade e a eficiência operacional;*
- ✓ *Melhorar a gestão de incidentes e a sua prevenção;*
- ✓ *Minimizar as perdas."*

Os **problemas e desafios** relativos à norma *ISO* 31000 estão relacionados directamente aos seus princípios:

- ✓ Criação de valor;
- ✓ Ser parte integrante dos processos organizacionais;
- ✓ Ser levada em conta na tomada de decisão;
- ✓ Ser sistemática, estruturada e oportuna;
- ✓ Ser baseada na melhor informação disponível;
- ✓ Ser adaptável;
- ✓ Levar em consideração factores humanos e culturais;
- ✓ Ser transparente e inclusiva;
- ✓ Ser dinâmica, interactiva e dar resposta às mudanças;
- ✓ Facilitar a melhoria contínua da organização.

O que se pretende no fundo com este tipo de norma é melhorar a identificação de oportunidades e ameaças, a conformidade com requisitos legais/reguladores e normas internacionais, as demonstrações financeiras e a governação.

"O maior desafio enfrentado pela ISO 31000 *está em estabelecer uma terminologia comum, assim como padronizar as melhores práticas e frameworks para que organizações possam implementar práticas de gestão de riscos em seus processos*[98]*"*.

"A certificadora internacional GL acaba de conceder ao Instituto Biocor[99] *o primeiro certificado do mundo derivado da nova norma ISO* 31000 *de Gestão de Riscos.*

A conquista da certificação em tempo recorde pelo Biocor é atribuída à elevada maturidade dos sistemas de gestão já existentes na instituição, que já é certificada nos padrões ISO 9001 *(Qualidade, desde 1997), ISO* 14001 *(Gestão Ambiental, desde 2008) e OHSAS* 18001 *(Segurança e Saúde no Trabalho, também desde 2008), além de possuir a acreditação no "nível 3 com Excelência" da ONA, desde 2005, e a acreditação internacional NIAHO, obtida em 2009*[100]*"*. Como se pode ler no site desta empresa *"para o fundador e director geral do Instituto Biocor, Dr. Vrandecic, Mario a GRN em nossa instituição é desenvolvida, implementada e mantida de forma a permitir a sustentabilidade do Biocor, protegendo nossos clientes/pacientes, a organização, os colaboradores, o corpo clínico, os bens, os recursos e a sua imagem"*. O Sistema de GRN do *Biocor* abrange todos os tipos de riscos enfrentados pela instituição, os quais foram agrupados em cinco grandes categorias: riscos ao paciente, ambientais, ocupacionais, de responsabilidade civil e financeiros.

"Os riscos somos nós. Eles foram fundamentais para a conquista dessa importante e inédita certificação, ampliando e consolidando a incorporação da GRN na cultura da nossa instituição, tanto no discurso como, principalmente, no nosso dia-a-dia e em todos os processos e actividades que realizamos", orgulha-se o Dr. *Vrandecic*, que afirma ainda *"o trabalho em equipa na nossa instituição não é uma opção, mas sim uma obrigação"*[101].

O certificado pode ser consultado em anexo a este trabalho[102].

"A norma como já se disse não é destinada a certificação, mas o Instituto Biocor por razões operacionais e estratégicas, manifestou interesse em se certificar apoiando-se totalmente na nova referência mundial em GRN, que é a ISO 31000.

[98] http://www.softexpert.com.br/norma-iso31000.php, consultado em 20 Jul.2010.
[99] O Biocor Instituto é hoje um complexo hospitalar de referência a nível nacional e internacional, que prima pela qualidade total de seus serviços, em http://www.biocor.com.br/, consultado em 27.Ago.2010.
[100] http://www.qsp.org.br/biocor.shtml, consultado a 27.Ago.2010.
[101] http://www.biocor.com.br/novo/detalhes.php?id=17, consultado em 27.Ago.2010.
[102] http://www.biocor.com.br/novo/detalhes.php?id=17, consultado em 27.Ago.2010.

O desafio era como utilizar uma norma de directrizes ou recomendações para isso e a solução foi criar uma norma de referência que fosse auditável e, consequentemente, certificável, integralmente baseada na ISO 31000, tendo surgido a QSP 31000:2010, que não pode ser comercializada nem distribuída.

Fundamentalmente as recomendações foram transformadas em pontos a auditar e o framework convertido num sistema de gestão de riscos, tendo sido acrescentados os requisitos da documentação e da AI[103]*".*

3.4 *ISO Guide* 73 – Termos e Definições da Gestão de Riscos

A GRN está em constante evolução, mas as tentativas de uma certa padronização para facilitar a vida aos *stakeholders* e a todas as partes interessadas no sentido de adoptarem uma linguagem comum é difícil porque os riscos são próprios de cada organização.

"O ISO Guide 73 Risk Management – Vocabulary, define 29 termos da GRN, agrupados nas seguintes categorias:

- ✓ *Termos básicos;*
- ✓ *Termos relacionados a pessoas ou organizações afectadas por riscos;*
- ✓ *Termos relacionados à avaliação de riscos;*
- ✓ *Termos relacionados ao tratamento e controle de riscos*[104]*".*

A *FERMA* adopta a definição de risco conforme estabelecido na *ISO*/IEC *Guide* 73 – **a combinação da probabilidade de um acontecimento e das suas consequências**[105].

A importância da criação do *ISO Guide* 73 reside no facto de ser fundamental que as organizações possam adoptar conceitos e terminologia, previamente definidos que contribuam para criar finalmente uma linguagem comum nas diferentes áreas, funções e processos relacionadas com a GRN, padronizando assim o que vem a ser uma análise de risco, uma gestão de risco, probabilidade, etc.

[103] http://www.iso31000qsp.org/2010/08/esclarecimento-sobre-certificacao.html, consultado em 1.Set.201.
[104] http://www.csomeeting.com.br/comunidade/entrevistas/612-gestao-de-riscos-pela-norma-asnzs-4360, consultado em 27.Ago.2010.
[105] http://pt.wikipedia.org/wiki/Gerenciamento_de_riscos_do_projeto, consultado em 20.Fev.2010.

Uma das secções ou um dos capítulos da norma, como já vimos, é o capítulo de terminologia e, especificamente essa terminologia empregada na *ISO* 31000 é a própria terminologia definida no *ISO Guide* 73.

Há contudo termos e conceitos definidos no *ISO Guide* 73 que não fazem parte da Norma 31000 já que a proposta da *ISO Guide* 73 é mais abrangente que a da norma, com termos e definições um pouco mais específicos de uma área ou de um sector, mas que para efeito de padronização se considerou para tentar chegar a uma linguagem única e uniforme.

"Exemplo de algumas definições básicas que constam da ISO 31000:2009 e do ISO Guide, 73:2009, já em sua versão oficial em português:

- ✓ ***Política de gestão de riscos**: declaração das intenções e directrizes gerais de uma organização relacionadas com a GRN.*
- ✓ ***Proprietário do risco**: pessoa ou entidade com a responsabilidade e a autoridade para gerir um risco.*
- ✓ ***Atitude perante o risco**: abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do risco.*
- ✓ ***Aversão ao risco**: atitude de afastar-se de riscos*[106]*".*

Gestão de Riscos (3.1.7)				
	Análise e avaliação de Riscos (3.3.1)			
		Análise de riscos (3.3.2)		
			Identificação de fontes (3.3.4)	
			Estimativa de riscos (3.3.5)	
		Avaliação de riscos (3.3.6)		
	Tratamento do risco (3.4.1)			
		Acção de evitar o risco (3.4.6)		
		Optimização do risco (3.4.3)		
		Transferência do risco (3.4.7)		
		Retenção do risco (3.4.9)		
	Aceitação do risco (3.4.10)			
	Comunicação do risco (3.2.4)			

Figura 5 – A Gestão de Riscos Segundo a Norma 31000

Fonte: http://www.abnt.org.br/imagens/Paginas_especiais/ABNT_SP_15999-_3jun2008.pdf

[106] http://www.iso31000qsp.org/search/label/ISO%20Guia%2073%3A2009, consultado em 27.Jun.2010.

3.5 Software de Gestão de Riscos

Para o primeiro curso de *"capacitação em gestão de riscos e auditoria baseada em riscos"*, de acordo com a nova norma *ISO* 31000:2009 o QSP permite a utilização do software *RISK REGISTER - ISO* 31000 durante o treino, para facilitar o desenvolvimento da parte prática do curso, no que se refere à aplicação de métodos e técnicas para utilizarem depois softwares específicos[107].

Por exemplo o *SoftExpert Excellence Suite* oferece ferramentas para a gestão completa dos riscos da organização, em conformidade com a norma *ISO* 31000, garantindo a padronização e a correcta utilização da informação para a obtenção da excelência na gestão dos riscos[108].

> *"Dispõe de um conjunto de módulos multi-idiomas, que automatizam os processos envolvidos nas necessidades de melhoria e optimização das diversas áreas de negócio das organizações, aprimorando a gestão, reduzindo custos e facilitando o atendimento às principais regulamentações internacionais, complementando e optimizando o uso dos sistemas de gestão empresarial, adaptando-se às necessidades específicas do cliente, ao nível de outros ERP's existentes no mercado[109]"*.

A auditoria tem evoluído no sentido de acompanhar a gestão e o foco é agora a GRN do negócio.

Verificando-se que a organização tem uma certa apetência para o risco, é normal partir para a implementação de um processo pró-activo de GRN, que permita antes dos acontecimentos, prever e equacionar a melhor forma de gerir todo o processo e retirar vantagens competitivas que criem valor aos *stakeholders*.

A nova norma *ISO* 31000 não certificável permite aliar as definições de uma correcta GRN, com o apoio do *ISO Guide* 73, sendo uma ferramenta por excelência de ligação entre a gestão e a auditoria. Pretende-se que as organizações de toda a espécie e de todo o mundo possam adoptar de uma vez por todas uma linguagem comum que lhe facilite a vida em termos de GRN do negócio e faça a ponte entre a gestão e a auditoria, simplificando o processo, mas tornando-o ao mesmo tempo altamente eficaz.

[107] http://www.qsp.org.br/capacitacao_gr.shtml, consultado em 20.Jun.2010.
[108] http://www.softexpert.com.br/se-suite.php, consultado em 20.Jul.2010.
[109] http://www.softexpert.com.pt/partnercenter/noticias.php?nid=457, consultado em 26.Ago.2010.

4. Revisão da literatura sobre apetência das Organizações para a Gestão de Riscos de Negócio

Este capítulo apresenta a revisão de literatura sobre o tema, utilizando para o efeito várias opiniões credenciadas de especialistas nestas matérias que falam sobre a aplicabilidade das ferramentas de GRN anteriormente analisadas e de como as organizações estão mais alertadas para a GRN e mais focalizadas para a necessidade da tomada de riscos, como forma de criar valor**.**

Foi o próprio *Donaldson, William* então presidente da *SEC* um ano após a publicação da lei, a declarar que "*eu me preocupo com a perda da tomada de riscos. ... Sarbanes-Oxley desencadeia toneladas de advogados em todo o país… [O resultado é] uma enorme preocupação com os perigos e riscos de fazer o menor erro, ao contrário de uma abordagem razoável para riscos do negócio*[110]*".*

Da mesma forma, em Julho de 2003, o presidente em exercício da Reserva Federal *Greenspan, Alan* afirmou que "*executivos de empresas e conselhos de administração são claros, na sequência do recente foco sobre o comportamento das empresas, como um aumento no risk-taking da sua parte seria visto pelos accionistas e reguladores. Como resultado, as empresas têm sido bastante cautelosas ao falar em realizar novos investimentos de vulto*[111]".

Comentários similares foram ouvidos na comunidade empresarial, especialmente a partir de executivos de empresas em indústrias de alto risco. Por exemplo, em 2004, *Siebel, Tom* ex-CEO da empresa de *software* da *Siebel Systems*, afirmou que "*podemos ter matado a galinha dos ovos de ouro... ao mitigar todos os riscos possíveis que podem ser concebidos. O risco não costumava ser uma coisa má*[112]*…"*

> *Antes do pico da crise de crédito, as empresas financeiras queixaram-se do crescimento "do peso da regulamentação" com que tiveram de lidar, o dinheiro e o tempo gasto para se colocar em conformidade com a mudança dos standards*

[110] Michaels, Adrian, "After a year of U.S. clean-up, William Donaldson calls for a return to risktaking,"FinancialTimes.com, July 24, 2003, traduzido de http://www.trolp.org/main_pgs/issues/v12n2/Terwilliger_Format.pdf, consultado em 19.Jan.2010.
[111] Testimony of Chairman Alan Greenspan before the Committee on Financial Services, U.S. House of Representatives, July 15, 2003, traduzido de http://www.aei.org/docLib/20070615_LehnSOX.pdf, consultado em 13.Dez.2009.
[112] Kontzer, Tony "Siebel Sees Sarbanes-Oxley Taking Toll on Economy," Information Week, October 13, 2004, traduzido de http://www.aei.org/docLib/20070615_LehnSOX.pdf, consultado em 13.Dez.2009.

contabilísticos, as expectativas de governação, e outras exigências regulamentares que estavam fora de controlo, alegaram; foram ficando pelo caminho os seus esforços para gerir uma empresa e obter lucro. Ultimamente, a forma como as pessoas falam sobre regulação mudou, diz *Boyle, Paul* executivo-chefe do *FRC, regulador de contabilidade e governação do RU.*

A escala de custos de cumprimento que os bancos e empresas financeiras foram reclamando *"são totalmente diminuídos à escala da destruição de riquezas e à dimensão do dinheiro dos contribuintes"* que foi gasto apenas para manter o sistema bancário a funcionar. *Como consequência, a discussão sobre se o custo de regulação é justificado mudou fundamentalmente*, argumenta *Boyle*[113]*"*.

Em muitas organizações, a auditoria interna suportou o peso da SOX e do trabalho inicial de cumprimento e, muitas vezes ficou atolada nas várias fases desta lei, incluindo o fluxograma dos processos de negócios, a análise de risco e controlo e a resposta mais óbvia à Sarbanes-Oxley Secção 404 - Os testes de controlo extensivo em nome da administração. Estas são todas as medidas necessárias no processo de Sarbanes-Oxley, mas seis anos mais tarde, alguns escritórios de auditoria ainda estão a realizar testes à gestão, para grande desgosto dos seus CAE's. Esses executivos de auditoria não podem mais esperar para descarregar o ónus da Sarbanes-Oxley e voltar às suas funções tradicionais, como auditorias operacionais, sistemas e auditorias especiais a projectos. No entanto, os CAE's, que olham com carinho para o passado, devem parar por um momento e reconsiderar. As organizações que olham para a Sarbanes-Oxley como uma aberração e desejam voltar aos "bons velhos tempos" estão a perder uma oportunidade de ouro para ter um impacto positivo e influente sobre o ambiente de controlo. Devem pensar sobre as oportunidades que a lei Sarbanes-Oxley pode trazer, mesmo agora, e em como tornar a sua actividade de auditoria mais eficiente, eficaz e valiosa para a organização em geral. Claro, o aconselhamento é uma coisa, a execução outra completamente diferente. Como é que os departamentos de AI fazem o trampolim para a Sarbanes-

[113] Traduzido de Balancing Risk and Opportunity by Neil Baker, artigo inserido na página 42 da Revista Internal Auditor de Abril 2009.

Oxley? Como podem o tempo e os recursos serem confrontados com a actividade de criação de valor?

Para aqueles que procuram respostas, estas lições Sarbanes-Oxley da Chevron Corp, de experiência em AI podem ser instrutivas[114].

O que pode estar a acontecer é que a gestão não quer confrontar o conselho de administração com projectos ou investimentos, incluindo aquisições, novas e caras em despesas de I & D, ou a expansão para novos mercados, que poderiam ser vistos por parte dos administradores independentes como excessivamente arriscados. O resultado é incorrer em menos riscos, e os estudos académicos mostram uma correlação entre o baixo desempenho da empresa e super maiorias de administradores independentes nos conselhos de empresas[115].

Grume, Louis[116]*, argumentou a propósito que "Essas mudanças têm sido controversas. As opiniões variam extensamente sobre a eficácia e o grau de exigência da SOX. Alguns dizem que faz com que as empresas sejam mais avessas ao risco. Outros queixam-se de que prejudica a competitividade global dos mercados americanos. Os custos do cumprimento têm sido muito superiores ao inicialmente previsto. Em particular, os custos para dar cumprimento à SOX - secção 404 de CI sobre a Informação Financeira foram condenados por muitos como injustos, principalmente para organizações menores. Não se iludam, a SOX não é perfeita, nem os seus controlos prescritos necessários para todos os tipos de empresas. Mas hoje, mais de cinco anos após a sua passagem, não pode haver dúvida de que, com a SOX, foi reforçada a responsabilidade das empresas e melhorou significativamente a confiança do público nos grandes negócios e nos mercados de títulos americanos. Embora a SOX possa ter afectado negativamente o lucro de algumas empresas, o melhor argumento em favor da lei trata simplesmente de olhar para o desempenho de nossos mercados financeiros. Entre 30 de Julho de 2002 e 30 de Junho de 2007, a S&P500 aumentou 67%, representando cerca de 4,2 trilião de dólares em valor de mercado.*

[114] Traduzido de Extracting Energy from Sarbanes-Oxley by auditors at Chevron, artigo inserido na página 45 da Revista Internal Auditor de Junho 2008.

[115] Artigo "Is Sarbanes-Oxley Impairing Corporate Risk-Taking?" de *Wallison, Peter J.* publicado em 18 Junho 2007, traduzido de http://www.aei.org/EMStaticPage/1534?page=Summary, consultado em 18.Jan.2010.

[116] Traduzido de http://www.nysscpa.org/cpajournal/2007/1107/perspectives/p7.htm, consultado em 10.Jan.2010.

Wallison,Peter J[117] afirmou a propósito *"Na conferência de hoje, vamos concentrar-nos noutro destes efeitos indesejados e a séria questão de saber se a SOX pode estar a causar um declínio no risk-taking nas empresas de capital aberto. Se assim for, este seria um problema grave para a nossa economia mais a longo prazo"*.

Quase todos os economistas concordam que é de risco a vontade para desenvolver novos produtos e buscar novos mercados, atendendo, entre outros aspectos, aos poderes da concorrência, inovação e crescimento da nossa economia. Se o risco for reduzido na nossa economia, a longo prazo será menor a produção de bens e serviços para todos nós. O estudo que *Lehn, Ken* e seus colegas produziram, torna num forte caso empírico que exista uma correlação entre o advento da *SOX* e um declínio na tomada de riscos por parte das empresas americanas cotadas. *Eu escolhi a palavra "correlação" com cuidado. O facto de poder haver um declínio no risk-taking após a SOX não prova que a SOX causou este declínio. Só muito raramente nas ciências sociais podemos saber por que os eventos ocorrem em oposição ao facto do que eles fazem ocorrer. … Bem, então, qual é a relação entre a SOX e a tomada de risco pelas organizações? E é uma correlação convincente o bastante para nós dizermos de forma plausível que a SOX é uma causa de um declínio no risco empresarial, ou, ao invés da declaração menos favorável que a SOX está associada a um declínio na tomada de risco pela gestão? Acho que há uma relação de causa e efeito, e funciona através dos recentes poderes independentes nos conselhos de administração das empresas cotadas"*.

No artigo *"Did the Sarbanes-Oxley Act Affect Corporate Risk-Taking?"* apresentado por *Litvak, Kate* da *University of Texas School of Law*, são abordadas duas questões importantes e relacionadas:

Primeiro, a *SOX* fez induzir as empresas a reduzir o risco?

Em segundo lugar, que efeito tem a Lei *Sarbanes-Oxley* sobre as empresas estrangeiras cotadas?

A resposta parece ser positiva para ambas, ou pelo menos no caso de empresas estrangeiras cotadas a apetência pelo risco diminuiu após a *SOX*, em função do tipo de empresa e das características de cada país. As conclusões sobre as mudanças dependem um pouco da medida de risco que se adopte. É possível que a *SOX* afecte de diferentes formas o modo pelo qual as

[117] Artigo "Is Sarbanes-Oxley Impairing Corporate Risk-Taking?" de *Wallison, Peter J.* publicado em 18 Junho 2007 traduzido de http://www.aei.org/EMStaticPage/1534?page=Summary, consultado em 18.Jan.2010.

empresas podem reduzir os seus riscos, mas pesquisas futuras poderão trazer à tona as diferenças com maior detalhe[118].

O seu aparecimento tem sido alvo de muitas críticas e entraves por parte das organizações, que vêm neste processo apenas mais uma forma de dificultar a sua vida e gastar recursos que poderiam ser empregues doutra forma.

A questão fundamental tem sido se os benefícios superam os custos, enquanto para outros é vista como uma das mais importantes peças de legislação relacionada com relatórios financeiros e de governação em termos de protecção do interesse dos *stakeholders.* Pela discussão acalorada que trouxe, há já vários estudos publicados sobre o impacto da mesma nas organizações.

No artigo "*Role in the Risk Management"* publicado pela *IIA* (Mar 2011) pode ler-se que "*desde a crise financeira de 2008, as pressões reguladoras e económicas estão a forçar as organizações a fazer um trabalho mais aprofundado na realização de avaliações de risco em toda a empresa, buscar oportunidades estratégicas e eficazes face aos riscos, aumentar a eficácia dos esforços de mitigação de risco, e concentrar-se numa abordagem mais holística da gestão de riscos*".

A pergunta que se põe é: *"Qual é, e qual deveria ser, o papel da AI?"*

Este artigo analisa os dados resultantes de pesquisas realizadas nos últimos dois anos e fornece uma análise sobre:

- ✓ A administração e as comissões de auditoria e de gestão.
- ✓ As actividades de GRN, as actividades que a AI está actualmente a efectuar e aquelas que espera executar nos próximos anos.

Enquanto as pesquisas recentes sobre as comissões de auditoria têm mostrado que a GRN é claramente a sua área, os dados obtidos indicam que não têm grandes expectativas quanto ao que deve ser o seu papel interno. Pouco menos de metade olha para a AI como fornecedora de conselhos sobre GRN e processos, e pouco mais de um quarto pediu à AI para realizar auditorias específicas de componentes da GRN.

[118] Traduzido de http://www.canlecon.org/.../Katherine%20Litvak%20Abstract%20and%20Paper.doc, consultado em 5.Jan.2010.

Três quartos dos entrevistados acreditam que há uma necessidade emergente para as comissões de auditoria de ganharem mais conhecimentos sobre os processos de GRN. É razoável presumir que a falta de consciência geral e de entendimento sobre os resultados da GRN de risco num nível mais baixo de apreciação, como as actividades de AI, podem fornecer ensinamentos significativos e garantia de actividades de gestão em torno do risco.

Também é possível que as comissões de auditoria não percebam que os auditores internos possuem as competências adequadas e experiência para avaliar as actividades de GRN. Curiosamente, há uma falta de dados de pesquisa abordando as expectativas da administração nas actividades de AI.

A maioria das actividades de AI usa um modelo baseado no risco para desenvolver o seu plano de auditoria que considera as solicitações da gestão. Se a comissão de auditoria e a gestão não têm um forte entendimento dos conceitos de GRN, não podem identificar e solicitar projectos adequados relacionados com as áreas de risco emergentes.

As respostas reforçam o facto de que a AI tem e continuará a desempenhar um papel importante na implementação e operação de programas de GRN. No entanto, é surpreendente que apenas 40 por cento actualmente forneça uma garantia independente de GRN e 25 por cento nunca espera fazê-lo, pois a GRN está integrada em *standards*. As percentagens mais baixas para ajudar e aconselhar sobre novas funções de GRN, em separado, destaca o facto de que muitas actividades de AI não estão a fornecer garantia de serviços de consultoria independente e tão frequentemente quanto se poderia esperar.

Estudos recentes identificaram que a AI pode ter um papel ainda menor relacionado com os riscos estratégicos de uma organização. Os riscos estratégicos tendem a ser mais difíceis de identificar e avaliar em auditoria. Como tal, muitas actividades de AI gastam pouco ou nenhum tempo com riscos estratégicos.

Pode parecer intuitivo recomendar que os auditores internos devem aumentar o seu papel na GRN, mas eles só devem fazê-lo se tiverem as competências certas e experiência.

No Relatório II sobre Levantamento de AI do IIA, que incidiu sobre as competências dos auditores internos, 72 por cento citaram "análise de risco e técnicas de avaliação de controlo" como muito importante. Essa competência foi classificada como a segunda mais importante, um pouco atrás de "entender o negócio" (73 por cento), que é um facilitador fundamental para a compreensão do risco em qualquer organização. Da mesma forma, "gestão de risco da

empresa" foi classificada como a área de conhecimento em quinto lugar como mais importante para os auditores internos (58 por cento). Essa pesquisa realizada em mais de 107 países, incluiu mais de 13.500 respostas dos entrevistados, pelo que representa claramente uma visão global das competências mais importantes para os auditores internos.

Dado que a GRN tem sido uma parte importante das normas há mais de uma década, porque é que praticamente todos os auditores internos não têm as competências e experiência nas áreas mencionadas acima?

O estudo permitiu concluir que é necessário um bom entendimento do negócio, bem como dos conceitos de GRN, *frameworks,* etc. Segue-se a competência em áreas de riscos específicos, mas comuns.

Assim, com formação adequada e esforço, não há nenhuma razão para que qualquer auditor interno não possa ser qualificado o suficiente para executar muitas funções de GRN. Segundo se pode ler no artigo "*ISO Standard 31000: Managing Risk - All the Risks*[119]*"a Gestão de risco não se refere a "risco zero", mas a tomada de riscos optimizado!*

Na entrevista a um dos membros do grupo de trabalho que desenvolveu esta nova norma, o Professor *Louisot, Jean-Paul*, que ensina gestão de risco em Paris na *Sorbonne University* afirma que "*precisamos de uma linguagem comum, um diálogo entre todos os actores chave, um método de gestão de risco que estabeleça o contexto de gestão de risco para determinar os objectivos da organização, identificar riscos, analisar a gravidade, a probabilidade, avaliar o nível de controlo de risco, e garantir a conformidade com os requisitos regulamentares e os da organização e seus parceiros, e gerir o risco*".

Ainda segundo este autor a *ISO* 31000 é o padrão de normas, porque ao oferecer alguns princípios, uma estrutura organizacional e uma GRN e processo de melhoria contínua aplicável a todas as actividades empresariais em qualquer país, o *standard* não-certificável *ISO* 31000:2009, acompanhado de um glossário, o *ISO Guide 73,* fornece o contexto a outras normas e melhora a coerência geral entre os 60 padrões *ISO* cobrindo "riscos" que actualmente existem.

> E termina afirmando: *a ISO 31000 fornece a melhor maneira de assegurar um desenvolvimento sustentável para uma organização existente, permite considerar*

[119]Traduzido de http://www.bureauveritas.nl/wps/wcm/connect/bv_com/group/home/news/latest-news/vision+-+standard+31000+managing+risk+- all+the+risks?presentationtemplate=bv_master/news_full_story_presentation, consultado em 18.Ago.2010.

novas oportunidades, a capacidade de lidar com eventos imprevistos, ou transformar um erro numa oportunidade. Os australianos têm vivido há quase 20 anos com gestão de risco padronizada; na Europa não temos uma versão do padrão global. A ISO 31000 deve ser entendida não como um padrão, uma vez que não é certificável, mas sim como um quadro de referência. Prevê o seguinte: uma estrutura organizacional, e um processo, mas fica aquém de uma metodologia adequada para a identificação, análise e avaliação de risco que devem ser oferecidos na futura ISO 31010. No entanto, vai ajudar as organizações a cumprir a sua responsabilidade para com seus stakeholders em termos de comunicação de riscos e consulta.

O desenvolvimento desta norma ocorre ao mesmo tempo, com o surgimento do ERM, nos Estados Unidos, a gestão global e integrada de risco. Desde que a crise financeira começou, o ERM explodiu na Europa e nos Estados Unidos!

No guia prático publicado pela IIA "*Assessing the adequacy of risk management using ISO 31000*", da *IPPF- Practice Guide publicado* em Dez 2010, pode ler-se que "A norma *ISO* 31000 de GRN fornece orientações para a *framework* de GRN aplicável a organizações de qualquer dimensão, como um "*conjunto de componentes que fornecem as bases e a estrutura organizacional para a concepção, execução, acompanhamento, revisão e melhoria contínua de GRN em toda a organização*." A *framework* de GRN, independentemente do nível de formalidade, é inerentemente incorporada na organização global de políticas estratégicas, operacionais e práticas. A *estrutura organizacional* inclui planos, relacionamentos, responsabilidades, recursos, processos e actividades.

O auditor interno deve avaliar se a *framework* leva em consideração e define as responsabilidades de GRN e da estratégia de GRN, e se os elementos da *framework* fornecem a construção de uma força de trabalho inteligente no meio ambiente face ao risco, enquanto permite a assunção de riscos responsáveis e de inovação.

Os quadros devem fornecer a supervisão da governação do *ERM* e devem compreender os elementos-chave do *ERM*, perguntar sobre a GRN, e concordar sobre certas decisões de gestão. Aos *stakeholders* devem ser dadas informações suficientes para compreender a atitude de risco da gestão e da administração, a fim de investir, de acordo com suas tolerâncias para a variação potencial no desempenho. As organizações devem dar a conhecer os níveis de risco

através de relatórios trimestrais e anuais, comunicados de imprensa, chamadas para os investidores, etc.

A administração tem a responsabilidade global de assegurar que os riscos são geridos e que há um sistema adequado de GRN em aplicação. Na prática, a administração vai delegar a operação da estrutura de GRN na equipa de gestão. Pode haver uma função separada com competências e conhecimentos especializados, que coordena e gere projectos e actividades, mas todos na organização desempenham um papel na garantia de sucesso e GRN em toda a empresa, e a responsabilidade principal para identificar e gerir riscos é da gestão.

A aplicação do *ERM* altera-se ao longo do tempo. A atitude face ao risco pode mudar devido a factores internos ou externos, uma vez que as respostas eficazes ao risco podem tornar-se irrelevantes, as actividades de controlo podem tornar-se menos eficazes ou não serem realizadas. As mudanças podem ser provocadas pela chegada de pessoal novo, mudanças na estrutura da entidade, ou introdução de novos processos.

Além disso, os objectivos da entidade, bem como a natureza dos eventos potenciais ou condições que possam afectar a consecução desses objectivos, vão mudar. Assim, a administração precisa de determinar se os componentes *ERM* continuam a ser relevantes e capazes de enfrentar novos riscos.

Os processos *ERM* devem incorporar a avaliação periódica dos riscos e classificações de riscos. Quanto maior for o grau e a eficácia da supervisão contínua, menor a necessidade de haver avaliações separadas. A frequência das avaliações específicas necessárias para a gestão ter uma garantia razoável sobre a eficácia do *ERM* é uma questão de julgamento da administração. Ao fazer essa determinação, deve-se considerar a natureza e o grau de mudanças, a competência e a experiência das pessoas, a implementação de respostas aos riscos e controlos relacionados, a natureza e o significado para o negócio dos riscos que estão a ser geridos e os resultados do curso da supervisão.

A supervisão contínua é recorrente nas actividades operacionais correntes de uma entidade. Pode ser mais eficaz do que avaliações separadas, porque é feita numa base de tempo real, reagindo de forma dinâmica às condições de mudança, e é enraizada na entidade. Os problemas podem, muitas vezes, ser identificados mais rapidamente através de processos de supervisão em curso com avaliações separadas a ocorrer após o facto.

Algumas entidades com actividades de supervisão em curso, podem no entanto realizar uma avaliação separada de *ERM*, ou parte dele. O nível de percepção de objectividade é maior para avaliações separadas do que para a auto-supervisão.

Uma entidade que percebe a necessidade de frequentes avaliações separadas deve concentrar-se em formas de melhorar as suas actividades de supervisão contínuas e portanto, deve concentrar-se em “construir” ao contrário de "acrescentar” no que se refere à supervisão.

A necessidade de garantia surge a partir dos processos de governação de uma organização. A sua origem está na relação entre a administração de uma organização e os seus *stakeholders*. Esta relação de mordomia das posições leva a estabelecer processos de ambos delegarem e limitarem o poder para perseguir a estratégia da organização e direcção de uma forma que melhore as perspectivas para o sucesso da organização a longo prazo. A garantia de processos vai permitir que a administração vigie o exercício desse poder.

A actividade de AI, fornece normalmente uma garantia de todo o processo de GRN, incluindo as actividades de GRN (ambos projectam a eficácia operacional), a gestão desses riscos classificados como "chave" (incluindo a eficácia dos controlos e respostas a esses controlos), a verificação do rigor e fiabilidade das avaliações de risco e comunicação do risco e estado de controlo.

Com a responsabilidade da supervisão e garantia de actividades tradicionalmente a ser partilhada entre as várias partes, incluindo a gestão de linha, os AI’s, especialistas em GRN, e a função de *compliance*, é importante que as actividades de garantia sejam coordenadas para assegurar que os recursos sejam utilizados da forma mais eficiente e eficaz. É comum que as organizações tenham grupos separados a executar diferentes formas de consultoria de GRN, conformidade e garantia de funções de forma independente umas das outras. Sem uma coordenação eficaz e de reporte, o trabalho pode ser duplicado ou os principais riscos podem ser ignorados ou mal avaliados.

Não é incomum numa organização a actividade de AI trabalhar em estreita cooperação com a função de GRN. Algumas organizações não têm uma função formal de GRN e, neste caso, a AI fornece muitas vezes de forma mais extensa, serviços de consultoria de GRN para a organização. A AI pode fornecer consultoria de GRN, desde que certas condições se apliquem:

- ✓ Deve ficar claro que a gestão continua a ser responsável pela GRN. Sempre que a AI consulta a equipa de gestão para estabelecer ou melhorar os processos de GRN, o seu plano de trabalho deve incluir uma estratégia clara e cronograma para a migração da responsabilidade destas actividades para os membros da gestão.
- ✓ A AI não pode dar garantia objectiva em qualquer parte da *framework* de GRN pela qual é responsável. Essa garantia deve ser fornecida por terceiros devidamente qualificados.
- ✓ A natureza de tais serviços prestados à organização deve ser documentada na Carta de AI e ser consistente com as suas outras responsabilidades.
- ✓ Qualquer aconselhamento de consultoria ou desafio (ou apoio) de gestão da decisão não envolve a tomada de decisões próprias da AI na GRN.

Para as áreas de maior risco, onde a administração reconheceu a necessidade de melhorar os controlos, pode haver uma oportunidade para a AI em agregar valor à organização através de actividades de consultoria.

Apesar da consultoria e das actividades de consultoria poderem ser uma parte valiosa de um plano de auditoria, o tópico deste guia prático incide sobre as actividades de garantia que podem ser classificadas em três tipos principais:

- ✓ Garantia sobre o processo de GRN em si;
- ✓ Garantia sobre os riscos significativos e as afirmações da administração;
- ✓ Acompanhamento do *status* do plano de tratamento de riscos.

A garantia no processo de GRN em si pode ser realizada para fornecer uma garantia razoável à gestão e à administração de que o programa de uma organização de GRN é efectivamente projectado, documentado e operacionalizado para atingir os seus objectivos.

Para o tratamento ou controlo de risco em planos de emergência relativos a uma maior exposição, especialmente quando são relativamente mais longos na duração, pode ser apropriado monitorar o desempenho tendo em conta o planeado. No mínimo, esse acompanhamento deve ser projectado para fornecer à gestão uma avaliação do progresso em relação aos padrões e validar o plano de gestão de risco nos relatórios da administração. Além disso, essa supervisão pode avaliar a estrutura organizacional, recursos, prestação de contas, gestão de projectos, etc., e fornecer recomendações e considerações para melhorar a probabilidade de sucesso do planeado.

A entidade responsável deve ser capaz de determinar até que ponto o processo de GRN na sua organização atende às necessidades da organização e adoptou as boas práticas geralmente aceites. A GRN é um componente crítico do sistema de CI, pelo que os processos de gestão deficiente de risco são um indicador de que o sistema de organização de CI pode ser deficiente.

É importante que uma organização obtenha garantias no seu processo de GRN. Essa garantia deve acomodar a possibilidade de o auditor interno não poder ser funcionalmente independente da função de GRN. Neste caso, a garantia pode ser obtida a partir de uma entidade externa.

O modelo de maturidade da abordagem baseia-se na afirmação de que a qualidade de uma organização no processo de GRN deve melhorar com o tempo. Sistemas imaturos de GRN de rendimento com muito pouco retorno para o investimento que foi feito muitas vezes funcionam como uma sobrecarga de conformidade ou uma imposição, mais preocupados com a comunicação de riscos do que com o seu tratamento eficaz. Os processos de GRN são desenvolvidos ao longo do tempo, com um valor acrescentado a ser evidenciado em cada etapa do processo de maturação. Esta abordagem fornece uma avaliação sobre se o processo de organização de GRN está numa curva de maturidade, de modo a que a gestão e a administração possam avaliar se ele considera as necessidades actuais da organização e está a evoluir como esperado.

A extensão da documentação do *ERM* de uma entidade depende da sua dimensão e complexidade. Organizações maiores têm geralmente manuais escritos de políticas, organogramas formais, descrições de funções, instruções, fluxogramas de sistemas de informação, e assim por diante. Organizações menores e menos complexas normalmente têm documentação consideravelmente menos detalhada.

5. Metodologia utilizada - Qual a importância da Gestão de Riscos de Negócio nas Organizações?

Neste quinto capítulo é apresentada a metodologia utilizada para responder à questão inicial do trabalho e que consistiu fundamentalmente num inquérito sobre a aplicabilidade da *ISO* 31000 às empresas do *PSI*20 da EuroNext Lisboa e também às organizações brasileiras ligadas ao QSP.

Em virtude da falta de respostas conclusivas, foi utilizada uma metodologia alternativa que consistiu na análise de três estudos sobre o tema em discussão e que permitiu tirar conclusões para responder à questão inicial deste trabalho.

5.1 Inquérito

Como metodologia inicial para este trabalho foi elaborado o questionário que se encontra em anexo, enviado a empresas do *PSI*20 e ainda para as empresas brasileiras que estão ligadas ao QSP, como resultado da necessidade de obter e tratar dados sobre a apetência das empresas, em face da GRN desenvolvida na organização, de virem a melhorar o processo com a adopção da norma *ISO* 31000.

As empresas portuguesas contactadas foram Altri, Banco Comercial Português, Banco Espírito Santo, Banco Português de Investimento, Banco Internacional do Funchal, Brisa, Cimpor, Edp, Galp, Jerónimo Martins, Mota Engil, Portucel, Portugal Telecom, REN, Semapa, Sonae Indústria e ZON.

E ainda Martifer, Média Capital, Soares da Costa, Teixeira Duarte, *Basf* e *Bayer*.

Das organizações brasileiras foram contactadas a *Abiquim*, *AkzoNobel*, *Cemig*, *Cetip*, *Dow Chemical Company*, *Dowcorning*, *Embraer, SA*, *Evonik Industries*, *Glintt*, *Lanxess*, Ouvidoria, *Petrobras, Petrom*, *Rhodia* e Solvay, SA.

Como foi apresentado no Capítulo III a Norma *ISO* 31000 de 2009 é uma norma geral de GRN, independente da área ou actividade, fornecendo linhas de orientação para a implementação da GRN nas organizações.

Esta norma da *International Organization for Standardization* perspectiva a GRN que, com a evolução dos mercados cada vez mais globalizada, fez da GRN parte essencial da estratégica a adoptar para o negócio, sendo responsabilidade de todas as áreas da organização e parte integrante do processo de tomada de decisão.

Tradicionalmente relacionada com riscos de segurança ocupacional (OHSAS 18001) ou riscos ambientais (*ISO* 14001), a Gestão do Risco abrange actualmente desde as tecnologias de informação, os factores sociais, os factores financeiros até à própria continuidade do negócio.

A ***ISO* 31000 de 2009** é projectada para ajudar as organizações a:

- ✓ Incentivar a gestão proactiva;
- ✓ Melhorar e identificar oportunidades e ameaças;
- ✓ Tomar consciência da necessidade de identificar e tratar os riscos em toda a organização, em termos dos seus pontos fortes e fracos;
- ✓ Melhorar a confiança das partes interessadas e consequentemente da informação;
- ✓ Melhorar a eficácia operacional e a eficiência da gestão;
- ✓ Melhorar a capacidade de resistência organizacional.

O inquérito apresentado no anexo II, foi composto por duas partes:

- ✓ Nota metodológica
- ✓ Inquérito

Na nota metodológica são apresentadas as razões da realização do mesmo.

O inquérito teve como objectivo central uma aproximação à temática da modernização da **GRN**, mais especificamente a adopção da nova ***ISO* 31.000**.

Sendo um tema sobre o qual ainda existe escassez de informação, dado que só recentemente foi publicada no Brasil (Novembro de 2009) e tendo estado em discussão pública no IPQ no início deste ano, configura um interesse acrescido para uma norma em começo de análise e aplicação.

A eleição do universo de empresas cotadas portuguesas e brasileiras será um ponto de partida para a comparação da apetência da sua aplicabilidade num e noutro país.

Neste contexto, a estratégia do inquérito assentou na preocupação de reduzir, dentro do possível, o número de variáveis a considerar e centralizar o questionário na caracterização

dessa apetência e/ou necessidade sentida da utilização de mais uma ferramenta de apoio à gestão de topo na **Gestão dos Riscos de Negócio**.

- ✓ Procurou-se focalizar o inquérito em quatro vertentes:
- ✓ Quais as empresas que não vão, pelo menos a curto prazo, apostar nesta ferramenta de trabalho;
- ✓ Quais as empresas que estão já a procurar acompanhar a sua adopção no mais curto espaço de tempo possível;
- ✓ De entre estas últimas, aquelas que começaram já a agendar e programar a sua adopção; e
- ✓ Finalmente tentar identificar e comparar o tipo de empresas portuguesas e brasileiras que irão adoptar este normativo.

De acordo com os objectivos definidos, as variáveis utilizadas foram fundamentalmente descritivas.

Finalmente o inquérito foi tratado em três bases distintas:

- ✓ **Base empresas portuguesas**: variáveis de caracterização da amostra em face das respostas recebidas, da sua opinião e identificação do número de possíveis projectos de adopção da norma 31.000;
- ✓ **Base empresas brasileiras**: o mesmo tipo de análise;
- ✓ **Estudo comparativo das amostras dos dois países** relativamente a este tema.

Visou-se a compilação posterior das respostas, de forma a tentar encontrar um padrão de comportamento das empresas portuguesas e das organizações brasileiras relativamente a esta nova norma.

As únicas respostas, pela negativa, foram da parte do Banif (a pedir para *"enviar por escrito"*, o que já havia sido feito), o BES (*"iam analisar"*), BPI e EDP *("não respondem a estudantes"*).

Da parte do Brasil, Abiquim *("são associação, não respondem"*), Ouvidoria (idem), Rhodia (enviou email especifico a pedir para reencaminhar mas nunca respondeu).

O facto de não se terem conseguido obter respostas concretas levou a que as expectativas não se concretizassem, pois não foi possível tirar conclusões sobre a importância da GRN, nem sobre o que pensam desta nova ferramenta - a *ISO* 31000.

Quando muito a falta de respostas ou a recusa em responder poderá indiciar um certo desinteresse das organizações relativamente à GRN e também para com a nova norma.

5.2 Metodologia Alternativa

Face ao insucesso descrito no ponto anterior, como metodologia alternativa, e tendo por base a ideia de que, como ficou provado na revisão de literatura, as organizações têm comportamentos diferentes em função da sua apetência para o risco, apresentam-se estudos, nos anexos III, IV e V, respectivamente, realizados sobre a aplicação da lei *SOX*.

O **primeiro estudo** (anexo III) foi publicado no artigo *"Sarbanes-Oxley and Corporate Risk-Taking"*, de *Bargeron, Leonce, Lehn, Kenneth, Zutter, Chad* da *University of Pittsburgh*, apresentado no *the American Enterprise Institute,* em 18 Junho de 2007, que partindo da comparação entre empresas homólogas Americanas e do Reino Unido prova, através de vários indicadores, que os factos estão directamente relacionados, ou seja a apetência ao risco diminuiu por força das exigências da *SOX*.

O estudo apresentado é composto de duas partes:

Em **primeiro lugar** é feita uma análise para verificar se houve mudanças significativas nas diversas medidas de risco para as empresas de capital aberto dos EUA desde a publicação da lei *SOX* em 2002. Para tal foram utilizados dois conjuntos de medidas:

1. Variáveis de base contabilística, para medir o nível e tipos de investimentos efectuados pelas empresas; e
2. Variáveis de base accionista, para determinar a avaliação do mercado a empresas de capital de risco.

Usando como referência uma amostra de empresas do Reino Unido, verifica-se que desde a adopção da *SOX* as empresas:

(i) reduziram significativamente os gastos em I&D,

(ii) reduziram significativamente os seus investimentos, e

(iii) aumentaram significativamente a sua liquidez, o que representa assumir investimentos de baixo risco não operacionais.

Assim, o **comportamento do investimento das empresas dos EUA revela uma redução significativa na tomada de riscos após a aprovação da *SOX*.**

Em **segundo lugar** foram examinados os dados sobre as ofertas públicas iniciais (*IPO's)* nos EUA e no RU para testar se a probabilidade de uma empresa aumentar o capital nos Estados Unidos em comparação com as empresas do RU, após a aprovação da *SOX*, está relacionada com o seu esforço em I&D, servindo este como um indicador para o risco das actividades da empresa. Foi verificado que:

(i) a probabilidade de um *IPO* ser realizado no RU, em vez de o ser nos EUA, aumentou acentuadamente após o *SOX;* e

(ii) quanto maior for a actividade I&D de uma empresa, maior a probabilidade de a empresa passar a recorrer ao mercado de capitais no RU após a *SOX*.

Para este estudo foi utilizada uma amostra constituída por 5.228 empresas de capital aberto que incluía 4.239 empresas dos EUA e 989 empresas do RU, de acordo com a base de dados da *Thomson One Banker*.

A amostra é constituída por pequenas e grandes empresas.

As empresas americanas fazem parte do índice *S&P*500[120].

De forma análoga as empresas do Reino Unido estão incluídas no *FTSE100 Index*[121].

Verifica-se pela análise da **proporção de gastos em I&D dos activos**, que ela é mais elevada para os EUA nos três períodos, mas a diferença diminuiu ao longo do tempo – ver tabela 2, anexo III.

[120] Índice composto por quinhentos activos (acções) qualificados devido ao seu tamanho de mercado, a sua liquidez e a sua representação de grupo industrial. É um índice ponderado de valor de mercado (valor do activo multiplicado pelo número de acções em circulação) com o peso de cada activo no índice proporcional ao seu preço de mercado que inclui a maioria das grandes empresas dos EUA e o seu nome refere-se à empresa de consultadoria financeira *Standard & Poors*., em http://pt.wikipedia.org/wiki/S&P_500, consultado em 18.Dez.2009.

[121] Índice das 102 mais bem capitalizadas empresas britânicas cotadas na Bolsa de Londres. Os dados sobre os preços diários das acções e retornos de acções mensais são calculados a partir do dia e os retornos diários dessas empresas sobre o correspondente retorno do *MSCI World Index - MSCI*, um índice global ponderado pelo valor composto pelas empresas de 24 países. Este índice é um índice de mercado accionista de 1500 stocks mundiais, mantido por *MSCI Inc*., anteriormente *Morgan Stanley Capital International* e é frequentemente utilizado como um referencial comum para o stock de fundos global. O índice inclui um conjunto de acções de todos os mercados desenvolvidos do mundo, tal como definido pela MSCI, inclui títulos de 23 países, mas exclui os stocks das economias emergentes em todo o mundo tornando-o menos do que o nome sugere. Destinado essencialmente a investidores norte-americanos foi complementado com o *MSCI EAFE*, que incluía o resto do mundo, fora dos Estados Unidos e Canadá, tendo em 1987 sido criado o *MSCI All Country World* que combina o universo de mercados desenvolvidos com o dos emergentes in "MSCI World: 40 anos de acções globais", newsletter n.º 427 do ActivoBank7 disponibilizada em 14.Jan.2010, traduzido de http://en.wikipedia.org/wiki/FTSE_100_Index, consultado em 18.Dez.2009.

A proporção de **gastos de capital em activos** também é mais elevada para a amostra dos EUA nos três períodos, mas o rácio diminuiu ao longo do tempo. A diferença nas taxas de lucro através das duas amostras não é significativa para o primeiro pré-período *SOX*, é mais elevada para a amostra do RU no segundo pré-período *SOX*, e é mais elevada para a amostra dos EUA no período pós *SOX*.

Portanto não existe nenhum padrão discernível na rentabilidade relativa das duas amostras ao longo do tempo, sugerindo que o padrão de diferenças em I&D, despesas de capital e investimentos ao longo do tempo estão relacionados com outros factores que não as diferentes taxas de lucro das duas amostras.

O desvio padrão dos retornos das acções, a medida de capital de risco total, é maior para a amostra dos EUA nos três períodos. Os dois componentes do risco de capital, mercado e empresa específica, também são mais elevados para a amostra dos EUA no mesmo período.

Para determinar se a tomada de riscos pelas empresas dos EUA de capital aberto diminuiu após a *SOX*, foram realizados dois conjuntos de testes:

O **primeiro conjunto** examina variáveis contabilísticas base para testar se houve uma mudança significativa no nível e risco de investimentos feitos por empresas dos EUA após a aprovação da *SOX*.

O **segundo conjunto** examina como variáveis base as acções para testar se a avaliação do mercado de capital de risco das empresas dos EUA versus RU mudou significativamente após a *SOX*.

Primeiro consideraram-se três variáveis que descrevem os tipos de activos em que as empresas investem - I&D, gastos de capital e investimentos - antes e depois da adopção da *SOX*. Para cada empresa nas amostras dos EUA e do RU foi calculado o valor médio entre:

(i) a relação de I&D vs gastos em activos,

(ii) a proporção de despesas de capital nos activos, e

(iii) a relação de participações em numerário em activos nos períodos 1995/1997, 1998/2000 e 2003/2006.

A proporção mediana das despesas de I&D em activos diminuiu para ambas as amostras após a *SOX*, mas o declínio foi maior para a amostra dos EUA. O rácio médio de despesas de capital para activos também diminuiu para ambas as amostras antes e depois de *SOX* e, também aqui, a diminuição foi maior para as empresas dos EUA – tabela 3, anexo III.

Os resultados mostram que, ao examinar a amostra completa de empresas dos EUA e do RU, houve uma diminuição estatisticamente significativa em I&D e nas despesas de capital para empresas dos EUA contra os seus homólogos britânicos e um aumento estatisticamente significativo na tesouraria das empresas dos EUA, porque o I&D e as despesas de capital constituem gastos em projectos de risco e tesouraria e representam investimentos não operacionais baixos em activos de risco.

Esta evidência é consistente com a visão de que a *SOX* diminuiu a tomada de riscos por parte das empresas dos EUA.

Para testar as alterações na actividade de tomada de riscos dos variados sectores, a amostra foi dividida em três grupos - as empresas que operam em sectores com alta, moderada e baixa I&D. O aumento médio na tesouraria das empresas dos EUA é maior após a *SOX* que a variação correspondente do dinheiro das participações de empresas do RU para a maioria dos subgrupos.

As três medidas de risco baseadas em acções diminuíram para as empresas dos EUA, em comparação com empresas do RU após a aprovação da *SOX* – ver tabela 5, anexo III.

As acções baseadas nas três medidas de risco em geral diminuíram mais para a amostra dos EUA versus o RU em todos os sectores de actividade. – ver tabela 6, anexo III.

Além de analisar se as medidas da assunção de riscos pelas empresas dos EUA se alteraram significativamente após a *SOX*, foi analisado se as empresas que operam em sectores de maior risco tinham maior probabilidade de aumentarem o seu capital no RU contra os EUA após a *SOX*.

Da mesma forma, a percentagem de *IPO's* de empresas dos EUA com baixa I&D aumentou após a *SOX*. Existe uma enorme diferença antes e depois da *SOX* na percentagem das receitas obtidas pelas empresas de baixo risco nos EUA e no RU. Na medida em que a *SOX* tem abalado a tomada de riscos pelas empresas dos EUA, é possível que o resultado seja que o mercado de *IPO's* dos EUA venha a enfraquecer. Em particular, as empresas de capital não aberto nos Estados Unidos podem optar mais frequentemente por permanecer privadas na era pós *SOX*. A percentagem relativa de *IPO's* do RU aumentou drasticamente, sugerindo que mais empresas dos EUA estão a optar por permanecer privadas em resposta à legislação *SOX*. É possível, no entanto, que a mudança em percentagens relativas não seja devida a uma redução nos *IPO's* dos EUA, mas sim a um aumento no número de *IPO's* do RU perante o

número de *IPO's* dos EUA. O número de *IPO's* nos EUA diminuiu substancialmente no pós-*SOX*, enquanto o número de *IPO's* no RU não é notavelmente diferente dos níveis históricos. Outra possível explicação para o aumento da percentagem relativa de *IPO's* no RU e da redução dos *IPO's* nos EUA, é que a redução na actividade dos *IPO's* dos EUA ocorreu devido a uma recessão no mercado de acções dos EUA, e não devido à *SOX*. A bolsa de mercados do RU não pode ser altamente correlacionada com o mercado de acções dos EUA, pelo contrário, o mercado de acções do RU é altamente correlacionado com o mercado de acções EUA, devendo ganhar força relativa desde que o mercado de acções EUA foi ultrapassando o mercado do RU durante o período pós *SOX*.

Globalmente, os dados resumo discutidos acima, sugerem que a actividade com IPO diminuiu no EUA em relação ao RU desde a SOX, especialmente entre as empresas que operam nas indústrias de alta intensidade em I&D. A probabilidade de uma empresa abrir o capital no RU contra o fazê-lo nos EUA é coerente com o pressuposto de que a SOX teve um efeito inibidor sobre o risco das empresas e as que operam em sectores de baixo risco tem cada vez mais *IPO's* realizados no RU desde *SOX*.

O **segundo estudo** (anexo IV) foi publicado no IIA "*Why Enterprise Risk Management is Vital"*de *Steve G. Sutton,* (Fevereiro 2009), através da investigação feita a empresas que estavam interessadas em aplicar ou manter as exigências da secção 404 da lei *SOX*, foi possível concluir que mesmo em PME, em processos de venda ou fusão com outras empresas, privadas ou que pretendem abrir o capital, quanto maior o foco no *ERM* maior a facilidade de conseguir levar a cabo, ou adaptar-se às exigências que o processo de implementação da referida secção da lei obriga.

Este artigo apresenta ainda a conclusão, em face das empresas escolhidas na amostra, que o envolvimento da alta administração foi fundamental para ditar quais os valores indicados para passar a mensagem aos colaboradores envolvidos em tarefas de conformidade.

Quanto menores e mais flexíveis as organizações e de acordo com uma atitude positiva e uma forte ênfase no cumprimento, por parte da gestão, mais facilmente os quadros envolvidos, em geral, entraram na linha do cumprimento do processo de implementação. Por outro lado, quanto mais processos de controlo automatizados, mais fácil o seu cumprimento, enquanto os controlos mais manuais precisam de ser implementados com maior impacto aparente na cadeia de flexibilidade e desempenho.

De acordo com este estudo o *ERM* foi o principal impulsionador subjacente para facilitar a flexibilidade estratégica das organizações, que por sua vez ajudou a minimizar a dificuldade do processo de conformidade. Com processos *ERM* mais eficazes, uma melhor flexibilidade estratégica foi mantida e conseguido um desempenho mais eficaz.

A disponibilidade e acessibilidade das informações em toda a empresa através das TI's formaram um elo crítico na compreensão da relação entre o *ERM* e o desempenho global organizacional. Foi possível concluir que o ambiente de controlo da organização foi um catalisador fundamental para a relação entre flexibilidade estratégica e processos eficazes de implementação de conformidade da *Sarbanes-Oxley*, e que há também uma preocupação generalizada sobre o impacto dos sistemas de controlo na competitividade das organizações e na sua capacidade de atender às expectativas dos parceiros de negócios para o desempenho da cadeia de valor. Estas questões têm sido motivo de preocupação, ainda maior no caso das PME. De facto, a pesquisa feita com foco especificamente sobre o controlo de gestão e o seu papel na orientação estratégica das organizações, constatou que, quanto mais orientada estrategicamente a organização, mais fortes terão de ser os processos de controlo de gestão necessários para que tais organizações mantenham a sua capacidade de responder às alterações estratégicas do mercado.

Claramente, o objectivo desta lei foi forçar as organizações a desenvolver uma melhor governação e a implementar melhores controlos financeiros, componentes chave do *ERM*, que por sua vez, sendo inicialmente eficaz, parece fundamental para tornar os processos de conformidade mais eficientes e, ao mesmo tempo, reforçar o desempenho, facilitando o cumprimento do preconizado nesta lei.

O **terceiro estudo** (anexo V) também publicado no IIA *"Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-organizational Settings"*, de Shannon W.Anderson, Margaret H. Christ e Karen L. Sedatole (Janeiro 2006), tem como principal contribuição fornecer evidências descritivas dos diferentes tipos de riscos que afectam as empresas que se envolvem em alianças estratégicas e as práticas de controlo de gestão que essas empresas usam para gerir os riscos inerentes. Para isso, foi realizada uma pesquisa online que se baseou em questões relativas à gestão de alianças estratégicas, em geral, bem como questões específicas sobre o tipo de aliança estratégica com que os entrevistados estão mais familiarizados. Usando o *COSO ERM*, forneceram dados que

descrevem os riscos enfrentados quando as organizações operam dentro de cada uma das categorias de aliança: parcerias estratégicas, as parcerias a jusante, parcerias de marketing e parcerias em I&D. Além disso, o estudo integra o quadro das Alavancas de Controlo de *Simons* para fornecer uma base para organizar e entender os tipos de mecanismos de controlo comummente usados pelas empresas para gerir os riscos que surgem como resultado da sua participação nas alianças estratégicas.

As quatro alavancas de controlo identificados por *Simons* são:

1. Crenças em sistemas - normas organizacionais usadas para reforçar os valores fundamentais da empresa,

2. Sistemas de fronteira - a regulamentação sobre o que os parceiros não estão a fazer,

3. Diagnóstico dos sistemas de controlo - sistemas de *feedback* tradicional,

3. Sistemas de controlo interactivos - sistemas de informação formais que permitam à gestão envolver-se regular e pessoalmente nas actividades do parceiro.

Analisaram ainda as correlações entre os riscos de empresas que efectuam alianças estratégicas e as práticas de controlo implementadas para gerir esses riscos.

O estudo inclui evidências descritivas de práticas de controlo utilizadas por três grandes empresas e uma empresa de consultoria nacional especializada em GRN com base em extensas entrevistas.

Foram obtidas evidências preliminares sobre as mudanças para controlar as empresas que têm práticas implementadas para dar resposta à *SOX*, que exige que as mesmas avaliem os riscos e as práticas de CI dos seus parceiros estratégicos.

Os resultados indicam que, enquanto a maioria dos riscos introduzidos por alianças estratégicas não são altamente prováveis, muitos seriam altamente prejudiciais para a empresa se ocorressem.

Além disso, demonstrou-se que as empresas dependem de muitos tipos de mecanismos de controlo para gerir os seus riscos relacionados com o parceiro estratégico.

Especificamente, as empresas tendem a confiar de igual forma em cada uma das quatro alavancas de controlo de *Simons*.

Consistentes com as alavancas de controlo da *framework*, as respostas obtidas para cada tipo de parceiro, indicaram igual dependência em cada um dos quatro tipos de sistemas de controlo.

As empresas procuram um equilíbrio nas suas práticas de controlo com vista a melhorar o ambiente geral de controlo. Utilizando as quatro alavancas, as empresas são capazes de revelar os valores fundamentais, capacitar os seus parceiros estratégicos para a consecução dos objectivos, e incentivar o sucesso a longo prazo. Embora os dados sugiram que as empresas dependem igualmente em cada uma das quatro grandes categorias das Alavancas de Controlo, independentemente do tipo de parceiro, a investigação sugere ainda que o mecanismo de controlo específico utilizado difere e está dependente do tipo de parceiro estratégico, como evidenciado no quadro 10 do anexo V.

Em geral, as empresas depositaram uma confiança moderada em códigos de conduta escritos, independentemente do tipo de aliança estratégica em que estão envolvidos (embora a dependência seja um pouco mais baixa para alianças em I&D). Importante é que todas as empresas indicam uma dependência relativamente alta na confiança entre parceiros, sendo este resultado consistente com a ideia de que a gestão realizada numa aliança estratégica eficaz depende tanto do controlo como da confiança.

Todas as empresas parecem depender significativamente de cláusulas contratuais diferentes. Especificamente, e independentemente do tipo de parceiro estratégico, os entrevistados indicam, em média, maior dependência no contrato, detalhando as condições de pagamento específicas, datas de entrega, etc.

Empresas com parceiros estratégicos no marketing têm uma maior dependência nos termos do contrato sobre a atribuição do direito de propriedade e para abordar a manipulação de falhas para atender os termos do contrato do que outras empresas.

Curiosamente, as empresas com parceiros no marketing indicam uma maior dependência no reporte do que as outras empresas. Além disso, empresas com parceiros a montante e a jusante sabem que eles colocam muito pouca (se houver) dependência no reporte. Também digna de nota é a maior confiança em auditorias periódicas sem aviso prévio por parte das empresas envolvidas em parcerias de I&D, do que noutras empresas, com maior dependência sobre as auditorias periódicas.

Os parceiros de investigação e desenvolvimento indicam menor dependência do processo de revisão formal para a selecção de parceiros estratégicos, especificando os termos do contrato na avaliação de desempenho, e termos do contrato de parceria para a dissolução do que outras empresas.

Empresas com parcerias em marketing parecem estar mais propensas à forma de participação nos lucros das entidades (tais como *joint ventures*) do que as outras empresas. Por outro lado, empresas com parcerias a jusante indicam muito pouca dependência sobre formas de participação nos lucros das entidades. Em vez disso, essas empresas mostram uma maior dependência na prestação de contas para a selecção do parceiro estratégico. Finalmente, as empresas com parcerias estratégicas confiam pouco na composição da equipa de gestão da parceria.

Em conclusão, os entrevistados indicam que estão a fazer um uso significativamente maior de relatórios como um meio de demonstrar que são a chave para os parceiros estratégicos terem práticas adequadas de CI, do que antes da promulgação da *Sarbanes-Oxley*.

Para as empresas com parcerias estratégicas que se expõem ao risco de negócios adicionais, como resultado da parceria, a *SOX*, que exige a realização de uma avaliação anual dos seus sistemas de CI, tem levado muitas empresas a aumentar a fiscalização dos mecanismos de CI dos seus parceiros estratégicos. Vinte e cinco (25) entrevistados *CAE* e 23 consultores responderam à parte *Sarbanes-Oxley* da pesquisa. Cinco dos 25 *CAE*s (20%) trabalham para empresas em que a *SEC* detectou fraquezas na aplicação dos controlos internos no momento deste estudo.

Três dos 23 consultores (13%) indicam que os seus clientes têm declarações arquivadas na *SEC*. Aproximadamente metade dos *CAE*s e 57% dos consultores indicaram que as suas empresas (clientes) têm implementado novos sistemas de controlo sobre os seus parceiros estratégicos como resposta à *Sarbanes-Oxley*.

Os participantes foram inquiridos sobre qual dos seguintes mecanismos de controlo é comummente usado nas empresas que pretendem assegurar o cumprimento da *SOX*:

(i) exercer o direito de auditar as cláusulas contratuais,

(ii) confiar em "procedimentos acordados", reporte e / ou

(iii) contar com os controlos do seu parceiro estratégico.

Como o quadro 11 do anexo V ilustra, a maioria das empresas dependem de mais do que um desses mecanismos de controlo específicos. Além disso, os entrevistados indicaram que aproximadamente 67% das empresas pretendem exercer o seu direito à cláusula de auditoria incluído nos termos iniciais do contrato de parceria. Também foi pedido aos entrevistados para descrever a extensão em que seus parceiros estratégicos estão a exigir a alteração da estrutura de CI existente. Cerca de 29% (12/42) indicam que nenhuma alteração de CI é necessária nas suas empresas por parte dos seus parceiros estratégicos. No entanto, 40% indicam que os seus parceiros as exigem em graus variados.

Finalmente, foi pedido que fosse indicado o nível de confiança da empresa e das empresas parceiras para assegurar que os mecanismos adequados de CI estavam correctamente aplicados. O quadro 12 do anexo V indica que o número de empresas que colocou pouca ou nenhuma confiança no reporte diminuiu como resultado da *Sarbanes-Oxley*. Além disso, o número de empresas que classificaram como moderada a dependência tem aumentado na era pós *SOX* e vários entrevistados (aproximadamente 14%) indicaram que as suas empresas ou clientes agora requerem relatórios de todos os seus parceiros estratégicos.

Em conclusão, este estudo demonstra que as alianças estratégicas oferecem às empresas oportunidades de crescimento e inovação, mas apresentam um desafio único. Essas alianças são inerentemente arriscadas, como evidenciado pela alta incidência no fracasso das alianças. Assim, as empresas que as utilizam têm necessidade de desenvolver e manter novas práticas de controlo de gestão para mitigar de forma efectiva o risco de transaccionar com os seus parceiros estratégicos.

Ao considerar a gestão global da sua rede de alianças estratégicas, os entrevistados indicaram que, no que se refere a:

(i) selecção de risco,

(ii) risco, monitorização e

(iii) identificação de riscos de falhas,

cada um destes itens tem um impacto de moderado a alto nas operações da empresa, sugerindo que o impacto e a probabilidade de cada um é maior do que média.

Além disso, na avaliação dos riscos específicos (como eles se aplicam a um parceiro específico), os entrevistados indicaram que a ocorrência da maioria dos riscos teria um impacto significativo sobre as operações da empresa, embora a probabilidade seja baixa. No

entanto, essas avaliações indicam que uma análise cuidadosa e de avaliação destes riscos é necessária. Usando as alavancas do quadro de controlo, o estudo dividiu e examinou o controlo de empresas para as práticas utilizadas para mitigar os riscos dos parceiros estratégicos. As empresas parecem utilizar os mecanismos de controlo de cada alavanca da mesma forma. Isto indica que as empresas usam uma variedade de mecanismos complementares de controlo para minimizar os riscos com o seu parceiro estratégico. Os dados também sugerem que as empresas contam com altos níveis de confiança entre os parceiros para preservar a aliança e minimizar o receio de comportamentos oportunistas. Além disso, os entrevistados indicam confiança nos termos contratuais para a gestão da parceria estratégica.

Como as alianças estratégicas continuam a ser uma força dominante na comunidade empresarial, a sua efectiva gestão e controlo é crítica. Os auditores internos estão numa posição única, como especialistas em controlo de risco para avaliar as alianças estratégicas antes de sua formação, ao longo de seu ciclo de vida, e aquando da sua dissolução. As *frameworks* de risco, tais como o *COSO ERM*, podem ajudar os auditores internos nestas avaliações.

Por outro lado, a gestão eficaz dos riscos durante todas as fases da parceria estratégica, pode aumentar a sua probabilidade de sucesso e impulsionar a organização para a consecução dos seus objectivos estratégicos.

5.3 A reter

Resumindo os estudos apresentados, devemos reter que:

- ✓ Após a aprovação da *SOX*, o comportamento quanto a decisões de investimento nas empresas dos EUA revela uma redução significativa no que se refere à tomada de riscos;
- ✓ Comparativamente com empresas do RU, verifica-se que as empresas dos EUA, após a *SOX*, e devido ao efeito inibidor desta lei na tomada de riscos, apresentam uma baixa probabilidade de abrir o seu capital;
- ✓ O objectivo desta lei foi impor uma forte governação e controlos financeiros mais apertados, que são aliás os componentes chave do *ERM*, o que combinado com as TI e o envolvimento da alta administração, permite mais facilmente um cumprimento eficaz

das exigências da *SOX*, mesmo em PME, em processos de venda ou fusão com outras empresas;

- ✓ No caso das parcerias foi demonstrado como o *COSO ERM* é importante na GRN para dar cumprimento às exigências desta lei;
- ✓ A gestão deverá, em parceria com a auditoria interna, procurar implementar um processo de GRN que melhor sirva os interesses da organização, pelo que os auditores devem ter competências nessa matéria, tendo-se determinado que o conhecimento do negócio era a mais importante, seguindo-se a análise de risco e a aplicação de técnicas de avaliação dos controlos.

6. Análise empírica - Qual a importância da Gestão de Riscos de Negócio nas Organizações?

Neste sexto e último capítulo é apresentada uma análise empírica dos vários riscos considerados como importantes por todas as organizações presentes actualmente no *PSI*20 da EuroNext Lisboa.

Inicialmente faz-se um resumo, retirado dos relatórios de apresentação das contas, da sua actividade. Segue-se um mapa resumo de todos os riscos contemplados pelas referidas organizações e são retiradas conclusões sobre a importância dos mesmos.

6.1 Organizações presentes no *PSI*20 da EuroNext Lisboa

São as seguintes as organizações que actualmente constituem este índice, a que se segue um resumo extraído dos relatórios de contas do ano de 2011:

- ✓ **Altri** - Empresa de produção papeleira e energética
- ✓ **Banco Comercial Português** - Empresa de finanças e capitalização
- ✓ **Banco Espírito Santo** - Empresa de finanças e investimentos
- ✓ **Banco Português de Investimento** - Empresa de finanças e investimentos
- ✓ **Banif** - Empresa de finanças e investimentos
- ✓ **Brisa** - Empresa concessionária de auto-estradas
- ✓ **EDP** - Empresa de produção e distribuição de electricidade
- ✓ **EDP Renováveis** - Empresa de produção de energias renováveis
- ✓ **Galp** - Empresa petrolífera e de combustíveis
- ✓ **Jerónimo Martins** - Empresa de grande distribuição maioritariamente distribuição alimentar
- ✓ **Mota-Engil** - Empresa de construção civil
- ✓ **Portucel** - Empresa de comercialização de papeis de alta qualidade
- ✓ **Portugal Telecom** - Empresa de telecomunicações e de multimédia
- ✓ **REN** - Empresa de geração e de distribuição de electricidade

- ✓ **Semapa** - Empresa de produção de cimentos
- ✓ **Sonae** - Empresa de indústria de matéria-prima, distribuição e venda de alimentos, administração de centros comerciais, turismo, construção, telecomunicações, transporte e capitais de risco
- ✓ **Sonae Indústria** - Empresa de administração de recursos próprios
- ✓ **Sonaecom** - Empresa de comunicação social, telecomunicações, internet e informática
- ✓ **ZON** - Empresa de distribuição de multimédia

Tendo a sua génese sido o resultado de um processo de reestruturação do Grupo Cofina com o objectivo de agregar numa holding distinta as áreas de actividade industrial, a Altri foi até 1 de Junho de 2008 detentora de interesses nos sectores de Pasta e Papel, bem como nos Aços e Sistemas de armazenagem, data em que procedeu à cisão da actividade de Aços e Sistemas de armazenagem. Esta reestruturação inseriu-se numa lógica de focalização e transparência dos negócios da Altri, visando conferir a cada uma das áreas uma maior visibilidade e percepção de valor pelo mercado.

As principais participações financeiras em que a Altri é maioritária são detidas indirectamente e são as seguintes: Caima – Indústria de Celulose (Constância), produção e comercialização de pasta de papel; Celbi – Celulose da Beira Industrial (Figueira da Foz), produção e comercialização de pasta de papel; Celtejo – Empresa de Celulose do Tejo (Vila Velha de Ródão), produção e comercialização de pasta de papel; Altri Florestal (Constância), unidade gestora de recursos florestais do grupo.

Adicionalmente, com o objectivo de apoiar as suas necessidades energéticas e expandir a sua actividade para um sector considerado interessante do ponto de vista estratégico, o Grupo detém ainda uma participação de 50% no capital da EDP Bioeléctrica[122].

O Conselho de Administração considera que o Grupo se encontra exposto aos riscos normais decorrentes da sua actividade, nomeadamente ao nível das unidades operacionais[123].

[122] Página 8 do Relatório do Conselho de Administração 2011.
[123] Página 35 do Relatório do Conselho de Administração 2011.

27 anos de história, uma história de sucesso encetada, em Junho de 1985, a par e passo com a liberalização e desenvolvimento do sistema financeiro português.

Desde a sua fundação até ao presente, ao longo de mais de um quarto de século, o Banco Comercial Português conseguiu afirmar-se como líder em Portugal, assumindo-se como uma instituição de referência em diversas áreas nos diferentes mercados onde actua, sob a marca Millennium.

Em nome de cada Cliente e de um serviço de excelência, o Millennium bcp aposta na criação de valor através de produtos e serviços bancários e financeiros de referência no sector, pautando-se por elevados padrões de responsabilidade corporativa.

Hoje contamos com mais de 1.700 sucursais e 21.000 Colaboradores em diversas geografias, que dão resposta a 5,4 milhões de clientes espalhados pelo mundo.

Numa conjuntura desafiante, a agenda estratégica do Millennium bcp assenta agora em quatro pilares estratégicos:

- ✓ Manter a integridade e consistência do Grupo, apostando nas operações internacionais como alavancas de internacionalização das empresas portuguesas e criação de valor;
- ✓ Preservar a atractividade do Banco, enquanto projecto privado, tendo o Estado como parceiro temporário de referência;
- ✓ Criar condições para o reembolso do Investimento Público até ao final de 2016 (sem prejuízo do prazo superior de que o Banco dispõe para o efeito), minimizando impactos potencialmente negativos;
- ✓ Capitalizar as vantagens competitivas do Millennium bcp, explorando sinergias, *know how* e capacidades das diversas operações[124].

A Comissão de Risco e a Subcomissão de Acompanhamento do Risco de Crédito têm vindo a reunir-se com uma frequência significativa, para tomar conhecimento e para analisar os reportes que diversas áreas do Banco, em Portugal, são chamadas a produzir, como forma de proporcionar ao Conselho de Administração Executivo (CAE) uma monitorização cada vez mais incisiva da evolução do risco inerente à carteira de crédito.

[124] http://ind.millenniumbcp.pt/pt/Institucional/quemsomos/Pages/historia.aspx, consultado em 6.Set.2012.

À Comissão para as Matérias Financeiras (CMF) são cometidas, designadamente, as matérias de fiscalização da gestão, dos documentos de reporte financeiro e ainda das medidas qualitativas de aperfeiçoamento dos sistemas de controlo interno, da política de gestão de riscos e da política de *compliance*, competindo-lhe ainda supervisionar a actividade de auditoria interna, bem como zelar pela independência do Revisor Oficial de Contas e emitir recomendação sobre a contratação de Auditores Externos, formulação da respectiva proposta de eleição e condições contratuais de prestação de serviços por parte destes e receber as comunicações de irregularidades apresentadas por Accionistas, Colaboradores ou outros, assegurando o seu acompanhamento pela Direcção de Auditoria Interna ou pela Provedoria do Cliente[125].

A Comissão de Risco é responsável por acompanhar os níveis globais de risco (riscos de crédito, de mercado, de liquidez e operacional), assegurando que os mesmos são compatíveis com os objectivos, os recursos financeiros disponíveis e as estratégias aprovadas para o desenvolvimento da actividade do Grupo[126].

BANCO ESPIRITO SANTO

O Banco Espírito Santo, S.A. é um grupo financeiro universal com o seu centro de decisão em Portugal, o que confere ao território nacional o seu mercado privilegiado. Em 31 de Dezembro de 2011, a actividade do Grupo em Portugal representava 74% dos activos totais. Com presença em quatro continentes, actividade em 25 países e mais de 9 800 colaboradores, o Grupo BES é actualmente o maior banco nacional cotado em Portugal por capitalização bolsista (2,0 mil milhões de euros em 31 de Dezembro de 2011) e a segunda maior instituição financeira privada em Portugal em termos de activos (80,2 mil milhões de euros em 31 de Dezembro de 2011)[127].

A Comissão executiva define o apetite de risco através de:

Comité de Risco	Reunião mensal	DRG
Conselho Financeiro e de Crédito	Reunião diária	
ALCO (Assets and Liabilities Committee)	Reunião mensal	

[125] Página 162 do Relatório e contas 2011.
[126] Página 163 do Relatório e contas 2011.
[127] Página 12 do Relatório e contas 2011.

O Departamento de Risco Global - DRG tem como funções principais:

- ✓ Identificar, avaliar e controlar os diferentes tipos de risco assumidos, de forma a permitir a gestão global do risco;
- ✓ Implementar as politicas de risco definidas pela Comissão Executiva, homogeneizando princípios, conceitos e metodologias em todas as unidades do Grupo BES;
- ✓ Contribuir para os objectivos de criação de valor através do aperfeiçoamento de ferramentas de apoio a estruturação, *pricing* e decisão de operações, bem como do desenvolvimento de técnicas de avaliação de performance e de optimização da base de capital;
- ✓ Acompanhar a estratégia de internacionalização do Grupo BES, colaborando no desenho das soluções organizativas e na monitorização e reporte do risco assumido pelas diferentes áreas internacionais[128].

O Grupo BPI – liderado pelo Banco BPI – é um grupo financeiro, multiespecializado, centrado na actividade bancária, dotado de uma oferta completa de serviços e produtos financeiros para os Clientes empresariais, institucionais e particulares.

A actividade do Grupo desenvolve-se principalmente em Portugal, um mercado desenvolvido e concorrencial onde o BPI detém uma forte posição competitiva – a terceira por volume de negócios entre os bancos privados –, e em Angola, uma economia emergente que tem registado um crescimento forte e sustentado ao longo dos últimos anos, onde o BPI, através da participação no BFA, é líder de mercado[129].

A gestão global de riscos do Grupo BPI é da competência global da Comissão Executiva do Conselho de Administração. Ao nível da Comissão Executiva, o pelouro das direcções de risco é atribuído a um Administrador sem responsabilidade directa por direcções comerciais.

Existem ainda, a nível superior, duas comissões executivas especializadas: a Comissão Executiva de Riscos Globais (riscos globais de mercado, liquidez, crédito, país, operacionais)

[128] Página 65 do Relatório e contas 2011.
[129] Página 8 do Relatório e contas 2011.

e a Comissão Executiva de Riscos de Crédito, cuja atenção incide sobre a análise das operações de maior relevo[130].

O Banif - Banco Internacional do Funchal renovou o reconhecimento da qualidade dos produtos e serviços prestados aos Clientes através da certificação dos seus processos pela norma internacional NP EN ISO 9001:2008. Desde 2006, ano em que o Banif obteve as primeiras certificações de qualidade, o Banco tem vindo a garantir a manutenção dos certificados obtidos. Na Certificação de 2010, para além da manutenção dos processos já certificados anteriormente - Banca Electrónica, Banca Telefónica, Provedoria do Cliente, Crédito Habitação, Crédito Pessoal e Atendimento nas Agências - destaca-se a extensão deste reconhecimento ao Atendimento nos Centros de Empresas e Banif Privado, assim como à Conta Gestão Tesouraria[131].

A marca Banif atingiu, durante o ano anterior, um valor (*brand value*) de 174 milhões de dólares. A avaliação, realizada pela *Brand Finance*, volta a colocar o Banif entre as 500 marcas financeiras mais valiosas do mundo. O Banif, que ocupa a 487.ª posição do *ranking*, é uma das cinco Instituições Bancárias Portuguesas a integrar o "Global 500 *Banking Brands Index*"[132].

O Banif dispõe de um modelo interno de avaliação dos seus recursos financeiros disponíveis – Modelo de *Risk Taking Capacity* – que garante a adequação dos níveis de capital e recursos financeiros existentes para fazer face aos riscos actuais e a assumir no futuro, sem afectar a sua solvabilidade, respeitando os objectivos estratégicos definidos.

O modelo existente considera os principais riscos da actividade, dos quais se salienta o risco de crédito, risco de liquidez, risco cambial, risco operacional, sistemas de informação, *compliance* e reputacional[133].

[130] Página 77 do Relatório e contas 2011.
[131] http://www.banif.pt/xsite/Empresas/Institucional/Historia.jsp?CH=4051, consultado em 6.Set.2012.
[132] http://www.banif.pt/xsite/Empresas/Institucional/ClippingdeNoticias.jsp?PID=341799&CH=3743&PCH=null, consultado em 6.Set.2012.
[133] Página 62 do Relatório e contas 2011.

Com 40 anos de actividade, a Brisa Auto-Estradas é uma das maiores operadoras de auto-estradas do mundo e a maior empresa de infraestruturas de transporte em Portugal.

A empresa mãe (Brisa Auto-Estradas de Portugal) detém no seu portfólio um conjunto de activos divididos por quatro áreas de negócio: concessões rodoviárias, serviços de mobilidade, área internacional e outros negócios de infraestruturas de transporte.

Em Portugal, a Brisa Auto-Estradas detém seis concessões rodoviárias – Concessão Brisa (BCR), Atlântico, Brisal, Douro Litoral, Baixo Tejo e Litoral Oeste –, que integram 17 autoestradas e totalizam 1 678 km. A Concessão Brisa destaca-se por abranger um total de 1 124,0 km, distribuídos por 12 auto-estradas que cobrem o país de Norte a Sul e de Leste a Oeste[134].

O Grupo Brisa, à semelhança da generalidade das empresas, encontra-se exposto a um conjunto de riscos financeiros que resultam da sua actividade.

Todas as operações de gestão de risco financeiro, nomeadamente as que envolvem a utilização de instrumentos financeiros derivados são submetidas à aprovação prévia do Administrador Financeiro ou da Comissão Executiva[135].

A **EDP – ENERGIAS DE PORTUGAL, S.A.** é uma sociedade emitente de acções que se encontram admitidas à negociação no mercado regulamentado da NYSE *Euronext Lisbon* (denominado *Eurolist by NYSE Euronext Lisbon*). A EDP está estabelecida em Portugal, organizada sob as leis de Portugal e registada no Registo Comercial de Lisboa, sob o n º. 500.697.256. A sede social está situada na Praça Marquês de Pombal, nº. 12, 1250-162 Lisboa, Portugal.

[134] Página 3 do Relatório e contas 2011.
[135] Página 148 do Relatório e contas 2011.

A EDP foi inicialmente constituída como uma empresa pública, em 1976, nos termos do Decreto-Lei n º. 502/76, de 30 de Junho, como resultado da nacionalização e fusão das principais empresas Portuguesas do sector da electricidade em Portugal continental.

Posteriormente, a EDP foi transformada numa sociedade de responsabilidade limitada (sociedade anónima) nos termos do Decreto-Lei n. º. 7/91, de 8 de Janeiro, e do Decreto-Lei n.º. 78-A/97, de 07 de Abril[136].

A auditoria interna no Grupo EDP é uma função corporativa e é exercida pela Direcção de Auditoria Interna, que depende do Presidente do Conselho de Administração Executivo, sendo supervisionada pela Comissão para as Matérias Financeiras / Comissão de Auditoria, à qual comunica o exercício das actividades da auditoria interna do Grupo.

O Grupo EDP incorporou na sua gestão o sistema de controlo interno, formalizado através do SCIRF - Sistema de Controlo Interno do Relato Financeiro, desenhado com base nas melhores práticas internacionais e nos modelos de referência COSO e COBIT.

Tendo como objectivo garantir a manutenção de mecanismos e procedimentos de controlo que mitiguem o risco de fraude e de ocorrências e erros materialmente relevantes nas demonstrações financeiras, tem formalizado um modelo de responsabilidades, que define as actividades que compõem o ciclo SCIRF, os responsáveis que nele participam a nível corporativo, unidades empresarias e de negócio e a definição de responsabilidades aos diversos níveis da organização.[137].

A diversidade das linhas de negócio do Grupo continuou a assegurar um nível de risco intrínseco baixo, principalmente devido:

- ✓ ao elevado peso relativo dos negócios regulados,
- ✓ ao crescimento em actividades de baixo risco, nomeadamente produção eólica com reduzida exposição a preços de mercado de electricidade,
- ✓ à aplicação de políticas de *hedging* adequadas a promover a mitigação dos riscos financeiros, de combustíveis e de preço e volume de electricidade colocada ou comprada em mercado, e ainda

[136] Página 6 do Relatório e contas 2011.
[137] Página 128 do Relatório e contas 2011.

- ✓ a um aumento da diversificação geográfica do risco com uma diminuição do peso de Portugal[138].

A EDPR está empenhada em melhorar de forma continuada o seu desempenho em Sustentabilidade, tal como é destacado na sua Visão e Missão, como forma de criar valor para os seus accionistas e para a sociedade. Como um dos principais agentes no sector das energias renováveis, a EDPR desempenha um papel essencial dentro do Grupo EDP, líder mundial em 2011 nos Índices *Dow Jones* de Sustentabilidade, entre as empresas do sector energético.

A EDPR está assim uma vez mais empenhada em seguir as diretrizes G3.1 da *Global Reporting Initiative* (GRI) no que diz respeito aos relatórios de sustentabilidade[139].

A gestão de risco é aprovada pela Equipa de Gestão, apoiada directamente pelo Comité de Gestão de Risco e posta em prática por todos os gestores da empresa. Este processo integrado garante a identificação e priorização de riscos críticos, o desenvolvimento de estratégias de gestão de risco adequadas e a implementação de controlos para assegurar o alinhamento da exposição da EDPR de acordo com o perfil de risco definido pela empresa[140].

A Galp Energia é um operador integrado de energia cujas diversas actividades em vários países, no sector do petróleo e do gás natural, se encontram em fase de forte desenvolvimento e expansão. As actividades de refinação e distribuição de produtos petrolíferos e de gás natural estão centradas na Península Ibérica.

A Galp Energia tem também uma presença forte no eixo de Exploração & Produção do Atlântico Sul, que inclui o pré-sal da bacia de Santos, no Brasil, e o *offshore* angolano. Na África Oriental, nomeadamente no *offshore* moçambicano, onde foram recentemente

[138] Página 129 do Relatório e contas 2011.
[139] Página 4 do Relatório e contas 2011.
[140] Página 61 do Relatório e contas 2011.

descobertos importantes reservatórios de gás natural, a Galp Energia tem igualmente uma posição relevante[141].

A comissão executiva, auxiliada por várias entidades internas, é responsável por instituir, no grupo Galp Energia, um mecanismo de identificação e avaliação dos riscos internos e externos que podem afetar o desempenho da Empresa.

A Galp Energia tem promovido a sistematização da avaliação dos riscos e dos sistemas de controlo interno nas diferentes unidades de negócio. Estas iniciativas abrangem os riscos identificados por cada unidade de negócio, que também é responsável pela sua gestão[142].

JERÓNIMO MARTINS

O Grupo detém um portefólio de negócios focado na área alimentar, que conjuga o crescimento da Biedronka na Polónia com a força das posições de mercado das operações de Retalho e Grosso em Portugal e com a maturidade e rentabilidade dos activos industriais da parceria com a Unilever, também em Portugal[143].

A sociedade e, em particular, o seu Conselho de Administração, dedicam grande atenção aos riscos subjacentes aos seus negócios e objectivos. O sucesso nesta área depende da capacidade para identificar, compreender e tratar as exposições a eventos que, estejam ou não sob o controlo directo da equipa de gestão, podem afectar materialmente os activos físicos, financeiros e/ou organizacionais da Sociedade. A Política de Gestão de Risco do Grupo formaliza esta preocupação ao procurar estimular ou reforçar o tipo de comportamentos necessários a esse sucesso[144].

MOTA-ENGIL, SGPS, S.A.

O Grupo Mota-Engil encontra-se estruturado em 3 grandes áreas de negócio: Engenharia e Construção, Ambiente e Serviços e Concessões de Transportes.

[141] Página 4 do Relatório e contas 2011.
[142] Página 57 do Relatório e contas 2011.
[143] Página 13 do Relatório e contas 2011.
[144] Página 232 do Relatório e contas 2011.

Através da sua participada MARTIFER, onde detém uma importante posição societária e com quem mantém uma parceria estratégica, actua ainda no sector da Indústria e Energia.

Desenvolve ainda um conjunto de actividades na área do Turismo nos sectores do desporto e lazer e hotelaria e restauração.

O Grupo Mota-Engil tem vindo a internacionalizar a sua actividade nos últimos anos. Para além de uma presença histórica em Angola, onde se manteve desde sempre acompanhando e apoiando o processo de desenvolvimento do país, o Grupo Mota-Engil opera ainda nos restantes territórios africanos de expressão portuguesa[145].

A Gestão de Risco tem como objectivo central a criação de valor, através de processos de gestão e controlo das incertezas e ameaças que podem atingir o Grupo e as suas participadas, estando subjacente uma perspectiva de continuidade das operações no longo prazo.

A exposição ao risco por parte de qualquer participada do Grupo Mota-Engil deverá estar sempre subordinada à sua estratégia e ser limitada e acessória à actividade de cada empresa, para que se prossigam e atinjam os objectivos traçados nas diversas áreas de negócio[146].

O processo de Gestão de Risco é da responsabilidade de cada uma das administrações das áreas de negócio do Grupo, concretizando-se genericamente num conjunto sequencial de etapas ou fases que se repetem ciclicamente[147].

grupo Portucel Soporcel

Com uma posição de grande relevo no mercado internacional de papel e de pasta e papel, o Grupo Portucel Soporcel é hoje líder na Europa na produção de papéis de escritório de elevada qualidade, posição conquistada com o arranque da nova fábrica de Setúbal[148].

As actividades do Grupo estão expostas a uma variedade de factores de riscos financeiros: risco cambial, risco de taxa de juro, risco de crédito e risco de liquidez.

[145] http://www.mota-engil.pt/AreaDetail.aspx?contentId=88&Language=1, consultado em 15.Set.2012.
[146] Página 49 do Relatório e contas 2011.
[147] Página 50 do Relatório e contas 2011.
[148] http://www.portucelsoporcel.com/pt/group/index.php , consultado em 20.Set.2012.

O Grupo mantém um programa de gestão do risco, focado na análise dos mercados financeiros, procurando minimizar os potenciais efeitos adversos no seu desempenho financeiro[149].

A PT é um operador global de telecomunicações líder a nível nacional em todos os segmentos em que actua e oferece, de forma global e integrada, os seus serviços, produtos e soluções a um universo que ultrapassa os 93 milhões de clientes.

Assume-se como a entidade empresarial portuguesa com maior projecção nacional e internacional, estando presente nos continentes europeu, americano, asiático e africano.

Dispõe de um portfólio de negócios diversificado, em que a qualidade e inovação constituem aspectos determinantes, estando ao nível das mais avançadas empresas internacionais do sector.

Destaca-se no plano internacional a actuação no mercado brasileiro, ao qual a Empresa tem dedicado uma parte significativa dos seus investimentos[150].

A Gestão de Riscos é promovida pela Comissão Executiva em articulação com as equipas de gestão dos vários negócios, a nível nacional e internacional, de forma a identificar, avaliar e gerir as incertezas e ameaças que possam afectar a prossecução do plano e objectivos estratégicos. Importa igualmente referir que todo o processo é acompanhado e supervisionado pela Comissão de Auditoria, órgão de fiscalização autónomo composto por membros não executivos independentes[151].

Por onde passa toda a energia que nos traz conforto e que faz crescer o país. Uma rede que garante o fornecimento de electricidade e gás natural a 10 milhões de habitantes. Que contribui para o desenvolvimento das pequenas e grandes empresas com rigor, experiência e segurança.

[149] Página 23 do Relatório e contas 2011.
[150] Página 20 do Relatório do Governo da Sociedade.
[151] Página 112 do Relatório e contas 2011.

Uma rede atenta ao que a rodeia, ao ambiente e às energias renováveis, centrada em oferecer um futuro melhor e mais sustentável para todos[152].

O Gabinete de Auditoria Interna (GAI) tem como missão verificar a existência, o funcionamento e a eficácia do modelo de controlo dos riscos de gestão e dos sistemas de controlo interno e de governação do Grupo, através de um acompanhamento objectivo, independente e sistemático. Reporta funcionalmente à Comissão de Auditoria, sem prejuízo da sua relação hierárquica com a administração executiva da Sociedade[153].

A Semapa é um dos maiores grupos industriais portugueses com mais de 5.000 colaboradores e presença em 5 continentes, com mais de 3/4 do seu volume de negócios gerados no mercado externo. Tem como actividade a gestão de participações organizadas em 3 áreas de negócio de cariz industrial - Papel e pasta de papel, Cimentos e derivados e Ambiente, Controlando os Grupos Portucel (78%), Secil (51%) e ETSA (96%)[154].

O Grupo Semapa tem um programa de gestão de risco que concentra a sua análise nos mercados financeiros com vista a minimizar os potenciais efeitos adversos na performance financeira do Grupo Semapa. A gestão do risco é conduzida pela Direcção Financeira da *holding* e dos principais subgrupos de acordo com políticas aprovadas pelas respectivas Administrações. Existe ainda junto da Semapa uma Comissão de Controlo Interno com funções específicas na área do controlo de riscos da actividade da sociedade.[155]

A carteira de negócios da Sonaecom compreende fundamentalmente duas unidades de negócio: a Optimus, cuja ambição é tornar-se no melhor operador integrado de telecomunicações em Portugal; e a área de *Software* e Sistemas de Informação (SSI). As mais-valias da Sonaecom decorrem da ambição, da inovação, das capacidades de *marketing* e de execução, qualidades que operam em conjunto com a

[152] Página 2 do Relatório e contas 2011.
[153] Página 87 do Relatório e contas 2011.
[154] Página 14 do Relatório e contas 2011.
[155] Página 155 do Relatório e contas 2011.

infraestrutura de telecomunicações, bem como com a capacidade de compreender e superar as expectativas dos clientes[156].

A Sonaecom está empenhada em desenvolver e implementar as melhores praticas no que diz respeito à gestão e ao controlo de risco, dado que estas áreas são consideradas como as bases fundamentais da estratégia da empresa, apoiada num sistema sólido de Governo da Sociedade. A empresa implementou um sistema que coloca a responsabilidade do controlo interno e gestão de risco nas áreas funcionais de cada negócio, apoiadas pela equipa de Gestão do Risco, em conjunto com a equipa de Auditoria Interna, os Auditores Externos e a equipa de Planeamento e Controlo de Gestão[157].

A Sonae Indústria é uma das maiores empresas industriais do sector dos derivados de madeira do mundo. A sua gama de produtos abrange, nomeadamente aglomerado de partículas de madeira (*particleboard*), MDF (*Medium Density Fibreboard*), aglomerado de fibras duro (*Hardboard*), OSB (*Oriented Strand Board*), produtos e serviços de valor acrescentado - componentes, soluções e sistemas - para as indústrias de mobiliário, construção, decoração e para o sector de bricolage e ainda laminados decorativos de alta pressão e produtos químicos (formaldeído, resinas à base de formaldeído e papeis impregnados)158.

A Sonae Indústria enfrenta uma diversidade de riscos, internos e externos, os quais têm de ser avaliados, estando por isso implantada uma cultura de prevenção e de detecção preventiva, tendo sido concebido um sistema integrado de gestão transversal de risco (*Enterprise-Wide Risk Management Framework*), o qual é mantido devidamente actualizado[159].

A ZON Multimédia é um grupo empresarial que integra o principal índice bolsista nacional, o *PSI*-20. Lidera o mercado de *pay* TV em Portugal e é o segundo

[156] Página 6 do Relatório e contas 2011.
[157] Página 130 do Relatório e contas 2011.
[158] http://www.sonaeindustria.com/page.php?ctx=2,0,17, consultado em 18.Set.2012.
[159] Página 48 do Relatório do Governo da Sociedade

maior Internet *provider*. À escala nacional, é também líder no mercado de exibição cinematográfica.

As origens e desenvolvimento da ZON confundem-se com a génese e o desenvolvimento das indústrias do entretenimento e das telecomunicações de massas em Portugal[160].

As actividades do grupo ZON estão expostas a uma variedade de factores de risco financeiro, de crédito, de liquidez e de mercado.

Desde o *spin-off* do Grupo PT em Novembro de 2007, o Conselho de Administração da ZON passou a ser o responsável por definir os princípios para a gestão dos riscos e a políticas que cobrem áreas específicas como o risco da taxa de câmbio, da taxa de juro, de crédito, do uso de derivados e outros instrumentos financeiros não derivados, bem como o investimento do excesso de liquidez[161].

6.2 Principais riscos considerados pelas organizações do *PSI*20

Nas páginas seguintes são apresentados os principais riscos considerados no capítulo de gestão de riscos que faz parte integrante do relatório e contas destas organizações.

Para a **ALTRI** é importante o risco de variabilidade nos preços dos *commodities* (pasta de papel)[162] e os riscos relacionados com a gestão florestal de 85.000 hectares e a produção do eucalipto que representa 79% desse património através da Altri Florestal[163].

No **BCP** nos riscos de mercado estão incluídos como subcategorias a carteira de negociação, o risco da taxa de juro e das acções na carteira bancária e o risco imobiliário[164].

Contudo o risco de taxa de juro é o de maior peso representando 16,5% em Dezembro de 2011. O risco de acções e imobiliário têm um peso semelhante, 7,2% e 7,5%, respectivamente.

No **BES** os riscos de mercado incluem o risco da taxa de juro, o risco cambial, o risco de acções, o risco de volatilidade e o risco de *spread* de crédito[165].

[160] http://www.zon.pt/institucional/PT/sobre-a-zon/Historia/Paginas/historia.aspx, consultado em 18.Set.2012.
[161] Página 201 do Relatório e contas 2011.
[162] Página 36 do Relatório do Conselho de Administração 2011.
[163] Página 37 do Relatório do Conselho de Administração 2011.
[164] Página 166 do Relatório e contas de 2011.
[165] Página 76 do Relatório e contas de 2011.

São medidos através da estimação das perdas potenciais em condições adversas de mercado, utilizando a metodologia *Value at Risk* (VaR), complementada com *Stress Testing* para avaliar possíveis perdas potenciais[166].

No **BPI** o risco de mercado ou de preço inclui taxas de juro, taxas de câmbio, preço das acções, preço das mercadorias e outros[167], a cargo da Comissão de Riscos Financeiros.

O risco país é muito semelhante ao risco de contraparte e está associado a alterações de natureza económica ou financeira nos locais onde operam as contrapartes.

A lista dos países onde é autorizada a exposição a este risco é aprovada pela Comissão Executiva do Conselho de Administração[168].

No **BANIF** o risco de mercado inclui análise de sensibilidade à taxa de juro e à taxa de câmbio e aos riscos de preços[169].

No âmbito da melhoria da função de gestão de riscos são incluídas outras tipologias menos tradicionais como os riscos de reputação e de estratégia[170].

Na **BRISA** a gestão de riscos financeiros engloba o risco de taxa de juro, o risco cambial, o risco de crédito, o risco de contraparte e o risco de liquidez[171].

Na **EDP** a gestão de riscos é feita ao longo da cadeia de valor na produção de electricidade e gestão de energia, na comercialização em mercado, e de último recurso ou do serviço universal com tarifas reguladas, na distribuição de electricidade, noutras geografias e actividades e de riscos transversais[172].

Na **GALP** a gestão de riscos divide-se em riscos de mercado, riscos operacionais que incluem riscos de não conclusão de projectos ou não desenvolvimento de reservas e da dependência de terceiros, os riscos de conformidade e os riscos financeiros[173].

Na **Jerónimo Martins** a gestão dos principais riscos inclui os riscos estratégicos, os riscos operacionais e os riscos financeiros. A gestão do risco de capital tem em vista manter um nível

[166] Página 75 do Relaório e contas de 2011.
[167] Página 88 do Relatório e contas de 2011.
[168] Página 87 do Relatório e contas de 2011.
[169] Página 73/75 do Relatório e contas de 2011.
[170] Página 81 do Relatório e contas de 2011.
[171] Página 148 do Relatório e contas de 2011.
[172] Página 129 do Relatório e contas de 2011.
[173] Página 53 do Relatório e contas de 2011.

adequado de capitais próprios que lhe permita assegurar a continuidade e o desenvolvimento da sua actividade[174].

Na **Mota Engil** a gestão de riscos financeiros inclui riscos da taxa de juro, cambial, de transacção e de conversão, de liquidez e crédito.[175].

Na **Portucel** são considerados riscos específicos dos sectores de actividade em que o grupo está presente como o sector florestal, produção e comercialização de *BEKP* e de papel *UWF* e de energia[176].

Na **PT** a gestão de riscos relevantes inclui os riscos da envolvente, financeiros e riscos das operações[177].

Na **REN** apenas são considerados os riscos financeiros e de capital[178].

Na **Semapa** os factores de risco operacional incluem os riscos associados ao segmento da pasta e do papel, ao segmento do cimento e derivados e ao segmento ambiente[179].

Na **Sonae** são considerados riscos económicos, relacionados com a envolvente do negócio, estratégia, operações, tecnologia e processamento de informação, e*mpowerment* e integridade[180].

Na **ZON** compete ao Conselho de Administração a definição dos princípios para a gestão dos riscos e as políticas que cobrem áreas específicas[181].

Consideram que as actividades do grupo estão expostas a uma variedade de factores de risco financeiro: risco de crédito, risco de liquidez e risco de mercado[182].

[174] Página 158/164 do Relatório e contas de 2011.
[175] Página 51 do Relatório e contas de 2011.
[176] Página 23 das Notas às Demonstrações Financeiras Consolidadas 2011.
[177] Página 112 do Relatório e contas de 2011.
[178] Página 334 do Relatório e contas de 2011.
[179] Página 160 do Anexo às Demonstrações Financeiras Consolidadas 2011.
[180] Página 134 do Relatório e contas de 2011.
[181] Página 135 do Relatório e contas de 2011.
[182] Página 201 do Relatório e contas de 2011.

Riscos	ALTRI	BCP	BES	BPI	BANIF	BRISA	EDP	GALP	Jer Mart	Mota Engil.	PORTUCEL	PT	REN	SEMAPA	SONAE	ZON
Risco de crédito	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Risco de mercado	■	■	■	■	■			■	■							■
Risco operacional		■	■	■	■		■	■	■					■	■	
Risco ambiental e social			■				■	■	■		■	■		■		
Risco país				■												
Risco de liquidez	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Riscos legais				■			■		■		■			■	■	
Risco fundo pensões/plano reformas		■		■				■								
Risco de negócio e estratégico Continuidade do negócio		■		■							■				■	
Risco regulação/regulatório	■						■	■	■			■	■		■	

Riscos	ALTRI	BCP	BES	BPI	BANIF	BRISA	EDP	GALP	Jer Mart	Mota Engil.	PORTUCEL	PT	REN	SEMAPA	SONAE	ZON
Risco concorrência									■		■	■		■	■	
Risco parcerias tecnológicas Inovação tecnologica									■			■		■	■	
Risco envolvente económica												■		■		
Risco taxas de câmbio	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Risco taxas de juro	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Riscos economicos															■	
Risco obtenção e retenção talento Recursos humanos							■	■			■	■		■		
Risco preço	■				■		■	■	■		■		■	■		
Risco volume							■									
Risco segurança física e de pessoas								■	■							

Riscos	ALTRI	BCP	BES	BPI	BANIF	BRISA	EDP	GALP	Jer Mart	Mota Engil.	PORTUCEL	PT	REN	SEMAPA	SONAE	ZON
Risco sistemas de informação																
Risco florestal																
Risco de conformidade																
Risco de capacidade infraestrutura																
Risco financeiro																
Risco de Fraude																
Risco sobre ética e transparência																
Risco de segurança alimentar																
Risco de contraparte																
Risco de capital																

Verifica-se assim que todas estas organizações contemplam riscos como o risco de crédito e de liquidez, o risco de taxa de juro e taxa de câmbio.

Há porém alguns riscos que são específicos.

Na **ALTRI** o risco florestal é específico da sua actividade e procura a optimização dos recursos disponíveis salvaguardando o ambiente e os valores ecológicos do seu património[183].

No **BCP** o controlo de risco de liquidez inclui um plano de contingência de capital e liquidez PCCL para fazer face a uma possível situação de contingência de liquidez[184].

O risco do Fundo de Pensões decorre da desvalorização potencial dos activos desse fundo e está a cargo da Subcomissão de Risco do Fundo de Pensões.

O risco de negócio e estratégico está relacionado com os impactos negativos nos resultados e/ou capital, sendo a variação da cotação da acção BCP um indicador relevante para a medição deste tipo de risco[185]

O **BPI** é o único do sector financeiro a considerar o risco país, por análise de risco país individual com recurso a *ratings* e análises externas[186].

Na **Brisa** destaca-se o risco de contraparte a que as aplicações de excedentes financeiros e com instrumentos financeiros derivados expõem o grupo[187].

A **EDP** considera o risco volume que está relacionado com a migração de clientes para o mercado livre e com as condições climatéricas e económicas e que faz variar o volume de energia a vender a clientes finais[188].

Relativamente à sua gestão de riscos transversais consideram o risco associado ao investimento para acompanhar e monitorar os riscos operacionais e o seu potencial impacto no valor esperado[189].

A **GALP** tem na sua gestão de riscos os riscos de conformidade relacionados com possíveis alterações de impostos e tarifas a que está sujeita ou das políticas e regulamentos em vigor nos países onde opera e obrigações de responsabilidade empresarial[190].

[183] Página 37 do Relatório do Conselho de Administração 2011.
[184] Página 183 do Relatório e contas de 2011.
[185] Página 184 do Relatório e contas de 2011.
[186] Página 87 do Relatório e contas de 2011.
[187] Página 150 do Relatório e contas de 2011.
[188] Página 133 do Relatório e contas de 2011.
[189] Página 134 do Relatório e contas de 2011.
[190] Página 54 do Relatório e contas de 2011.

Da mesma forma na **REN** podemos destacar os riscos de actividade regulada que está relacionado com os ganhos registados em cada exercício de acordo com o considerado pelo regulador ERSE ao definir as tarifas reguladas para o sector de electricidade e gás.

A gestão do risco de capital utiliza um conceito mais amplo do que o capital próprio para manter uma estrutura financeira optimizada[191].

Na **Jerónimo Martins** procuram manter um nível de capitais próprios adequado à continuação e desenvolvimento da sua actividade[192].

Esta organização também dá muita importância aos riscos de segurança alimentar a cargo das direcções de qualidade e segurança alimentar das diferentes companhias do grupo[193].

Na **Mota-Engil** a gestão do capital humano do grupo tem por objectivo efectuar uma gestão global das pessoas, promovendo a internacionalização e a mobilidade dos quadros, cultivar a meritocracia e fomentar uma cultura homogénea e partilhada[194].

Na **PT** é de salientar o risco de capacidade infra-estrutura cuja gestão lhe permite assegurar uma prestação de serviços com qualidade apesar das avarias e incidentes próprios da sua actividade[195].

A capacidade da empresa obter e reter talento é um risco a cargo da Direcção de Recursos Humanos, cuja importância tem vindo a aumentar[196].

A **Semapa**[197] e a **Portucel**[198] também consideram este último tipo de risco mas está incluído nos riscos associados ao grupo em geral – recursos humanos.

Na **Sonae**[199] e na **Jerónimo Martins**[200] destacam-se os riscos de sistemas de informação pois são empresas com grande utilização de tecnologia, media e telecomunicações.

Na Sonae destaque para o risco de fraude de clientes e de terceiros que é um risco comum no sector das telecomunicações. Na Sonae existe mesmo um Comité de Segurança da Informação[201].

[191] Página 337 do Relatório e contas de 2011.
[192] Página 164 do Relatório e contas de 2011.
[193] Página 160 do Relatório e contas de 2011.
[194] Página 54 do Relatório e contas de 2011.
[195] Página 115 do Relatório e contas de 2011.
[196] Página 116 do Relatório e contas de 2011.
[197] Página 165 do Relatório e contas de 2011.
[198] Página 26 das Notas às Demonstrações Financeiras Consolidadas 2011.
[199] Página 138 do Relatório e contas de 2011.
[200] Página 161 do Relatório e contas de 2011.
[201] Página 140 do Relatório e contas de 2011

Nesta organização é também dada muita importância à gestão de risco sobre ética e transparência nas áreas de conflitos de interesses, práticas de remuneração e comunicação de irregularidades, a que os accionistas dão particular atenção[202].

Na **ZON** o risco de capital é gerido com o objectivo de salvaguardar a continuidade das operações do grupo, com remuneração adequada aos accionistas e gerando benefícios para os terceiros interessados[203].

[202] Página 146/147 do Relatório e contas de 2011
[203] Página 213 do Relatório e contas 2011.

Conclusão

Este trabalho, através da revisão de literatura de artigos da especialidade, pretendeu responder à questão de saber se a Gestão de Riscos de Negócio é imprescindível para as organizações criarem valor.

Começou-se por um enquadramento histórico de vários acontecimentos importantes que levaram as organizações a repensar a necessidade de reforçar a gestão dos riscos do negócio, devido à complexidade que se instalou nas mesmas, quer pelo peso das entidades reguladoras, quer pela globalização dos mercados e a própria evolução do contexto da economia mundial que transformaram o simples em complexo.

Face às várias crises de credibilidade enfrentadas pelo Mercado de Capitais Norte-Americano e aos vários escândalos em empresas bem conceituadas mundialmente, o Congresso Americano viu-se na necessidade de, para evitar maiores prejuízos e recuperar a credibilidade do mercado, aprovar a implementação de uma nova legislação: a *SOX*.

Seguiu-se uma descrição sobre as várias ferramentas que têm surgido para ajudar a gestão a enfrentar os riscos de negócio, como a *ISO* 26000, o *COSO ERM*, as TI's, a *ISO* 27003, a *ISO* 31000 e recentemente a *ISO* 31010.

Através da revisão de literatura sobre o tema foram analisadas várias opiniões credenciadas sobre o mesmo.

A metodologia escolhida traduziu-se no envio às empresas do *PSI*20 da EuroNext Lisboa e também às organizações brasileiras ligadas ao QSP de um inquérito sobre o tema.

Dada a falta de respostas conclusivas, recorreu-se a uma metodologia alternativa, que consistiu na análise de três estudos sobre o tema em discussão e que permitiu retirar algumas conclusões para responder à questão inicial deste trabalho.

De todas as opiniões colhidas e aqui apresentadas, podemos concluir que, após a crise financeira iniciada em 2002 e repercutida em todo o mundo, a visão sobre a maneira de gerir os riscos evoluiu muito.

Todos estes meios postos à disposição das organizações, dispendiosos é certo, têm vindo a tornar-se imprescindíveis para uma boa Gestão de Riscos de Negócio, criando valor para os

stakeholders, dado que a complexidade dos mesmos tornou mais provável a perda de controlo nas organizações, caso não passe a existir uma maior atenção aos riscos a que estão expostas.

A controvérsia inicial causada pela aprovação da *SOX*, por um lado, pelos custos inerentes superiores ao previsto, e pela maior intervenção da Auditoria Interna, por outro, reforçou a confiança dos investidores nos negócios e nos mercados de títulos.

Porém a sua entrada em vigor provocou uma diminuição acentuada da assunção para o risco e para algumas empresas a sua aplicação resultou mesmo em mais custos do que benefícios.

À luz do debate acalorado sobre o efeito da *SOX* nas empresas americanas e no mercado de capitais, as evidências, embora empíricas, sugerem, pelo menos para algumas empresas, que não só a Lei *SOX* não foi vista como favorável, como diminuiu a apetência das mesmas para a assunção de riscos, preferindo evitar investir em novos projectos de I&D e despesas de capital em activos, apesar da necessidade da sua existência.

A literatura académica consultada sobre a *SOX* parece ser unânime quanto a esta conclusão, como se verificou pelos depoimentos de especialistas da matéria que foram recolhidos e aqui apresentados. Apesar de não se terem encontrado quaisquer opiniões contrárias, tal não significa que estas não existam.

O papel do auditor interno não está contudo bem definido nesta fase, como vimos.

Há uma falta de dados de pesquisa nesta fase, sobre aquilo que a administração espera que seja o papel dos auditores internos nesta questão. Porém, como ficou evidenciado as competências do auditor são fundamentais no conhecimento do negócio, para evitar que o seu trabalho seja duplicado ou alguns riscos passem despercebidos.

As expectativas inicialmente colocadas neste trabalho, nomeadamente com o inquérito elaborado, foram frustradas pela falta de colaboração das organizações contactadas.

Se tivesse havido essa colaboração teria sido interessante tratar os resultados obtidos e fazer a comparação dos mesmos em Portugal e no Brasil, relativamente à nova norma *ISO* 31000.

Dado tratar-se de uma ferramenta nova, também não foi possível recolher estudos ou ensaios que demonstrem as reacções que as organizações estão a ter face a essa nova ferramenta, só alguns depoimentos do que se passa no Brasil, mas não conclusivos em termos quantitativos.

No entanto a ideia mantém-se como muito interessante do ponto de vista da análise do contributo de mais esta ferramenta de gestão de riscos de negócio, pelo que seria útil conseguir obter esse *feedback* em trabalhos futuros.

Em conclusão, poderemos afirmar que a falta de respostas ou a recusa em responder verificadas, poderá indiciar um certo desinteresse das organizações relativamente ao tema proposto.

Em relação à questão inicialmente colocada e em face das opiniões recolhidas pode-se concluir que, embora a gestão de risco seja importante para as organizações, e nalguns casos haja mesmo indícios de que é necessária para o êxito da organização, presentemente e no seguimento dos acontecimentos nefastos que têm marcado os mercados financeiros, há uma acentuada diminuição da assunção para correr riscos, o que se traduz num refrear da aplicação de uma gestão de riscos de negócio o mais completa possível.

Bibliografia

- Almeida, B. (2005). *Auditoria e Sociedade, Diferenças de Expectativas. Publisher Team.* Lisboa.
- Baker, N. (2009). Balancing Risk and Opportunity. *Revista Internal Auditor.*42-45.
- Beasley, M, (2009). Time to teach ERM. *Revista Internal Auditor.*61-63.
- Beja, R. (2004). *Risk Management – Gestão, Relato e Auditoria dos Riscos de Negócio*. Áreas Editora. Lisboa.
- Brasiliano, A. 31000 e Brasiliano – Técnicas e Ferramentas de GR pelo Criador do Método Contemplado. (2010). *Revista Gestão de Riscos. Brasiliano & Associados*. Edição 56. 25-28.
- Carneiro, A. (2009). *Auditoria e Controlo de Sistemas de Informação*. FCA – Editora de Informática. Lisboa.
- Cooper, R. (2006). *Ordem e Caos no século XXI*. Editorial Presença. Lisboa.
- Hubbard, L. (2009). The Matrix Revisited. *Revista Internal Auditor.* 55.
- J Dreyer, S. (2010) *"Standard & Poor's Looks Further Into How Nonfinancial Companies Manage Risk"*. Global Credit Portal.
- Lage, M., Machado, M., Galhardo, M. e Dias, A. (2004). *Útil – Como Organizar?* – Formação do utilizador. IPP. Porto.
- Meireles, M. (2001). *Sistemas de Informação*. Volume I. Primeira Edição. Editora Arte & Ciencia, Coleção Sapientia. S.Paulo.
- Moreau, F. (2003). *Compreender e Gerir os Riscos*. Bertrand Editora. Lisboa.
- Mouchayleh, I. (2007). The Model Approach. *Revista Internal Auditor*. 73-75.
- Pereira, A. e Poupa, C. (2008). *Como escrever uma tese, monografia ou livro cientifico usando o Word*. 4ª Edição. Editora Síbalo. Lisboa.
- Quivy, R. e Campenhoudt. L. (2008). *Manual de Investigação em Ciências Sociais, Trajectos*. 2ª. Edição. Gradiva. Lisboa.
- Redmond, G., Reiling, M. e Miller, P. Extracting Energy from Sarbanes-Oxley. *Revista Internal Auditor.*45-48.
- Jackson, R. (2007). The Human Side of Rrisk. *Revista Internal Auditor*. 38-44.

- Sousa, G., (2005). *Metodologia da Investigação, Redacção e apresentação de trabalhos científicos*. Livraria Civilização Editora. Porto.
- Wells, Joseph T., (2009). *Manual da Fraude na Empresa – prevenção e detecção*. 2ª Edição. Almedina. Coimbra.
- Anderson, S., Christ, M. e Sedatole K. (2006, Janeiro). Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-organizational Settings. *IIA Research Foundation.*
- Sutton, S. (2009, Fevereiro).Why Enterprise Risk Management is Vital. *The IIA Research Foundation.*
- Bargeron, L., Lehn, K., Zutter C. (2007, 18 Junho). Sarbanes-Oxley and Corporate Risk-Taking. *Social Science Research Network*.

Sites Consultados

- http://aeiou.expressoemprego.pt/PageTree.aspx?PageTreeId=4983, consultado em 17.Ago.2010.
- http://andrepitkowski.wordpress.com/tag/iso27001/, consultado em 15.Ago.2010.
- http://careerplanning.aboutcom/cs/legalissues/a/fair_labor.htm, consultado em 16.Dez.2009.
- http://construcoesverdes.blogspot.com/2010/03/norma-iso-26000-e-aprovada-para.html, consultado em 17.Ago.2010.
- http://dandelife.com/story/25779,consultado em 15.Nov.2009.
- http://en.wikipedia.org/wiki/Civilian_Conservation_Corps, consultado em 17.Dez.2009.
- http://en.wikipedia.org/wiki/Export-Import_Bank_of_the_United_States, consultado em 16.Dez.2009.
- http://en.wikipedia.org/wiki/FTSE_100_Index, consultado em 18.Dez.2009.
- http://en.wikipedia.org/wiki/Public_Works_Administration, consultado em 16.Dez.2009.
- http://en.wikipedia.org/wiki/Social_Security_(United_States)#Creation:_The_Social_Security_Act, consultado em 16.Dez.2009.

- http://en.wikipedia.org/wiki/Tennessee_Valley_Authority, consultado em 17.Dez.2009.
- http://eur-lex.europa.eu/LexUriServ/site/pt/com/2001/com2001_0366pt01.pdf/, consultado em 6.Jan.2010.
- http://europa.eu/legislation_summaries/employment_and_social_policy/employment_rights_and_work_organisation/n26034_pt.htm., consultado em 19.Ago.2010.
- http://g1.globo.com/Noticias/Economia_Negocios/0,,AA1540117-9356,00.html, consultado em 14.Nov.2009.
- http://ind.millenniumbcp.pt/pt/Institucional/quemsomos/Pages/historia.aspx, consultado em 6.Set.2012.
- http://iso27000.wik.is/Area_Normas, consultado em 15.Ago.2010.
- http://latamnews.globalcrossing.com/2009/06-jun/Sec_DC_Out/Sec_DC_Out_10POR_jun.htm, consultado em 15.Ago.2010.
- http://pt.euronews.net/2007/10/19/crash-de-1987-faz-20-anos/,consultado em 11.Nov.2009.
- http://pt.shvoong.com/exact-sciences/1740108-entendendo-bolha-imobili%C3%A1ria-americana/, consultado em 22.Nov.2009.
- http://pt.wikipedia.org/wiki/Com%C3%A9rcio_eletr%C3%B4nico, consultado em 16.Dez.2009.
- http://pt.wikipedia.org/wiki/Crash_da_bolsa,consultado em 10.Nov.2009.
- http://pt.wikipedia.org/wiki/Crise_do_subprime#cite_note-3, consultado em 14.Nov.2009.
- http://pt.wikipedia.org/wiki/Crise_do_subprime, consultado em 3.Nov.2009.
- http://pt.wikipedia.org/wiki/Defla%C3%A7%C3%A3o_ (economia), consultado em 4.Nov.2009.
- http://pt.wikipedia.org/wiki/Gerenciamento_de_riscos_do_projeto, consultado em 20.Fev.2010.
- http://pt.wikipedia.org/wiki/KPI, consultado em 24.Ago.2010.
- http://pt.wikipedia.org/wiki/NASDAb Q, consultado em 29.Nov.2009.
- http://pt.wikipedia.org/wiki/S&P_500, consultado em 18.Dez.2009.

- http://revistaepoca.globo.com/Epoca/0,6993,EPT341656-1662,00.html, consultado em 14.Nov.2009.
- http://revistaepoca.globo.com/Epoca/0,6993,EPT344659-1663-1,00.html, consultado em 14.Nov.2009.
- http://torquemanagement.newsweaver.co.uk/TorqueManagement/1dvfvtvm56c, consultado em 14.Nov.2009.
- http://uniethos.tempsite.ws/iso26000/iso-26000-o-que-e/a-norma-iso-26000/, consultado em 18.Ago.2010.
- http://vestibular.uol.com.br/ultnot/resumos/crise-economica-1929.jhtm, consultado em 4.Nov.2009.
- http://wiki.answers.com/Q/Why_was_the_Emergency_Banking_Act_during_FDR's_presidency_the_first_legislation_passed_by_Roosevelt_and_Congress, consultado em 16.Dez.2009.
- http://www.abnt.org.br/imagens/Paginas_especiais/ABNT_SP_15999-_3jun2008.pdf, consultado a 13.Mai.2010
- http://www.aei.org/docLib/20070615_LehnSOX.pdf, consultado em 13.Dez.2009.
- http://www.aei.org/EMStaticPage/1534?page=Summary, consultado em 18.Jan.2010.
- http://www.answers.com/topic/federal-deposit-insurance-corporation, consultado em 17.Dez.2009.
- http://www.banif.pt/xsite/Empresas/Institucional/ClippingdeNoticias.jsp?PID=341799&CH=3743&PCH=null, consultado em 6.Set.2012.
- http://www.banif.pt/xsite/Empresas/Institucional/Historia.jsp?CH=4051, consultado em 6.Set.2012.
- http://www.bbc.co.uk/portuguese/economia/020628_xeroxcg.shtml, consultado em 14.Nov.2009.
- http://www.bbc.co.uk/portuguese/economia/story/2003/12/031230_parmalatml.shtml, consultado em 4.Nov.2009.
- http://www.biocor.com.br/, consultado em 27.Ago.2010.
- http://www.biocor.com.br/novo/detalhes.php?id=17, consultado em 27.Ago.2010.
- http://www.blogger.com/feeds/5432916894862042050/posts/default, consultado em 22.Ago.2010.

- http://www.brasiles, consultado em 4.Nov.2009.
- http://www.brasilescola.com/historiag/crise29.htm, consultado em 10.Nov.2009.
- http://www.brasilescola.com/informatica/bolha-dos-anos-2000.htm, consultado em 18.Nov.2009.
- http://www.bureauveritas.nl/wps/wcm/connect/bv_com/group/home/news/latest-news/vision+-+standard+31000+managing+risk+-all+the+risks?presentationtemplate=bv_master/news_full_story_presentation consultado em 18.Ago.2010.
- http://www.canlecon.org/.../Katherine%20Litvak%20Abstract%20and%20Paper.doc, consultado em 5.Jan.2010.
- http://www.clubeinvest.com/_technical_analysis/forex/1987crash_bolsa1929/1987crash_bolsa1929.php, consultado em 12 Nov.2009.
- http://www.computerworld.com.pt/media/2010/07/WP_9025.pdf, consultado em 20.Ago.2010.
- http://www.constelar.com.br/revista/edicao23/bolsany1.htm,consultado em 10.Nov.2009.
- http://www.coso.org/Publications/NCFFR.pdf, consultado em 23.Ago.2010.
- http://www.csomeeting.com.br/comunidade/entrevistas/612-gestao-de-riscos-pela-norma-asnzs-4360, consultado em 27.Ago.2010.
- http://www.deloitte.com/view/en_CA/ca/services/enterpriserisk/risk-consulting/dd30be87be927210VgnVCM100000ba42f00aRCRD.htm, consultado em 26.Jun.2010.
- http://www.elogroup.com.br/download/Apresenta%C3%A7ao%20IBRACON%20-%20Gestao %20de%20Risco%20e%20a%20ISO%2031000.pdf, consultado em 3.Abr.2010.
- http://www.engenhariadigital.com.br/engenhariadigital/noticias.asp?arquivo=dinheiro/ult91u108013.shtml, consultado em 14.Nov.2009.
- http://www.fraudes.org/showpage1, consultado em 22.Nov.2009.
- http://www.google.pt/imgres?imgurl=http://www.mises.org.br/images/articles/enron.jpg&imgrefurl=http:// http://www.google.pt/imgres?imgurl=http://www.mises.org.br/images/articles/enron.jp

g&imgrefurl=http://www.mises.org.br/Article.aspx%3Fid%3D28&h=311&w=401&sz=27&tbnid=F3dpJHCWP2cwoM:&tbnh=96&tbnw=124&prev=/images%3Fq%3Denron&hl=pt-PT&usg=__aGeWsijWV6i0v1L5CNdsc35Ve-I=&ei=mLcfS7i-Et_OjAeqpsmmCw&sa=X&oi=image_result&resnum=4&ct=image&ved=0CBkQ9QEwAw, consultado em 14.Nov.2009.

- http://www.iapmei.pt/iapmei-art-03.php?id=1860/, consultado em 19.Ago.2010.
- http://www.indiana.edu/~liblilly/wpa/wpa_info.html, consultado em 17.Dez.2009.
- http://www.infopedia.pt/$new-deal, consultado em 10.Nov.2009.
- http://www.iso.org/iso/pressrelease.htm?refid=Ref1302, consultado a 15.Ago.2010.
- http://www.iso26000qsp.org/search/label/A%20quest%C3%A3o%20ambiental%20na%20ISO%2026000, consultado em 17.Ago.2010.
- http://www.iso31000qsp.org/, consultado em 17.Ago.2010.
- http://www.iso31000qsp.org/2010/08/esclarecimento-sobre-certificacao.html, consultado em 1.Set.2010.
- http://www.iso31000qsp.org/search/label/ISO%20Guia%2073%3A2009, consultado em 27.Jun.2010.
- http://www.jacoby.pro.br/fraudes.doc, consultado em 14.Nov.2009.
- http://www.marsh.nl/documents/nieuwsenmedia/Rapport_SP_ERM.pdf, J Dreyer, Steven “Standard & Poor's Looks Further Into How Nonfinancial Companies Manage Risk”, consultado em 24 Jun.2010.
- http://www.miradaglobal.com/index.php?option=com_content&view=article&id=80:la-crisis-moral-del-capitalismo&catid=28:economia&Itemid=32&lang=pt, consultado em 14.Nov.2009.
- http://www.mota-engil.pt/AreaDetail.aspx?contentId=88&Language=1, consultado em 15.Set.2012.
- http://www.nirf.org/_upl/presentasjon_vedr_coso_erm_av_martin_stevens_paa_nfrfs_aarskonferanse_i_stockholm_april_2004.pdf, consultado 22.Out.2009.
- http://www.novelguide.com/a/discover/egd_01/egd_01 _00189.html, consultado em 17.Dez.2009.
- http://www.nysscpa.org/cpajournal/2007/1107/perspectives/p7.htm, consultado em 10.Jan.2010.

- http://www.ourdocuments.gov/doc.php?flash=old&doc=66, consultado em 17.Dez.2009.
- http://www.portaldaempresa.pt/CVE/pt/Gestao/ResponsabilidadeSocial/, consultado em 6.Jan.2010.
- http://www.portucelsoporcel.com/pt/group/index.php , consultado em 20.Set.2012.
- http://www.qsp.org.br/biocor.shtml, consultado a 27.Ago.2010.
- http://www.qsp.org.br/capacitacao_gr.shtml, consultado em 20.Jun.2010.
- http://www.qsp.org.br/GI_26000.shtml, consultado em 17.Ago.2010.
- http://www.scribd.com/doc/6841023/O-caso-Enron, consultado em 4.Nov.2009.
- http://www.seguridadinformatica.es/profiles/blogs/publicada-isoiec-270032010, consultado em 15.Ago.2010.
- http://www.smartsec.com.br/iso_27000.html, consultado em 15.Ago.2010.
- http://www.softexpert.com.br/norma-iso31000.php, consultado em 20 Jul.2010.
- http://www.softexpert.com.br/norma-sox.php, consultado em 14.Dez.2009.
- http://www.softexpert.com.br/se-suite.php, consultado em 20.Jul.2010.
- http://www.softexpert.com.pt/partnercenter/noticias.php?nid=457, consultado em 26 .Ago.2010.
- http://www.sonaeindustria.com/page.php?ctx=2,0,17, consultado em 18.Set.2012.
- http://www.spartacus.schoolnet.co.uk/USARagriculture.htm, consultado em 16.Dez.2009.
- http://www.terra.com.br/istoedinheiro/253/negocios/253_herois_capitalismo.htm, consultado em 14.Nov.2009.
- http://www.theiia.org/, consultado em 15.Jan.2010.
- http://www.trolp.org/main_pgs/issues/v12n2/Terwilliger_Format.pdf, consultado em 19.Jan.2010.
- http://www.vidabrasil.com.br/exibe_noticias.asp?cod_noticia=515&edicao=316&data=15/10/2002, consultado em 14.Nov.2009.
- http://www.webartigos.com/articles/24670/1/o-caso-enron/pagina1.html, consultado em 14.Dez.2009.

- http://www.wharton.universia.net/index.cfm?fa=viewfeature&id=1118&language=portuguese, consultado em 14.Nov.2009.
- http://www.zon.pt/institucional/PT/sobre-a-zon/Historia/Paginas/historia.aspx, consultado em 18.Set.2012.
- http://www-05.ibm.com/pt/ibm/ccr/ars.html, consultado em 17.Ago.2010.

Anexo I – Certificação da Biocol

Sistema de Gestão de Riscos

Germanischer Lloyd Industrial Services do Brasil Ltda., Av. Pompéia 2425 – São Paulo – Brasil,
certifica pelo presente que a empresa

BIOCOR – HOSPITAL DE DOENÇAS CARDIOVASCULARES LTDA
Av. Alameda da Serra nº 217 - Vila da Serra
34000-000 - Nova Lima - Minas Gerais - Brasil

estabeleceu e mantém um Sistema de Gestão Integrada de Riscos abrangendo

Instituto Biocor – Hospital Geral focado em Cirurgia Cardiovascular.

A empresa foi auditada pelo Germanischer Lloyd Industrial Services do Brasil Ltda, tendo-se evidenciado que o Sistema de Gestão Integrada de Riscos satisfaz aos requisitos da seguinte norma:

QSP 31000:2010 – Sistema de Gestão de Riscos

A validade deste certificado condiciona-se à aplicação e à manutenção do Sistema de Gestão Integrada de Riscos pela empresa, em conformidade com a norma indicada. Esta condição será monitorada pelo Germanischer Lloyd Industrial Services do Brasil Ltda.

Data Certificação: 27/06/2010.

Este certificado é válido até: 26/06/2013.

São Paulo, 05/07/2010.

Certificado No. **SGR-0818-BR**

O processo foi conduzido por:
Nairson de Oliveira
Auditor Líder

Reginaldo Maia
Diretor Executivo

GL

Anexo II – Inquérito

Inquérito às Empresas - Introdução

O presente inquérito é o resultado da necessidade de obter e tratar dados sobre a apetência das empresas, em face da GRN desenvolvida na organização, de virem a melhorar o processo com a adopção da norma 31000 e insere-se no trabalho de dissertação do mestrado de auditoria do Instituto Superior de Contabilidade e Administração do Porto.
A Norma *ISO* 31000 de 2009 é uma norma geral de Gestão de Riscos, independente da área ou actividade, fornecendo linhas de orientação para a implementação da Gestão de Riscos nas organizações.
Esta norma da *International Organization for Standardization* perspectiva a Gestão do Risco de Negócio que, com a evolução dos mercados cada vez mais globalizada, fez da Gestão do Risco parte essencial da estratégica a adoptar para o negócio, sendo responsabilidade de todas as áreas da organização e parte integrante do processo de tomada de decisão.
Tradicionalmente relacionada com riscos de segurança ocupacional (OHSAS 18001) ou riscos ambientais (ISO 14001), a Gestão do Risco abrange actualmente desde as tecnologias de informação, os factores sociais, os factores financeiros até à própria continuidade do negócio.

A **ISO 31000 de 2009** é projectada para ajudar as organizações a:

- Incentivar a gestão proactiva;
- Melhorar e identificar oportunidades e ameaças;
- Tomar consciência da necessidade de identificar e tratar os riscos em toda a organização, em termos dos seus pontos fortes e fracos;
- Melhorar a confiança das partes interessadas e consequentemente da informação;
- Melhorar a eficácia operacional e a eficiência da gestão;
- Melhorar a capacidade de resistência organizacional.

O inquérito é composto por duas partes:

- Nota metodológica
- Inquérito

As respostas obtidas serão depois tratadas e elaborado um relatório final a disponibilizar a todos os participantes, sendo assegurada a sua confidencialidade.

I. Nota metodológica

O inquérito aqui lançado tem como objectivo central uma aproximação à temática da modernização da **GRN**, mais especificamente a adopção da nova ***ISO* 31000**.

Sendo um tema sobre o qual ainda existe escassez de informação, dado que só recentemente foi publicada no Brasil (Novembro de 2009) e tendo estado em discussão pública no IPQ – Instituto Português de Qualidade no início deste ano, aqui em Portugal, configura um interesse acrescido para uma norma em começo de análise e aplicação.

A eleição do universo de empresas cotadas portuguesas e brasileiras será um ponto de partida para a comparação da apetência da sua aplicabilidade num e noutro país.

Neste contexto, a estratégia do inquérito assentou na preocupação de reduzir, dentro do possível, o número de variáveis a considerar e centralizar o questionário na caracterização dessa apetência e/ou necessidade sentida da utilização de mais uma ferramenta de apoio à gestão de topo na **Gestão dos Riscos de Negócio**.

Procurou-se focalizar o inquérito em quatro vertentes:

- ✓ as empresas que não vão, pelo menos a curto prazo, apostar nesta ferramenta de trabalho;
- ✓ as empresas que estão já a procurar acompanhar a sua adopção no mais curto espaço de tempo possível;
- ✓ de entre estas últimas, aquelas que começaram já a agendar e programar a sua adopção.
- ✓ finalmente tentar identificar e comparar o tipo de empresas portuguesas e brasileiras que irão adoptar este normativo.

De acordo com estes objectivos definidos, as variáveis utilizadas foram fundamentalmente descritivas.

Finalmente o inquérito será tratado em três bases distintas:

- **Base empresas portuguesas**: variáveis de caracterização da amostra em face das respostas recebidas, da sua opinião e identificação do número de possíveis projectos de adopção da norma 31.000;
- **Base empresas brasileiras**: o mesmo tipo de análise;
- **Estudo comparativo das amostras dos dois países** relativamente a este tema.

As bases serão, após recolha, tratadas em EXCEL e os resultados finais disponibilizados a todos os participantes.

Este questionário enquadra-se no âmbito do projecto de Mestrado de Auditoria do Instituto Superior de Contabilidade e Administração do Porto, com orientação do docente Mestre Carlos Mendes.

O presente questionário destina-se a recolher informação sobre o conhecimento que existe por parte das organizações sobre Gestão de Riscos de Negócio e o impacto da implementação da nova Norma *ISO* 31000.

O tratamento da informação aqui recolhida será confidencial e reservada ao estudo em questão e tratamento estatístico.

Desde já grata pela participação e disponibilidade

Ana Jorge Neves de Barros

Grupo I – Questões Gerais

1.**Caracterização da Organização**

1.1 **Empresa**_____

Morada:_____
Telefone_____ Email_____

1.2. **Sector de actividade**

1.2.1 Código CAE ☐

1.3. Volume de negócios anual em M€ ☐

1.4. Capital Social ☐

1.5. Mercados
1.5.1 ☐Mercado interno
1.5.2. ☐Mercado externo
1.5.3. ☐Outros mercados _____

1.6. Número de empregados da empresa ☐

1.7. Empregados qualificados

- Licenciatura ☐
- Formação avançada ☐
- Outros ☐

Grupo II – Sistema de Gestão de Riscos

1- Já tinham conhecimentos sobre **Gestão de Riscos de Negócio**?

- ☐ Sim ☐ Não

2 – Se respondeu sim à anterior, explique por favor como obteve esse conhecimento?

- ☐ Internet ☐ Acções de Formação ☐ Outros

3 – Gostaria de obter mais informações e mais específicas sobre este tema?

- ☐ Sim ☐ Não

4 – Acha que um seminário sobre este assunto seria pertinente?

- ☐ Sim ☐ Não

5 – Na sua organização está implementada a Gestão de Riscos de Negócio?

- ☐ Sim ☐ Não

Nota: Se respondeu não à questão anterior, passe por favor à questão 12

6- Se respondeu sim à questão anterior, refira por favor que tipo de apoios obteve.

_____

_____

7 - Na sua opinião os Modelos de Gestão de Risco conhecidos, foram úteis para a implementação do Sistema de Gestão de Riscos de Negócio da sua Organização? Explique.

- ☐ Sim ☐ Não

  _____

8 – Para a sua Organização quais acha que serão as mais-valias de um Sistema de Gestão de Riscos de Negócio?

_____

_____

9 – Na implementação do Sistema de Gestão de Riscos de Negócio, quais as maiores dificuldades sentidas?

_____

_____

10 – Quantos colaboradores estiveram envolvidos (directa e indirectamente) na implementação do Sistema de Gestão de Riscos de Negócio na sua organização? ☐

11 - Após a implementação do Sistema de Gestão de Riscos de Negócio, verificam-se já melhorias nos seguintes itens?

	Sim	Não	Não tem a certeza
Comprometimento da Gestão de Topo			
Revisão efectiva pela Gestão de Riscos de Negócio			
Utilização dos indicadores (KPI´s, KRI´s, …) como ferramenta de Gestão			
Satisfação dos colaboradores			
Maior quota de mercado			
Melhoria nas relações verticais			
Melhoria da produtividade			

12 – Gostaria de iniciar a implementação de um sistema de Gestão de Riscos de Negócio na sua Organização?

- ☐ Sim ☐ Não

Porquê? _____

13 – Quais as vantagens que destacaria na sua organização após a implementação de um sistema Gestão de Riscos de Negócio na sua Organização?

_____

_____

14 – Necessita de saber mais informações sobre este assunto?

- ☐ Sim ☐ Não

15 – Como gostaria de obter essas informações (pode optar por mais do que uma opção):

- ☐ Seminário ☐ Workshop ☐ Gabinete de apoio ☐ Outros

_____

Grupo III - Norma *ISO* 31000

1- Conhece a norma *ISO* 31000?

- ☐ Sim ☐ Não

2 - Se a sua Organização já possui um sistema de Gestão de Riscos de Negócio, estaria disponível para implementar a norma *ISO* 31000?

- ☐ Sim ☐ Não

3 – Participou na discussão pública sobre esta Norma que o IPQ realizou?

- ☐ Sim ☐ Não

4 – Se respondeu não, acha importante participar?

- ☐ Sim ☐ Não

5 – Se respondeu sim, acha importante para a sua Organização a implementação de uma norma deste tipo?

- ☐ Sim ☐ Não

6 – Que benefícios/expectativas espera obter com este tipo de norma?

_____

_____

7 - Que efeito espera sobre o volume de documentação necessária produzir por via da implementação da norma (poderá responder a vários itens)?

- ☐ Diminui
- ☐ Mantém-se
- ☐ Aumenta
- ☐ Fica mais simples
- ☐ Fica mais complicado

8 - Que tipo de formação foi ministrada na sua organização (poderá responder a vários itens)?

- ☐ Transição da norma
- ☐ Recolha e análise de dados
- ☐ Específica na Gestão de Risco
- ☐ Outra _____

9 - Quantos colaboradores tiveram formação na Norma 31000?

- ☐ Menos de 6 pessoas
- ☐ 6 a 12 pessoas
- ☐ 12 a 24 pessoas
- ☐ Mais de 24 pessoas

10 - Qual o tempo total de duração da formação global?

- ☐ Menos de 1 mês
- ☐ 1 a 2 meses
- ☐ 2 a 4 meses
- ☐ Mais de 4 meses

11 – No caso de ter auditores internos que tipo de formação lhes proporcionou?

- ☐ Formação para a transição para este normativo
- ☐ Certificação em Gestão de Risco
- ☐ Outro _____

12 - Houve uma avaliação prévia, em termos de necessidades de formação?

- ☐ Sim ☐ Não

12.1 - Em caso afirmativo, quais as conclusões mais significativas que foram detectadas?

- ☐ Exclusões da gestão de topo
- ☐ Documentação
- ☐ Registos
- ☐ Controlo efectivo de processos
- ☐ Objectivos não mensuráveis
- ☐ Objectivos não consistentes com a política de Gestão de Riscos
- ☐ Recolha e análise de dados
- ☐ Competência de recursos
- ☐ Comprometimento e responsabilidade da gestão de topo
- ☐ Gestão de processos em outsourcing
- ☐ Outros _____

Nota – para as questões 13 e 14 proceda da seguinte forma : em 1.º lugar identifique-as e em 2.º lugar ordene-as por importância (1.º, 2º,…)

13 - Quais as áreas que mereceram maiores ajustamentos?

- ☐ Exclusões da gestão de topo
- ☐ Documentação
- ☐ Registos
- ☐ Controlo efectivo de processos
- ☐ Objectivos não mensuráveis
- ☐ Objectivos não consistentes com a política de Gestão de Riscos
- ☐ Recolha e análise de dados
- ☐ Competência de recursos
- ☐ Comprometimento e responsabilidade da gestão de topo
- ☐ Gestão de processos em outsourcing
- ☐ Outros _____

14 - Quais as áreas onde se detectaram as não conformidades mais relevantes?

- ☐ Exclusões da gestão de topo
- ☐ Documentação
- ☐ Registos
- ☐ Controlo efectivo de processos
- ☐ Objectivos não mensuráveis
- ☐ Objectivos não consistentes com a política de Gestão de Riscos
- ☐ Recolha e análise de dados
- ☐ Competência de recursos
- ☐ Comprometimento e responsabilidade da gestão de topo
- ☐ Gestão de processos em outsourcing
- ☐ Outros _____

15 - Quantos colaboradores estiveram ou têm estado envolvidos neste processo?

16 - Qual o tempo total dispendido pelos colaboradores afectos a esta tarefa?

17 – Pensa que os custos aumentarão comparativamente com as certificações existentes?

- ☐ Sim ☐ Não

17.1 - Em caso afirmativo, qual a percentagem

- ☐ Menos de 10%
- ☐ 10 a 20%
- ☐ 20 a 30%
- ☐ 30 a 40%
- ☐ 40 a 50%
- ☐ Superior a 50%

18 - Quantos colaboradores, a tempo integral, irá afectar a sua empresa na manutenção de um sistema deste tipo? ☐

19 – Conhece a ferramenta *Enterprise Risk Manager*, baseada numa abordagem simples e comprovado na redução do risco, apoiando a *ISO* 31000 e outras normas como a *ISO* 27001 / 17799 e COSO?

- ☐ Sim ☐ Não

20 – Já tinha anteriormente utilizado esta ferramenta? O que pensa sobre o seu uso?

- ☐ Sim. É útil ☐ Não. É complicada

_____

_____

Muito se agradece o tempo usado no preenchimento deste questionário, garantindo-se desde já que as respostas são absolutamente confidenciais, servindo apenas para tirar conclusões genéricas sobre o universo de empresas nacionais certifi*cadas.*

Anexo III – Primeiro estudo – *"Sarbanes-Oxley and Corporate Risk-Taking"*, de Leonce Bargeron, Kenneth Lehn, Chad Zutter da *University of Pittsburgh*

Sarbanes-Oxley and Corporate Risk-Taking

Leonce Bargeron, Kenneth Lehn, Chad Zutter
University of Pittsburgh

To be presented at the American Enterprise Institute

June 18, 2007

Abstract

Many policymakers and corporate executives have argued that the Sarbanes-Oxley Act of 2002 ("SOX") has had a chilling effect on the risk-taking behavior of U.S. corporations. This paper empirically examines this proposition. Using a large sample of U.S. and U.K. companies, we find that compared with their U.K. counterparts U.S. firms have significantly reduced their R&D and capital expenditures and significantly increased their cash holdings since SOX. We also find that the equity of U.S. companies has become significantly less risky vis-à-vis U.K. companies since SOX. Finally, using a large sample of U.S. and U.K. initial public offerings ("IPOs"), we find that the likelihood that an IPO was conducted in the U.K. increased significantly after SOX and that this effect was especially high for firms in high R&D industries. Taken together, the results support the view that SOX has had a chilling effect on risk-taking by publicly traded U.S. corporations.

The authors gratefully acknowledge funding support for the preparation of this paper from the National Research Institute at the American Enterprise Institute.

Sarbanes-Oxley and Corporate Risk-Taking

Leonce Bargeron, Kenneth Lehn, and Chad Zutter
University of Pittsburgh
June 2007

1. Introduction

Many commentators, including both supporters and critics of the Sarbanes-Oxley Act of 2002 ("SOX"), have argued that SOX has had a chilling effect on risk-taking by U.S. corporations. Among other things, this legislation, which expanded federal regulation of corporate governance for publicly traded U.S. corporations, requires (i) chief executive officers and chief financial officers to certify financial statements, (ii) companies to file annual internal control reports that evaluate the effectiveness of the controls, and (iii) audit committees to comply with new regulations governing their composition and procedures. In addition, SOX tightened regulation of auditors and provided the SEC with expanded enforcement authority against auditors, officers, and directors.

One year after the legislation was signed into law, William Donaldson, then chairman of the Securities and Exchange Commission, stated that "I worry about the loss of risk-taking zeal. …Sarbanes-Oxley unleashed batteries of lawyers across the country.

…[the result is] a huge preoccupation with the dangers and risks of making the slightest mistake, as opposed to a reasonable approach to legitimate business risk."[1]

Similarly, in July 2003, Alan Greenspan, then chairman of the Federal Reserve Board, stated that "corporate executives and boards of directors are seemingly unclear, in the wake of the recent intense focus on corporate behavior, about how an increase in risk-taking on their part would be viewed by shareholders and regulators. As a result, business leaders have been quite circumspect about embarking on major new investment projects."[2]

Similar comments have been heard from the corporate community, especially from executives of companies in high-risk industries. For example, in 2004, Tom Siebel, former CEO of software company Siebel Systems, stated that "we might have killed the goose that lays the golden egg. …You're mitigating every possible risk that can be conceived. Risk didn't used to be a bad thing."[3]

This paper empirically examines the merits of the view that SOX has chilled risk-taking by U.S. corporations. Our analysis consists of two parts.

First, we examine whether several measures of corporate risk-taking have changed significantly for publicly traded U.S. companies since SOX was signed into law in 2002. Specifically, we examine two sets of measures: (i) accounting-based variables, which measure the level and types of investments firms make and (ii) stock-based variables, which measure the market's assessment of a firm's equity risk.

---

[1] Adrian Michaels, "After a Year of US Corporate Clean-Up, William Donaldson Calls for a Return to Risk-Taking," *FinancialTimes.com*, July 24, 2003.
[2] Testimony of Chairman Alan Greenspan before the Committee on Financial Services, U.S. House of Representatives, July 15, 2003.
[3] Tony Kontzer, "Siebel Sees Sarbanes-Oxley Taking Toll on Economy," *Information Week*, October 13, 2004.

Using a sample of U.K. firms as a benchmark, we find that since the adoption of SOX U.S. companies have (i) significantly reduced expenditures on research and development ("R&D"), (ii) significantly reduced capital expenditures, and (iii) significantly increased holdings of cash, which represents non-operating, low-risk investments. Hence, the investment behavior of U.S. firms reveals a statistically significant reduction in risk-taking after the adoption of SOX.

The stock-based measures reveal that the equity of U.S. companies became less risky vis-à-vis U.K. companies after SOX. The standard deviation of stock returns (both daily and monthly), a conventional measure of a company's equity risk, declined significantly for U.S. firms as opposed to their U.K. counterparts, in the post SOX period. Furthermore, the two components of total equity risk declined significantly for U.S. firms, as compared with the U.K. firms, after SOX. The market risk of U.S. firms, measured by their "betas" vis-à-vis a worldwide index, declined significantly as compared with the corresponding beta of U.K. firms in the post-SOX period. This result is especially pronounced for firms in high risk, R&D intensive industries. In addition, the firm-specific risk of U.S. firms, measured by the root mean square error from estimation of the market model, fell significantly more for U.S. firms versus their U.K. counterparts after SOX.

Second, we examine data on initial public offerings ("IPOs") in the U.S. and U.K. to test whether the likelihood that a firm raises capital in U.S. versus U.K. public equity markets after the adoption of SOX is related to its R&D expenditures, which serves as a proxy for the risk of the firm's activities. Using a sample of 9,258 initial public offerings ("IPOs") conducted in the U.S. and U.K. from 1990-2006, we find that (i) the probability

that an IPO was conducted in the U.K. as opposed to the U.S. increased sharply after SOX and (ii) the higher a firm's R&D activity, the greater the increase in the probability the firm went public in the U.K. after SOX.

The paper is organized as follows. Section 2 describes the sample and data. Section 3 contains empirical results on risk-taking by U.S. corporations after SOX. Section 4 presents evidence on the relation between R&D activity and the choice of conducting an IPO in the U.S. versus the U.K. after SOX. Section 5 includes concluding comments.

2. Sample and data

Sample

Our sample consists of 5,228 U.S. and U.K. publicly traded corporations, including 4,239 U.S. corporations and 989 U.K. corporations, for which sufficient data exists on the Thomson One Banker database. These firms represent all U.S. and U.K firms in the database for which there is consistent time series data, spanning the adoption of SOX, on the key variables used in the analysis. Specifically, to be included in the sample we required that the following variables were available for at least one year during the 1998-2000 and 2003-2005 periods: sales, earnings before interest and taxes EBIT, assets, capital expenditures, cash holdings and daily stock returns. Because data on R&D expenditures is considerably sparser, existing for only 1,980 firms (1,746 U.S. firms, 234 U.K. firms), we do not require data on R&D expenditures for each period in order for firms to be included in the sample.

The sample consists of both large and small companies. The U.S. sample includes 412, or 82.4%, of the companies in the S&P 500, indicating that most large U.S.

corporations are included in the sample. Similarly, 69, or 67.6%, of the companies in the U.K.'s FTSE 100 Index (there are 102 companies in the index) are included in the sample. The sample also includes relatively small companies. For example, the sample includes 331 U.S. companies with average sales during the post-SOX period of less than $1 million and 75 U.K. companies with average sales of less than £1 million.

Table 1 shows the industry distribution of the U.S. and U.K. samples. Specifically, the table shows the number and percent of the two samples that operate in 74 different industries, defined by 2-digit SIC codes. The most represented industries in the U.S. sample are business services (15.9%), electrical and electronic equipment (8.3%), and paper and allied products (7.4%), while the most represented industries in the U.K. sample are holding and other investment offices (18.4%), business services (11.7%), and engineering and management services (5.4%). The least represented industries in the U.S. sample are museums, art galleries, botanical & zoological gardens (0.00%), legal services (0.02%), and justice, public order, and safety (0.02%). In the U.K. sample, nine of seventy-four industries are unrepresented: legal services; justice, public order, and safety; pipelines; agricultural production, environmental quality and housing; miscellaneous services, miscellaneous repair services; insurance carriers; and government agencies.

To determine whether the industry distributions of the two samples are similar, we calculated the correlation coefficient between the number of firms in each industry in the U.S. and U.K. samples. Across the 74 industries, the correlation coefficient is 0.64 and significant at the 0.01 level. Hence, the industry distributions of the two samples appear to be similar.

Data

Financial accounting data for the sample was collected from the Thomson One Banker database. For each firm in each year during the period of 1995 through 2005 we collected the following data: sales, EBIT, capital expenditures, R&D expenditures, total assets, and cash holdings. We express capital expenditures, R&D, cash, and EBIT as ratios to both assets and sales.

Data on stock prices, which is used to compute the stock-based risk measures, are collected from the Datastream database for both the U.S. and U.K. samples. Daily and monthly stock returns over the period of 1994 through 2006 are calculated from the daily adjusted stock prices To estimate equity betas and root mean square errors for the U.S. and U.K. samples, we regress the daily returns of these companies on the corresponding returns of the MSCI World Index ("MSCI"), a value-weighted global index consisting of companies across 24 countries.

Summary statistics

Table 2 presents descriptive information about the key variables for the U.S. and U.K. samples over various periods predating and succeeding SOX. Panel A tabulates the accounting measures over three three-year periods, 1995-1997 and 1998-2000, two periods preceding SOX, and 2003-2005, one period after SOX. Panel B tabulates the stock-based measures over three four year periods, 1994-1997, 1998-2001, and 2003-2006.[4] For each variable, we calculate the mean value for each firm within each period. We then calculate the mean and median values of these values for the U.S. and U.K.

[4] Because accounting data for fiscal year 2006 is unavailable for many firms, accounting variables are compiled over three year periods. To minimize potential microstructure issues return based measures are compiled over four year periods using monthly data.

samples. For the sake of brevity, Table 2 presents only the median values for both the U.S. and U.K. samples.

The table reveals significant differences across the two samples.

The ratio of R&D expenditures to assets is significantly higher for the U.S. sample in all three periods. However, the difference in the ratio has declined over time. For the U.S. sample, the ratio of R&D expenditures to assets increased from 0.0705 during 1995-1997 to 0.0782 during 1998-2000, and then declined to 0.072 during 2003-2005, the post-SOX period. For the U.K. sample, this ratio increased steadily over the three periods, from 0.0189 to 0.0288 to 0.0334. The difference in the ratio across the U.S. and U.K. samples declined from 0.0516 to 0.0494 over the two pre-SOX periods to 0.0386 in the post-SOX period.

The ratio of capital expenditures to assets also is significantly higher for the U.S. sample in all three periods. However, here too, the difference in the ratio has declined over time. For the U.S. sample, this ratio has steadily declined from 0.0542 during 1995-1997 to 0.0488 during 1998-2000 to 0.0303 during 2003-2005. It also has declined steadily for the U.K. sample, from 0.0477 to 0.0428 to 0.0253. The difference in the ratio across the U.S. and U.K. samples declined from 0.0065 to 0.0060 over the two pre-SOX periods to 0.0050 in the post-SOX period.

The table reveals that the ratio of cash holdings to assets is significantly higher for the U.S. sample in all three periods and that this difference widened considerably in the post-SOX period. The ratio declined from 0.0947 during 1995-1997 to 0.0922 during 1998-2000, and then increased sharply to 0.1149 during the post-SOX period for the U.S. sample. In contrast, for the U.K. sample, the ratio increased slightly from 0.0826 to

0.0832 over the two pre-SOX periods and then declined to 0.0796 in the post-SOX period. The difference in the ratio of cash holdings to assets across the U.S. and U.K. samples declined from 0.0121 to 0.0091 over the two pre-SOX periods and then widened to 0.0353 in the post-SOX period.

Little difference exists in the profit rate of the two samples, as measured by the ratio of EBIT to assets. This profit rate has declined steadily over time for both samples, from 0.0864 to 0.0575 to 0.0470 for the U.S. sample. The corresponding decline for the U.K. sample is from 0.0833 to 0.0672 to 0.0420. The difference in profit rates across the two samples is not significant for the first pre-SOX period, significantly higher for the U.K. sample in the second pre-SOX period, and significantly higher for the U.S. sample in the post-SOX period. Hence, no discernible pattern exists in the relative profitability of the two samples over time, suggesting that the pattern of differences in R&D, capital expenditures, and cash holdings over time are related to factors other than differences in the profit rates of the two samples.

The standard deviation of stock returns, the measure of total equity risk, is significantly higher for the U.S. sample in all three periods. It increased from 0.1291 to 0.2074 over the two pre-SOX periods for the U.S. sample, then declined to 0.1394 in the post-SOX period. Similarly, the standard deviation of returns increased from 0.0746 to 0.1225 over the pre-SOX periods for the U.K. sample and then declined to 0.087 in the post-SOX period. The difference in this variable across the two samples increased from 0.0546 to 0.0849 over the two pre-SOX periods and then declined to 0.0524 in the post-SOX period.

The two components of equity risk, market and firm specific, also are significantly higher for the U.S. sample in all three periods. The equity beta for U.S. firms, measured against the MSCI World Index, increases steadily across the three periods, from 0.6534 to 0.9403 to 1.2314. Similarly, the beta of U.K. firms increases from 0.46 to 0.7012 to 1.087. The difference in the beta for U.S. versus U.K. firms increases from 0.1934 to 0.2391 over the two pre-SOX periods and then declines to 0.1444 in the post-SOX period.

The root mean square error of U.S. firms, a measure of firm specific risk, increases from 0.126 to 0.199 over the two pre-SOX periods and then declines to 0.1331 in the post-SOX period. The corresponding changes for the U.K. sample are an increase from 0.0719 to 0.1173, followed by a decline to 0.0828 in the post-SOX period. The difference across the two samples increases from 0.0541 to 0.0816 over the pre-SOX periods and then declines to 0.0503 in the post-SOX period.

In sum, the data in Table 2 broadly show that (i) the proxies for risk-taking are significantly different for U.S. versus U.K. firms both before and after SOX and (ii) the differences in these proxies have changed since SOX in ways consistent with the view that SOX has chilled corporate risk-taking in the U.S. We now test more systematically whether there has been a statistically significant change in the proxies for risk-taking for U.S. corporations versus their U.K. counterparts.

3. Empirical results

To examine whether risk-taking by publicly traded U.S. corporations declined significantly after Sarbanes-Oxley, we conduct two sets of tests. The first set examines accounting-based variables to test whether there was a significant change in the level and

risk of investments made by U.S. companies after the adoption of SOX. The second set examines stock-based variables to test whether the market's assessment of the equity risk of U.S. versus U.K. companies changed significantly after SOX.

Accounting-based measures of the level and risk of corporate investment

We first consider three variables that describe the types of assets in which firms invest – R&D expenditures, capital expenditures, and cash holdings – before and after the adoption of SOX. For each firm in the U.S. and U.K. samples we calculate the mean value of (i) the ratio of R&D expenditures to assets, (ii) the ratio of capital expenditures to assets, and (iii) the ratio of cash holdings to assets in the 1995-1997, 1998-2000, and 2003-2005 periods. For each firm, we calculate the difference in the mean value of the respective variable during the post-SOX period and the corresponding mean values during 1995-1997 and 1998-2000, the two pre-SOX periods. We then calculate the median differences in these values for the entire sample of U.S. and U.K. companies. A negative median difference indicates that for the median firm the value of the respective variable declined in the post-SOX period.

Table 3 contains the median differences in values of the R&D, capital expenditures, and cash holdings variables for the U.S. and U.K. samples. The median ratio of R&D expenditures to assets declined for both samples after SOX, but the decline was larger for the U.S. sample. Using the period of 1998-2000 as the benchmark, the median changes were -0.00250 for the U.S. sample and -0.00045 for the U.K. sample, a difference that is significant at the 0.05 level. This difference is even larger when the period of 1995-1997 is used as the benchmark period (-0.00361 for the U.S., -0.00069 for the U.K.) and this difference is significant at the 0.01 level.

The median ratio of capital expenditures to assets also declined for both samples from before to after SOX, and, here too, the decline was larger for U.S. firms. When compared against the pre-SOX period of 1998-2000, the median difference in the U.S. was -0.01379, as compared with -0.00927 in the U.K. This difference across the two samples is not statistically significant. However, when compared with the 1995-1997 period, the median difference in the capital expenditures variables is significantly more negative for the U.S. (-0.01783) versus the U.K. sample (-0.01076). This difference is significant at the 0.01 level.

Table 3 shows that after SOX the median ratio of cash holdings to assets increased for the U.S. sample and decreased for the U.K. sample. Using the 1998-2000 benchmark period, the cash holdings to assets ratio of the median U.S. company increased by 0.0078 after SOX, as compared with a decrease of 0.00266 for the U.K. sample. The difference across the two samples is significant at the 0.01 level. Similar results obtain when the 1995-1997 period is used as the benchmark pre-SOX period.

In short, the results show that when examining the full sample of U.S. and U.K. firms, there was a statistically significant decline in R&D and capital expenditures of U.S. firms versus their U.K. counterparts and a statistically significant increase in the relative cash holdings of U.S. firms. Because R&D and capital expenditures involve outlays on risky projects and cash holdings represent investments in non-operating low risk assets, this evidence is consistent with the view that SOX has chilled risk-taking activity by U.S. corporations.

To probe whether the changes in risk-taking activity varied across industries, we divide the sample into three groups – firms operating in industries with high, moderate,

and low R&D activity. We define high, moderate, and low R&D industries based on total U.S. industry R&D expenditure over the benchmark period of 1994-1997. Seven 2-digit SIC code industries account for 92.1% of R&D expenditure in the U.S. during this period: chemicals and allied products, transportation equipment, industrial machinery and equipment, electrical and electronic equipment, business services, instruments and related products, and communications.. We disaggregate the seven 2-digit SIC code industries into their thirty-seven 3-digit SIC code industry components. We classify the fifteen of these 3-digit SIC code industries that account for at least 1% of the total U.S. R&D expenditure during the period as high R&D industries. We define the remaining twenty-two of these 3-digit SIC code industries as moderate R&D industries. We also classify the seventeen remaining 2-digit SIC code industries with at least $100 million in total R&D expenditure during the period as medium R&D industries. Finally, we classify the fifty-four 2-digit SIC code industries with less than $100 million in total R&D expenditure during the period as low R&D industries.

Table 4 presents the differences reported for the full sample in Table 3 across the three industry groups. The differences in the post-SOX values and the corresponding values over 1998-2000 and 1995-1997 are reported in Panels A and B, respectively. Whereas a significant decline in the R&D to assets and capital expenditures to assets ratios of U.S. versus U.K. firms exists for the full sample, the results within the subgroups of industries are weaker. For most subgroups the decline in R&D and capital expenditures is larger in the U.S. after SOX, but for most subgroups the differences are not significant at the 0.05 level. In contrast, the median increase in cash holdings of U.S.

firms is significantly higher after SOX than the corresponding change in the cash holdings of U.K. firms for most subgroups.

Stock-based measures of risk

Evidence on changes in the stock-based measures of risk after SOX are contained in Tables 5 and 6.

For each firm, we calculate three measures of risk over three four-year periods. The risk measures are the standard deviation of monthly stock returns, the estimated beta from a one factor market model in which the firm's returns are regressed on the corresponding returns of the MSCI World Index, and the root mean square error from this market model.

The three risk measures are estimated over one four-year period, 2003-2006, following the adoption of SOX, and two four-year periods, 1994-1997 and 1998-2001, before the adoption of SOX. We use four year periods for this analysis because unlike the accounting data, which for many firms was only available on the Thomson database for three years after SOX, stock return data was available on Datastream for four years after SOX. Hence, in order to take advantage of additional post-SOX data we chose to use a four-year period after SOX. To make the post-SOX data comparable to pre-SOX data, we also chose to use four year periods in the pre-SOX period.

Table 5 reveals that all three stock-based risk measures declined significantly for U.S. firms as compared with U.K. firms after the adoption of SOX. The median standard deviation of monthly stock returns declined by 0.0506 for the U.S. sample in the post-SOX period as compared with the pre-SOX period of 1998-2001. The corresponding decline for the U.K. sample is 0.0326. The difference in the median declines is significant

at the 0.01 level. The median standard deviation of monthly stock returns also declined more significantly for U.S. firms in the post-SOX period as compared with the pre-SOX period of 1994-1997.

The median beta of U.S. firms vis-à-vis the MSCI World Index increased by 0.27 in the post-SOX period as compared with the pre-SOX period of 1998-2000. The corresponding median increase for the U.K. sample is 0.3411. This difference in median values also is significant at the 0.05 level. Similarly, the median beta of U.S. firms increased during the post-SOX period as compared with the pre-SOX period of 1994-1997, but this difference was significantly less (at the 0.05 level) than the corresponding increase for the U.K. sample.

Finally, the median root mean square error, the measure of firm specific risk, declined by 0.0489 for the U.S. sample in the post-SOX period as compared with the pre-SOX period of 1998-2001. The corresponding decline for the U.K. sample is 0.0320. This difference in the median declines across the two samples is significant at the 0.01 level. The two median declines are smaller when measured against the pre-SOX period of 1994-1997, but here again the decline is significantly larger for the U.S. versus the U.K. sample.

Table 6 presents the differences reported for the full sample in Table 5 for the three industry subgroups. The stock-based risk measures generally declined significantly more for the U.S. sample versus the U.K. sample across the industry groups.

All three risk measures declined significantly more, at the 0.05 level, for the U.S. sample as compared with the U.K. sample for the high R&D group. For example, when compared against the 1998-2001 period, the median standard deviation of returns for U.S.

firms in the high R&D subgroup declined by 0.0803 after SOX, as compared with a decline of only 0.0509 for the U.K. sample. The corresponding median beta increased by only 0.0401 for the U.S. sample, as compared with an increase of 0.2819 for the U.K. sample. The corresponding median root mean square error declined in the post-SOX period by 0.0749 for the U.S. sample as compared with a decline of only 0.0486 for the U.K. sample. Similar results obtain when the post-SOX period is compared with the pre-SOX period of 1994-1997. The two other stock-based risk measures also decline significantly more for the U.S. versus the U.K. sample in the post-SOX period across the moderate and low R&D subgroups.

4. R&D expenditures, IPOs, and SOX

In addition to examining whether measures of risk-taking by U.S. companies changed significantly after SOX, we examine whether firms operating in risky industries were more likely to go public in the U.K. versus the U.S. after SOX. We first describe the sample and data used in the analysis and then present the results.

Sample and data

The sample of U.S. and U.K. IPOs is collected from the Securities Data Company's (SDC) Global New Issues Database. The sample consists of all completed common stock IPOs for the period 1990 through 2006 where the listing exchange is located in either the U.S. or U.K. The sample includes 9,262 IPOs, consisting of 1,882 U.K. IPOs (20% of the sample) and 7,380 U.S. IPOs (80% of the sample).

Table 7 contains summary information on characteristics of the IPOs before and after SOX. Of the 7,380 U.S. IPOs, 6,417, or 87%, occurred before SOX. Of the 1,882

U.K. IPOs, 1,284, or 68%, occurred before SOX. Hence, a substantially higher percentage of U.K. IPOs occurred after SOX than in the U.S.

Of the 6,417 U.S. IPOs that occurred before SOX, 2,472, or 39%, were done by firms in high R&D industries (using the taxonomy of industries described above). Of the 963 U.S. IPOs after SOX, only 283, or 29%, were done by firms in high R&D industries. Hence, the percentage of U.S. IPOs accounted for by firms in high R&D industries declined substantially after SOX. In contrast, there was little change in this percentage for the U.K. sample, from 24% before SOX (i.e., 314 of 1,284 IPOs) to 22% after SOX (i.e., 154 of 598 IPOs).

Similarly, the percentage of U.S. IPOs accounted for by firms in low R&D industries increased substantially after SOX, from 39% (i.e., 2,501 of 6,417 IPOs) to 52% (i.e., 501 of 963 IPOs). The percentage of U.K. IPOs accounted for by firms in low R&D industries actually declined from 53% before to 49% after SOX. Hence, the difference in these percentages across the U.S. and U.K. changed substantially from before to after SOX.

Total proceeds raised in IPOs differ substantially across the two samples. Over the entire period of 1990-2006, total proceeds raised in U.S. IPOs were $911 billion, as compared with $186 billion in U.K. IPOs. Of the total proceeds, 75% were raised before SOX for the U.S. sample, versus 79% for the U.K. sample. The percentage of proceeds raised by firms in high R&D industries declined substantially for the U.S. sample after SOX, from 34% (i.e., $229,088 of $680,840) to 17% (i.e., $39,259 of $230,286). In contrast, this percentage increased slightly in the U.K., from 10% (i.e., $14,690 of $147,639) to 12% (i.e., $4,484 of $38,687).

A dramatic difference exists in the percentage of proceeds raised by firms in low risk industries in the U.S. and U.K. before and after SOX. For the U.S. sample of IPOs, this percentage increased substantially from 39% before SOX (i.e., $263,519 of $680,840) to 65% after SOX (i.e., $148,609 of $230,286). For the U.K. sample, this percentage decreased substantially, from 59% before SOX (i.e., $87,203 of $147,639) to 40% after SOX (i.e., $15,512 of $38,687).

To the extent that SOX has dampened risk-taking by U.S. corporations, it is possible that the U.S. IPO market would soften as a result. In particular, private firms in the U.S. may opt more often to remain private vis-à-vis go public in the post-SOX era.

Figure 1 shows the relative percentages of IPOs going public in the U.S. versus the U.K. each year during the period of 1990 through 2006. It can be seen that the relative percentage of U.K. IPOs has increased dramatically, suggesting that more U.S. firms are opting to remain private in response to the SOX legislation. It is possible, however, that the change in relative percentages shown in Figure 1 is not due to a reduction in U.S. IPOs, but rather an increase in the number of U.K. IPOs vis-à-vis the number of U.S. IPOs.

Figure 2 reveals that the number of IPOs in the U.S. has decreased substantially post SOX, whereas the number of IPOs in the U.K. is not remarkably different from historic levels. Thus, Figure 2 strengthens the notion that fewer U.S. firms are going public after SOX.

Another potential explanation for the rise in the relative percentage of U.K. IPOs shown in Figure 1 and the decrease in U.S. IPOs shown in Figure 2 is that the reduction in U.S. IPO activity occurred because of a downturn in the U.S. stock market, not SOX.

Although there is considerable empirical evidence relating IPO volume to stock market performance, for the U.S. stock market to explain the relative changes shown in Figures 1 and 2 between U.S. and U.K. IPO markets the U.K. stock market cannot be highly correlated with the U.S. stock market. On the contrary, Figure 3 shows that the U.K. stock market is highly correlated with the U.S. stock market, represented by the FTSE All Share and the CRSP Value Weighted indices respectively. The figure clearly shows that the two stock markets run in parallel through time. The correlation in returns over the 1990 through 2006 time period is 0.73. Moreover to the extent that a difference in stock market performances explains the difference in IPO markets, Figure 3 suggests that the U.S. IPO market, and not the U.K. IPO market, should be gaining in relative strength since the U.S. stock market has been outpacing the U.K. stock market during the post-SOX period.

Overall, the summary data discussed above suggests that IPO activity has decreased in the U.S. vis-à-vis the U.K. since SOX, especially among firms operating in high R&D industries. We next turn to empirical tests of this proposition.

Empirical results

Table 8 presents results from a logit model in which we estimate the likelihood that a firm goes public in the U.K. versus the U.S. over the period of 1990-2006. The dependent variable takes the value of 1 if the IPO occurs in the U.K. and 0 if the IPO occurs in the U.S. The independent variables include the log of proceeds raised in the IPO, dummy variables for whether or not the firm is in a high or moderate R&D industry, a dummy variable if the IPO occurred after SOX, and two interaction variables consisting

of the product of the post-SOX dummy variable and the dummy variables for firms in high and moderate R&D industries.

All of the independent variables enter with estimated coefficients that are significant at the 0.01 level. Log of proceeds enters with a negative coefficient, indicating that larger firms are more likely to go public in the U.S. Both dummy variables for firms operating in high and moderate R&D industries enter with negative and significant coefficients (-0.865 and -0.423, respectively), indicating that compared with low R&D firms these firms were more likely to do IPOs in the U.S.

The dummy variable for post-SOX IPOs enters with a positive coefficient, indicating that in the years after SOX there was an increase in the likelihood that firms would do IPOs in the U.K. The two variables that interact the post-SOX dummy variable with high and moderate R&D enter with positive coefficients (0.542 and 0.707, respectively), indicating that after SOX, firms operating in high and moderate R&D industries were more likely to do IPOs in the U.K. This result is consistent with the proposition that SOX has had a chilling effect on corporate risk-taking and that, at the margin, firms operating in risky industries have increasingly conducted IPOs in the U.K. since SOX.

5. Concluding comments

This paper empirically examines whether risk-taking for U.S. firms vis-à-vis U.K. firms decreases between the pre-SOX and post-SOX periods. We approach the question from three different angles and find the results from each tell a similar story. Measures of risk for U.S. firms are generally lower in the post-SOX period than in the pre-SOX period. Moreover, decreases (increases) in risk measures for U.S. firms between the pre-

SOX and post-SOX periods are generally larger (smaller) than decreases (increases) in risk measures for U.K. firms between the same periods. These results are consistent with the hypothesis that SOX has chilled risk-taking by U.S. corporations.

First, we investigate accounting-based measures of risk. We find that since the adoption of SOX U.S. companies have (i) significantly reduced expenditures on R&D, (ii) significantly reduced capital expenditures, and (iii) significantly increased holdings of cash relative to U.K. firms. Subsequent to SOX U.S. firms have shied away from investments in R&D and capital expenditures in comparison to U.K. firms, preferring to hold more cash.

Second, we analyze stock-based measures of risk. We find that total risk and its two components, market risk and firm specific risk, have also decreased relative to U.K. firms since the adoption of SOX. Interestingly, the results are strongest in the high risk, R&D intensive industries. Hence, in addition to reducing risky investment subsequent to SOX, U.S. firms have reduced their equity risk relative to U.K. firms, particularly among those firms in riskier industries.

Finally, using a large sample of IPOs in the U.S. and U.K. during the period of 1990-2006, we find that the likelihood that an IPO occurred in the U.K. increased significantly after SOX and that this effect is especially pronounced for firms operating in high risk industries. This result is consistent with the view that SOX discourages risky firms from raising capital in U.S. public equity markets and it provides additional support for the view that SOX has had a chilling effect on risk-taking behavior by publicly traded U.S. corporations.

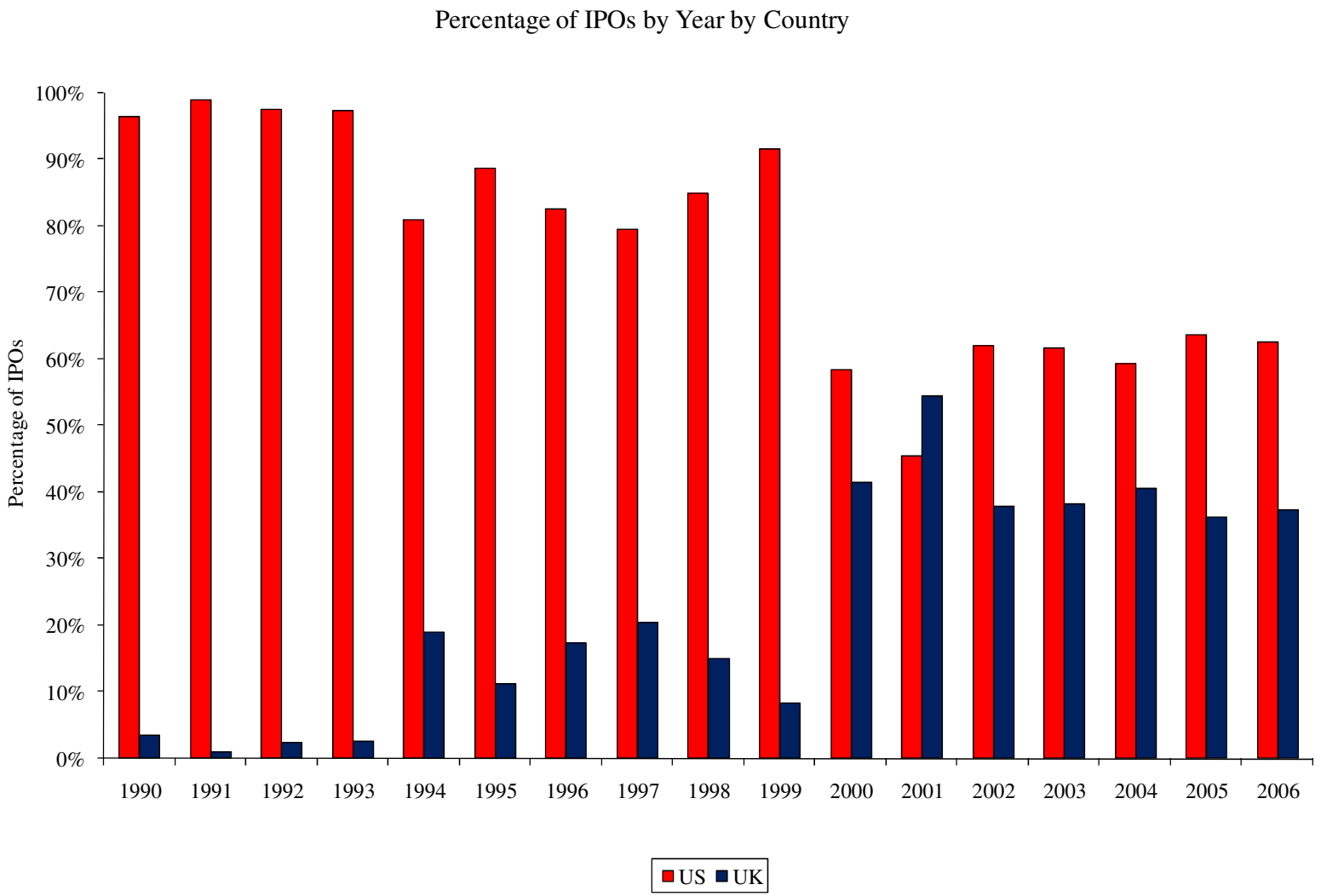


Fig. 1 Percentage of IPOs by Year by Country

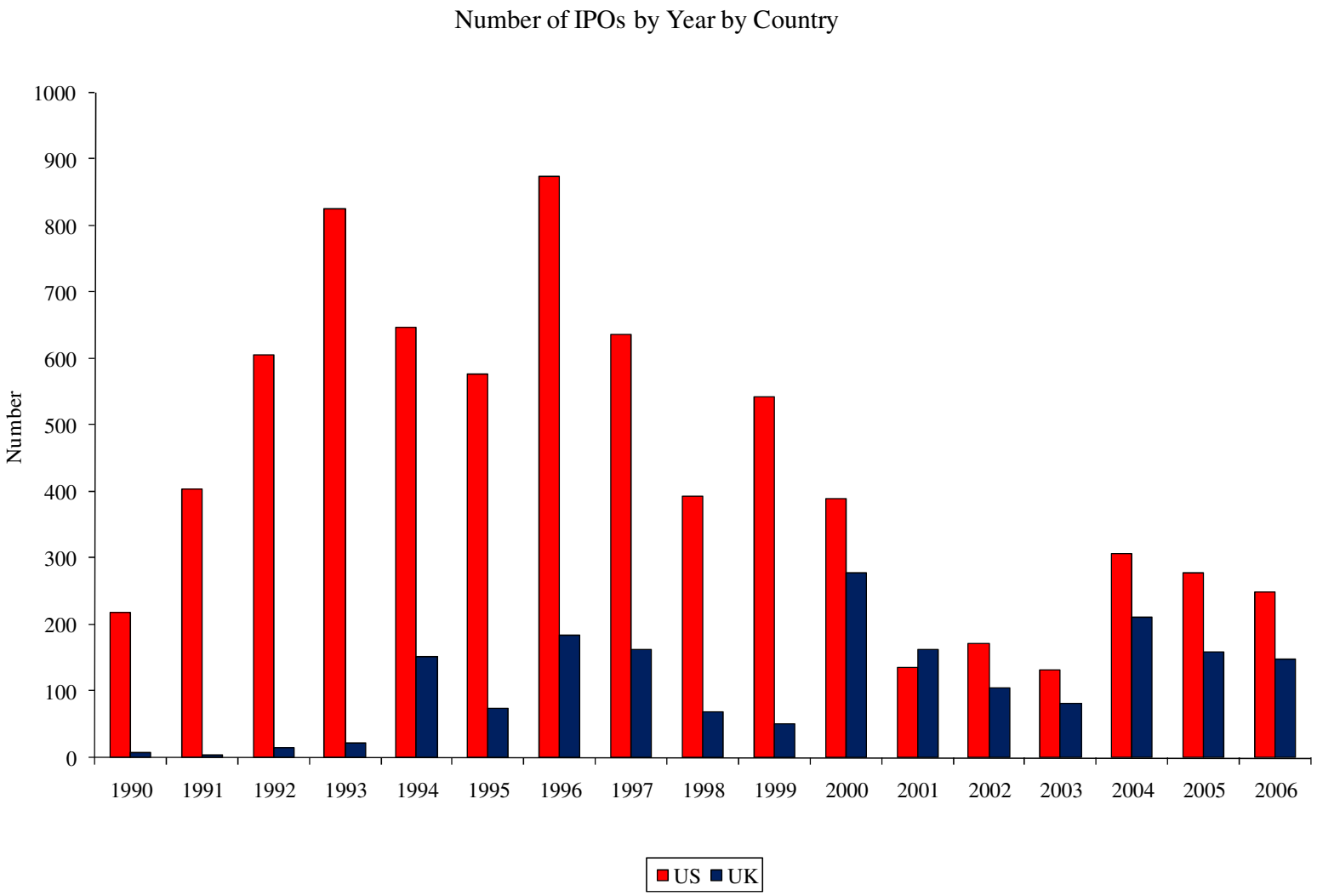


Fig. 2 Number of IPOs by Year by Country

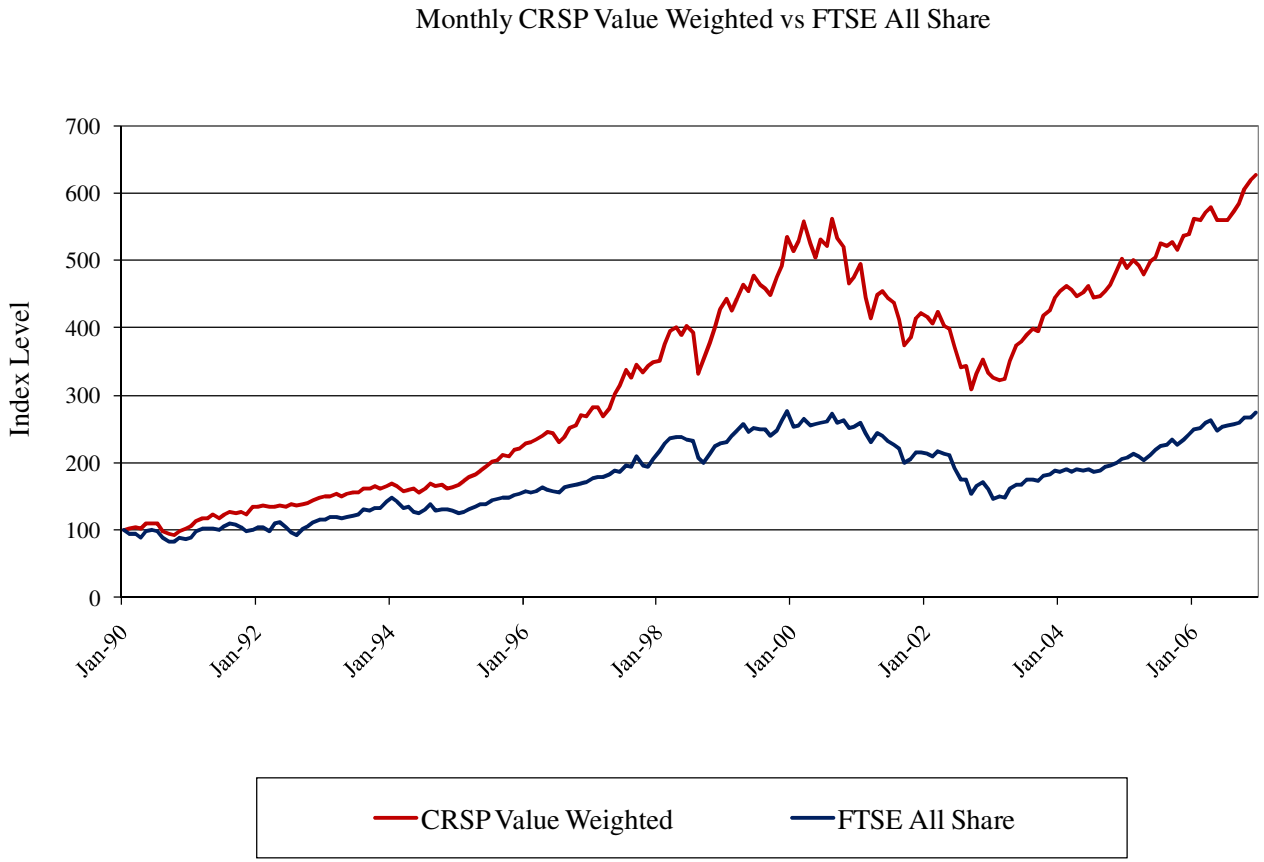


Fig. 3 Monthly CRSP Value Weighted and the FTSE All Share Indices Returns

Table 1: Industry Distribution

This table details the distribution of firms across industries for the U.K. sample and the U.S. sample. The first column lists the industry description for the 2-digit SIC code. The next two columns tabulate the number of firms in each industry for the U.K sample and the percentage of the entire U.K. sample represented by that industry. The last two columns repeat the analysis for the U.S. sample.

Industry Description	UK Firms	% of UK	US Firms	% of US
Agricultural production- crops	2	0.2%	10	0.2%
Agricultural production- livestock	0	0.0%	4	0.1%
Agricultural services	2	0.2%	5	0.1%
Forestry	3	0.3%	1	0.0%
Metal mining	6	0.6%	20	0.5%
Coal mining	3	0.3%	5	0.1%
Oil and gas extraction	16	1.6%	133	3.1%
Nonmetallic minerals, except fuels	2	0.2%	5	0.1%
General building contractors	25	2.5%	28	0.7%
Heavy construction contractors	1	0.1%	8	0.2%
Special trade contractors	6	0.6%	13	0.3%
Food and kindred products	21	2.1%	81	1.9%
Tobacco manufactures	3	0.3%	5	0.1%
Textile mill products	7	0.7%	14	0.3%
Apparel and other textile products	11	1.1%	37	0.9%
Lumber and wood products	1	0.1%	15	0.4%
Furniture and fixtures	3	0.3%	21	0.5%
Paper and allied products	6	0.6%	32	0.8%
Printing and publishing	19	1.9%	43	1.0%
Chemicals and allied products	43	4.3%	306	7.2%
Petroleum and coal products	2	0.2%	17	0.4%
Rubber and misc. plastics products	7	0.7%	39	0.9%
Leather and leather products	2	0.2%	13	0.3%
Stone, clay, glass, and concrete prod.	14	1.4%	24	0.6%
Primary metal industries	8	0.8%	53	1.3%
Fabricated metal products	18	1.8%	56	1.3%
Industrial machinery and equipment	17	1.7%	207	4.9%
Electrical and electronic equipment	36	3.6%	350	8.3%
Transportation equipment	14	1.4%	88	2.1%
Instruments and related products	26	2.6%	314	7.4%
Miscellaneous manufacturing industries	9	0.9%	47	1.1%
Railroads	1	0.1%	9	0.2%
Local and interurban passenger transit	4	0.4%	1	0.0%
Motor freight transportation and warehousing	3	0.3%	25	0.6%
Water transportation	5	0.5%	12	0.3%
Transportation by air	7	0.7%	30	0.7%
Pipelines, except natural gas	0	0.0%	5	0.1%
Transportation services	8	0.8%	15	0.4%
Communications	14	1.4%	142	3.3%

Electric, gas, and sanitary services	16	1.6%	155	3.7%
Wholesale trade--durable goods	35	3.5%	112	2.6%
Wholesale trade--nondurable goods	14	1.4%	67	1.6%
Building materials, hardware, garden supply	3	0.3%	5	0.1%
General merchandise stores	5	0.5%	25	0.6%
Food stores	6	0.6%	18	0.4%
Automotive dealers and gas service stations	5	0.5%	17	0.4%
Apparel and accessory stores	9	0.9%	50	1.2%
Furniture, home furnishings and equip. stores	2	0.2%	26	0.6%
Eating and drinking places	17	1.7%	66	1.6%
Miscellaneous retail	18	1.8%	63	1.5%
Depository institutions	2	0.2%	3	0.1%
Nondepository credit institutions	10	1.0%	38	0.9%
Security, commodity brokers, and services	13	1.3%	55	1.3%
Insurance carriers	0	0.0%	10	0.2%
Insurance agents, brokers, and service	3	0.3%	9	0.2%
Real estate	47	4.8%	57	1.3%
Holding and other investment offices	182	18.4%	159	3.8%
Hotels and other lodging places	8	0.8%	25	0.6%
Personal services	3	0.3%	12	0.3%
Business services	116	11.7%	676	15.9%
Automotive repair, services, and parking	4	0.4%	16	0.4%
Miscellaneous repair services	0	0.0%	7	0.2%
Motion pictures	9	0.9%	25	0.6%
Amusement and recreational services	24	2.4%	53	1.3%
Health services	1	0.1%	85	2.0%
Legal services	0	0.0%	1	0.0%
Educational services	5	0.5%	17	0.4%
Social services	3	0.3%	9	0.2%
Museums, art galleries, botanical gardens	1	0.1%	0	0.0%
Engineering and management services	53	5.4%	128	3.0%
Miscellaneous services	0	0.0%	5	0.1%
Justice, public order, and safety	0	0.0%	1	0.0%
Environmental quality and housing	0	0.0%	3	0.1%
Government & government agencies	0	0.0%	8	0.2%
All Industries	**989**	**100.0%**	**4,239**	**100.0%**

Table 2: Summary Statistics - Accounting and Stock-Based Variables

Panel A summarizes the key accounting variables for the three periods 1995-1997, 1998-2000, and 2003-2005. The ratios of CAPEX, R&D, CASH, and EBIT to ASSETS are calculated for each firm-year and the mean value for each firm over the three year period is computed. Panel B summarizes the key stock-based risk variables for the three periods 1994-1997, 1998-2001, and 2003-2006. Each firm's standard deviation of returns and market model estimates of firm beta and root mean square error are estimated over each four year period using monthly returns. The first two columns tabulate the median value within each country. The third column lists the difference between the median for the U.S. and the median for the U.K. The final column lists the p-value from Wilcoxon rank sum tests for differences between the countries. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

Panel A	**US**	**UK**	**US - UK**	**p-value**
RD/ASSETS				
1995 - 1997	0.0705	0.0189	0.0516	0.000***
1998 - 2000	0.0782	0.0288	0.0494	0.000***
2003 - 2005	0.0720	0.0334	0.0386	0.000***
CAPEX/ASSETS				
1995 - 1997	0.0542	0.0477	0.0065	0.000***
1998 - 2000	0.0488	0.0428	0.0060	0.000***
2003 - 2005	0.0303	0.0253	0.0050	0.000***
CASH/ASSETS				
1995 - 1997	0.0947	0.0826	0.0121	0.002***
1998 - 2000	0.0922	0.0832	0.0091	0.001***
2003 - 2005	0.1149	0.0796	0.0353	0.000***
EBIT/ASSETS				
1995 - 1997	0.0864	0.0833	0.0032	0.194
1998 - 2000	0.0575	0.0672	-0.0097	0.000***
2003 - 2005	0.0470	0.0420	0.0049	0.041**
Panel B	**US**	**UK**	**US - UK**	**p-value**
STD RETURNS				
1994 - 1997	0.1291	0.0746	0.0546	0.000***
1998 - 2001	0.2074	0.1225	0.0849	0.000***
2003 - 2006	0.1394	0.0870	0.0524	0.000***
BETA				
1994 - 1997	0.6534	0.4600	0.1934	0.000***
1998 - 2001	0.9403	0.7012	0.2391	0.000***
2003 - 2006	1.2314	1.0870	0.1444	0.000***
RMSE				
1994 - 1997	0.1260	0.0719	0.0541	0.000***
1998 - 2001	0.1990	0.1173	0.0816	0.000***
2003 - 2006	0.1331	0.0828	0.0503	0.000***

Table 3: Changes in Accounting Measures of Risk – All Firms

This table compares pre-SOX to post-SOX changes in accounting measures of risk in US firms to the changes in UK firms using all firms in our sample. The first column compares the Post-SOX 2003-2005 period to the Pre-SOX 1998-2000 period. The last column compares the Post-SOX 2003-2005 period to the Pre-SOX 1995-1997 period. The variables of interest are the firm level differences in the ratio of R&D expenditures to assets (RD/ASSETS), the ratio of capital expenditures to assets (CAPEX/ASSETS), the ratio of CASH to assets (CASH/ASSETS), and the ratio of EBIT to assets (EBIT/ASSETS) between the periods. For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	Post-SOX vs Pre-SOX 1998-2000	**Post-SOX vs Pre-SOX 1995-1997**
RD/ASSETS	[US LOWER]	[US LOWER]
p-value	*0.027***	*0.006****
Median Diff. UK	-0.00045	-0.00069
Median Diff. US	-0.00250	-0.00361
# Obs. - UK	234	159
# Obs. - US	1,746	953
CAPEX/ASSETS	[US LOWER]	[US LOWER]
p-value	*0.180*	*0.001****
Median Diff. UK	-0.00927	-0.01076
Median Diff. US	-0.01379	-0.01783
# Obs. - UK	989	716
# Obs. - US	4,239	2,378
CASH/ASSETS	[US HIGHER]	[US HIGHER]
p-value	*0.000****	*0.000****
Median Diff. UK	-0.00266	-0.00313
Median Diff. US	0.00780	0.00758
# Obs. - UK	989	716
# Obs. - US	4,239	2,378
EBIT/ASSETS	[US HIGHER]	[US HIGHER]
p-value	*.002****	*0.279*
Median Diff. UK	-0.01226	-0.02014
Median Diff. US	-0.01369	-0.02560
# Obs. - UK	988	714
# Obs. - US	4,091	2,284

Table 4 Panel A: Changes in Accounting Measures of Risk - By R&D Group

Panel A compares the changes in accounting measures of risk between the post-SOX 2003-2005 and pre-SOX 1998-2000 periods in US firms to the changes in UK firms for each of the three R&D groups. The variables of interest are the firm level differences in the ratio of R&D expenditures to assets (RD/ASSETS), the ratio of capital expenditures to assets (CAPEX/ASSETS), the ratio of CASH to assets (CASH/ASSETS), and the ratio of EBIT to assets (EBIT/ASSETS) between the periods. For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms for each R&D group using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	High R&D	**Mod. R&D**	**Low R&D**
RD/ASSETS	[US LOWER]	[US LOWER]	[US HIGHER]
p-value	*0.206*	*0.067**	*0.723*
Median Diff. UK	-0.00074	-0.00038	-0.00180
Median Diff. US	-0.00595	-0.00137	0.00048
# Obs. - UK	124	92	18
# Obs. - US	1,189	445	112
CAPEX/ASSETS	[US HIGHER]	[US HIGHER]	[US LOWER]
p-value	*0.085**	*0.856*	*0.623*
Median Diff. UK	-0.02197	-0.01276	-0.00018
Median Diff. US	-0.01933	-0.01252	-0.00908
# Obs. - GBR	188	278	523
# Obs. - USA	1,584	1,306	1,349
CASH/ASSETS	[US HIGHER]	[US HIGHER]	[US HIGHER]
p-value	*0.165*	*0.000***	*0.001***
Median Diff. UK	-0.01973	-0.00685	-0.00030
Median Diff. US	0.00792	0.00703	0.00861
# Obs. - UK	188	278	523
# Obs. - US	1,584	1,306	1,349
EBIT/ASSETS	[US HIGHER]	[US HIGHER]	[US HIGHER]
p-value	*0.003****	*0.001****	*0.931*
Median Diff. UK	-0.05635	-0.03238	-0.00393
Median Diff. US	-0.01074	-0.01630	-0.01296
# Obs. - UK	188	277	523
# Obs. - US	1,499	1,284	1,308

Table 4 Panel B: Changes in Accounting Measures of Risk - By R&D Group

Panel B compares the changes in accounting measures of risk between the post-SOX 2003-2005 and pre-SOX 1995-1997 periods in US firms to the changes in UK firms for each of the three R&D groups. The variables of interest are the firm level differences in the ratio of R&D expenditures to assets (RD/ASSETS), the ratio of capital expenditures to assets (CAPEX/ASSETS), the ratio of CASH to assets (CASH/ASSETS), and the ratio of EBIT to assets (EBIT/ASSETS) between the periods. For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms for each R&D group using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	High R&D	Mod. R&D	Low R&D
RD/ASSETS	[US LOWER]	[US LOWER]	[US HIGHER]
p-value	*0.085**	*0.033***	*0.803*
Median Diff. UK	0.00047	-0.00104	-0.00670
Median Diff. US	-0.00702	-0.00259	-0.00133
# Obs. - UK	73	74	12
# Obs. - US	624	281	48
CAPEX/ASSETS	[US HIGHER]	[US LOWER]	[US LOWER]
p-value	*0.776*	*0.353*	*0.121*
Median Diff. UK	-0.02623	-0.01911	0.00000
Median Diff. US	-0.02218	-0.01913	-0.01001
# Obs. - UK	118	224	374
# Obs. - US	790	799	789
CASH/ASSETS	[US HIGHER]	[US HIGHER]	[US HIGHER]
p-value	*0.005****	*0.004****	*0.002****
Median Diff. UK	-0.04286	-0.01129	0.00068
Median Diff. US	0.01471	0.00479	0.00853
# Obs. - UK	118	224	374
# Obs. - US	790	799	789
EBIT/ASSETS	[US HIGHER]	[US HIGHER]	[US HIGHER]
p-value	*0.012***	*0.432*	*0.255*
Median Diff. UK	-0.08913	-0.03678	-0.01065
Median Diff. US	-0.03689	-0.02864	-0.01523
# Obs. - UK	118	223	373
# Obs. - US	740	783	761

Table 5: Changes in Stock-Based Measures of Risk – All Firms

This table compares the pre-SOX to post-SOX changes in the stock-based measures of risk. The first column compares the Post-SOX 2003-2006 period to the Pre-SOX 1998-2001 period. The last column compares the Post-SOX 2003-2006 period to the Pre-SOX 1994-1997 period. The variables of interest are firm level differences in monthly standard deviation of returns (STD of Returns) between the periods, and firm level differences in the market model estimates of beta (Beta) and the root mean square error (RMSE) between the periods For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	Post-SOX vs Pre-SOX 1998-2001	**Post-SOX vs Pre-SOX 1994-1997**
STD of Returns	[US LOWER]	[US LOWER]
p-value	*0.000****	*0.000****
Median Diff. UK	-0.0326	0.0027
Median Diff. US	-0.0506	-0.0035
# Obs. - UK	989	716
# Obs. - US	4,239	2,378
Beta	[US LOWER]	[US LOWER]
p-value	*0.014***	*0.047***
Median Diff. UK	0.3411	0.5760
Median Diff. US	0.2700	0.5493
# Obs. - UK	989	716
# Obs. - US	4,239	2,378
RMSE	[US LOWER]	[US LOWER]
p-value	*0.000****	*0.000****
Median Diff. UK	-0.0320	-0.0002
Median Diff. US	-0.0489	-0.0059
# Obs. - UK	989	716
# Obs. - US	4,239	2,378

Table 6 Panel A: Changes in Stock-Based Measures of Risk – By R&D Group

Panel A compares the changes in the stock-based measures of risk between the post-SOX 2003-2006 and pre-SOX 1998-2001 periods in US firms to the changes in UK firms for each of the three R&D groups. The variables of interest are firm level differences in monthly standard deviation of returns (STD of Returns) between the periods, and firm level differences in the market model estimates of beta (Beta) and the root mean square error (RMSE) between the periods For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms for each R&D group using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	High R&D	**Mod. R&D**	**Low R&D**
STD of Returns	[US LOWER]	[US LOWER]	[US LOWER]
p-value	*0.002***	*0.054**	0.000***
Median Diff. UK	-0.0509	-0.0315	-0.0269
Median Diff. US	-0.0803	-0.0388	-0.0397
# Obs. - UK	188	278	523
# Obs. - US	1,584	1,306	1,349
Beta	[US LOWER]	[US LOWER]	[US HIGHER]
p-value	*0.016***	*0.589*	*0.793*
Median Diff. UK	0.2819	0.4361	0.3128
Median Diff. US	0.0401	0.4126	0.3470
# Obs. - UK	188	278	523
# Obs. - US	1,584	1,306	1,349
RMSE	[US LOWER]	[US LOWER]	[US LOWER]
p-value	*0.004****	*0.047***	*0.000****
Median Diff. UK	-0.0486	-0.0330	-0.0272
Median Diff. US	-0.0749	-0.0381	-0.0388
# Obs. - UK	188	278	523
# Obs. - US	1,584	1,306	1,349

Table 6 Panel B: Changes in Stock-Based Measures of Risk – By R&D Group

Panel B compares the changes in the stock-based measures of risk between the post-SOX 2003-2006 and pre-SOX 1994-1997 periods in US firms to the changes in UK firms for each of the three R&D groups. The variables of interest are firm level differences in monthly standard deviation of returns (STD of Returns) between the periods, and firm level differences in the market model estimates of beta (Beta) and the root mean square error (RMSE) between the periods For each firm we calculate the difference in the mean value of the variable between the early period and the later period. A negative difference indicates the variable declined in the post-SOX period. We then compare the distributions of differences of U.S. and U.K. firms for each R&D group using Wilcoxon rank sum tests. The bracketed terms describe whether the U.S. differences were higher or lower than expected relative to the U.K. differences based on the sum of scores. The p-values for the significance of the tests are in italics. The median difference for each country and the number of observations for each country are also tabulated. ***, **, * indicate significance at the 1%, 5%, and 10% levels respectively.

	High R&D	**Mod. R&D**	**Low R&D**
STD of Returns	[US LOWER]	[US LOWER]	[US LOWER]
p-value	*0.000****	*0.322*	*0.046***
Median Diff. UK	0.0112	0.0018	0.0015
Median Diff. US	-0.0116	0.0004	-0.0020
# Obs. - UK	118	224	374
# Obs. - US	790	799	789
Beta	[US LOWER]	[US LOWER]	[US LOWER]
p-value	*0.005****	*0.014***	*0.824*
Median Diff. UK	1.0244	0.6270	0.4893
Median Diff. US	0.6536	0.5369	0.4991
# Obs. - UK	118	224	374
# Obs. - US	790	799	789
RMSE	[US LOWER]	[US LOWER]	[US LOWER]
p-value	*0.000****	*0.418*	*0.113*
Median Diff. UK	0.0091	0.0012	-0.0019
Median Diff. US	-0.0153	-0.0012	-0.0042
# Obs. - UK	118	224	374
# Obs. - US	790	799	789

Table 7: Proceeds for Firms Going Public in the U.K. vs. the U.S.

This table presents total proceeds in millions of end-of-year 2005 CPI-adjusted U.S. dollars. The sample includes 9,262 IPOs from 1990 through 2006.

	1990-2006	Pre SOX (1990-2002)				Post SOX (2003-2006)			
Panel A: U.S. IPOs	**All Deals**	**All Deals**	**High R&D**	**Mod. R&D**	**Low R&D**	**All Deals**	**High R&D**	**Mod. R&D**	**Low R&D**
Number of IPOs	7,380	6,417	2,472	1,444	2,501	963	283	179	501
Sum of Proceeds in Million of U.S. Dollars	911,126	680,840	229,088	188,233	263,519	230,286	39,259	42,418	148,609
Mean Proceeds in Million of U.S. Dollars	123	106	93	130	105	239	139	237	297
Median Proceeds in Million of U.S. Dollars	41	35	32	33	43	122	72	135	173
	1990-2006	**Pre SOX (1990-2002)**				**Post SOX (2003-2006)**			
Panel B: U.K. IPOs	**All Deals**	**All Deals**	**High R&D**	**Mod. R&D**	**Low R&D**	**All Deals**	**High R&D**	**Mod. R&D**	**Low R&D**
Number of IPOs	1,882	1,284	314	287	683	598	154	153	291
Sum of Proceeds in Million of U.S. Dollars	186,326	147,639	14,690	45,746	87,203	38,687	4,484	18,691	15,512
Mean Proceeds in Million of U.S. Dollars	99	115	47	159	128	65	29	122	53
Median Proceeds in Million of U.S. Dollars	14	17	13	16	20	10	11	11	9

Table 8: Logistic Regression of Going Public in the U.K. vs. the U.S.

This table presents a logistic regression that models the occurrence of an IPO in the U.K. vs. the U.S. The sample includes 9,258 IPOs from 1990 through 2006. There are 1,878 U.K. IPOs and 7,380 U.S. IPOs. The dependent variable is 1 for U.K. IPOs and 0 for U.S. IPOs. The logit model estimates the probability of a U.K. IPO. Log of Proceeds is the natural log of the total proceeds in millions of end-of-year 2005 CPI-adjusted U.S. dollars. Top R&D Group is equal to 1 for IPOs in the Top R&D group. Mid R&D Group is equal to 1 for IPOs in the Mid R&D group. Post SOX is equal to 1 for IPOs taking place after 2002 or from 2003 through 2006. P-values refer to t-tests of parameter estimates equal to zero. ***, **, * Significant at the one, five, and ten percent levels, respectively.

Logistic regression of U.K. vs. U.S. IPOs			
	Parameter Estimate	**Standard Error**	**P-value**
Intercept	0.460	0.076	0.0001***
Log of Proceeds in Million of U.S. Dollars	-0.543	0.020	0.0001***
High R&D Group	-0.865	0.077	0.0001***
Mod. R&D Group	-0.423	0.082	0.0001***
Post SOX	1.138	0.096	0.0001***
High R&D Group * Post SOX	0.542	0.156	0.0005***
Mod. R&D Group * Post SOX	0.707	0.169	0.0001***
Correct predictions	72.5%		
Number of observations	9,258		

Anexo IV – Segundo estudo – “*Why Enterprise Risk Management is Vital* ” de *Steve G. Sutton*

Why Enterprise Risk Management is Vital

Learning from Company Experiences With Sarbanes-Oxley Section 404 Compliance

Principal Investigator and Project Manager
Steve G. Sutton

Co-Principal Investigators
Vicky Arnold
Tanya Benford
Joseph Canada

February 2009

The Institute of Internal Auditors Research Foundation

Disclosure

The IIARF publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The mission of The IIARF is to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN 978-0-89413-671-9
03/09 First Printing

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report documents the findings from a study funded by The Institute of Internal Auditors Research Foundation (IIARF). The authors wish to thank The IIARF for its generous funding and support of our research, IIARF members who participated in the survey portion of the study, and the organizations that participated in the case studies and exhibited a great willingness to share their experiences. Finally, we also thank Randy Kuhn for his research assistance during the early stages of this project.

ABOUT THE AUTHORS

Steve G. Sutton is KPMG Professor of Accounting in the Kenneth G. Dixon School of Accounting at the University of Central Florida and Professorial Fellow in the Department of Accounting and Business Information Systems at the University of Melbourne (Australia). He serves as editor of the *International Journal of Accounting Information Systems*. Professor Sutton has authored and co-authored five books, four research monographs, and more than 90 articles in a broad range of accounting (e.g., *Auditing: A Journal of Practice & Theory*, *Behavioral Research in Accounting*, *Journal of the American Taxation Association*), information systems (e.g., *MIS Quarterly*, *Journal of the Association for Information Systems*, *Decision Sciences*), and accounting information systems journals (e.g., *Journal of Information Systems*, *Journal of Emerging Technologies in Accounting*). His research has been funded by grants from The IIARF, the KPMG Foundation, Australian Research Council, and the Financial Industry Regulatory Authority (FINRA) Investor Education Foundation. Prior IIARF grants have resulted in one monograph widely used by internal audit departments to develop quality management programs, and a second monograph currently available to internal audit departments and others through The Institute of Internal Auditors (IIA) as a part of its enterprise risk management series.

Vicky Arnold is Ernst & Young Professor of Accounting in the Kenneth G. Dixon School of Accounting and professorial fellow in the Department of Accounting and Business Information Systems at the University of Melbourne. She is editor of *Advances in Accounting Behavioral Research*. Professor Arnold has authored and co-authored more than 50 articles in a broad range of accounting (e.g., *Auditing: A Journal of Practice & Theory*, *Behavioral Research in Accounting*, *Journal of the American Taxation Association*), information systems (e.g., *MIS Quarterly*, *Journal of the Association for Information Systems*, *Database*), and accounting information systems journals (e.g., *International Journal of Accounting Information Systems*, *Journal of Information Systems*, *Journal of Emerging Technologies in Accounting*). Her research has been funded by grants from The IIARF, the Australian Research Council, and the FINRA Investor Education Foundation. A prior IIARF grant resulted in a monograph currently available to internal audit departments and others through The IIA as a part of its enterprise risk management series.

Tanya Benford is assistant professor of accounting in the Kenneth G. Dixon School of Accounting and recently came to the University of Central Florida from Texas A&M University. Her research has been published in leading journals such as *Auditing: A Journal of Practice & Theory*, *International Journal of Accounting Information Systems*, and *Journal of Emerging Technologies in Accounting*. Her research and teaching interests are in the areas of business process control and corporate governance. She is a former KPMG Ph.D. Project fellow.

Joseph Canada is a Ph.D. candidate in the Kenneth G. Dixon School of Accounting at the University of Central Florida. His research appears in the *Journal of Emerging Technologies in Accounting*, *Critical Perspectives on Accounting*, and *Corporate Ownership & Control*. His research focuses on managerial control systems including risk management and Sarbanes-Oxley Section 404 compliance processes. His doctoral studies are being supported in part by the KPMG Ph.D. Project.

EXECUTIVE SUMMARY

The purpose of this study was to investigate the impact of the U.S. Sarbanes-Oxley Act of 2002 Section 404 internal control reporting and assurance requirements on the performance of small- and medium-sized enterprises (SMEs) conducting business in tightly coupled supply chain environments with publicly traded organizations. There have been numerous claims in the business press that the increased emphasis of Sarbanes-Oxley on internal controls may affect organizational flexibility and production cycle times as well as absorb funds that might otherwise be used to improve processes and maintain compatibility. To understand the challenges faced by SMEs and how organizations have overcome these challenges, this study systematically examined the impact of Sarbanes-Oxley compliance on accelerated filers to better understand: 1) the successes and challenges experienced, 2) the factors impacting compliance difficulty, 3) the methods employed to minimize the impact on supply chain performance, and 4) the ongoing challenges of continued compliance. The study was executed in three distinct parts:

Part I. Case Studies of SMEs: Four in-depth case studies were conducted with the individuals responsible for leading the Sarbanes-Oxley Section 404 compliance effort in their respective organizations. A diverse set of companies was selected to include both a successful and a challenged company representing both small and medium company sizes. Key findings indicated that:

1. The a priori development level of enterprise risk management (ERM) processes had a major impact on the organizations' ability to cope successfully with compliance requirements. The better the ERM focus, the less difficult the compliance process seemed to be across the four companies.

2. The behavior and attitude of senior management was key to dictating that of the employees involved in the compliance effort. When senior management exhibited a positive attitude and a strong emphasis on compliance, employees generally fell in line and the compliance implementation process was much smoother. This was even truer when the organizations were smaller and more flexible.

3. The accessibility of information necessary to maintain effective risk management and control of operations was key to understanding the pain experienced in meeting compliance. The more control processes that could be automated, the easier the compliance, while the more manual controls that needed to be implemented, the greater the apparent impact on supply chain flexibility and performance.

Part II. Survey of Chief Audit Executives: Using a Web-based survey, responses were collected from 251 chief audit executives (CAEs) via the Global Audit Information Network (GAIN), the premier benchmarking program of The Institute of Internal Auditors (IIA). Data were collected on pre- and post-Sarbanes-Oxley organizational characteristics and processes, along with Sarbanes-Oxley implementation experiences for the 139 CAE responses from organizations that had issued at least one compliance report. In addition, supply chain performance data were collected from the 155 respondent organizations for which it was applicable with approximately 60 percent of these organizations having completed Sarbanes-Oxley compliance. The survey was designed to expand upon findings from the initial case studies to improve the generalizability to a broader range of organizations. Key findings indicated that:

1. ERM was the key underlying driver facilitating organizations' strategic flexibility, which in tandem with ERM dictated the effectiveness of the implementation processes utilized, and in turn helped minimize the difficulty of the compliance process.

2. ERM, along with strategic flexibility, was fundamental to maintaining effective supply chain performance. The more effective ERM processes, the better strategic flexibility was maintained and the more effective supply chain performance.

3. The availability and accessibility of enterprisewide information through information technology (IT) systems formed a critical link in understanding the relationship between ERM and strategic flexibility, and the relationship between ERM and supply chain performance. Essentially, the availability of well-integrated enterprise systems was critical to effective ERM and overall organizational performance.

4. The control environment of the organization was a critical catalyst to the relationship between strategic flexibility and effective Sarbanes-Oxley compliance implementation processes. The proper "tone at the top" was critical and the creation of an organizational culture of control paramount. Further, ERM had a major impact on the strength of the control environment, but this impact was even further strengthened through the indirect impact of ERM through effective enterprise systems and strong organizational strategic flexibility.

Part III. Follow-up Case Studies on Subsequent Sarbanes-Oxley Challenges: During the course of the study, it became clear that the issues surrounding Sarbanes-Oxley Section 404 compliance led to another set of issues as organizations went through various evolutions. For instance, it is well known that a large number of organizations have attempted to delist on U.S. exchanges or go private. Additionally, the normal process of mergers and acquisitions can lead to new challenges of maintaining business processes and information systems that are Sarbanes-Oxley compliant during and after the integration process. Finally, there is great emphasis on firms easing the difficulty of the process by embracing Sarbanes-Oxley, but what happens to those organizations that continue to fight the regulatory mandates and fail to embrace them? Three additional case studies were conducted to look at company experiences under these various scenarios. Key findings indicated:

1. The decision to privatize can be fairly unpredictable. In our case, the original owner of the company made an offer to buy the company back and take it private because the owner believed Sarbanes-Oxley was impacting supply chain performance and hurting the company. The board of directors demonstrated due diligence by soliciting other bids, and a private equity firm topped the offer and eventually gained control. The company was merged with a U.K. company also owned by the private equity firm. The compliance knowledge gained through the experience of the acquired firm was used to help prepare the U.K. company to achieve compliance prior to a planned public offering.

2. The second company fought the Sarbanes-Oxley compliance mandates and had strong disagreements with its auditors. Eventually, the auditor dropped the company as a client. Weaknesses were clearly present as billing systems were unreliable and billing statements could not be supported. As the company continued to deteriorate, it began outsourcing operational functions on top of previously outsourced support functions, ultimately merging with an international competitor.

3. The Sarbanes-Oxley compliance process is one more process that must be coordinated during the merger of two public companies. In this case, a small utility company that had met Sarbanes-Oxley compliance requirements decided to sell off parts of its company due to other regulatory complexities and disadvantages in scalability. The company has been considered a model firm for how to address compliance in a proactive manner. Merger discussions led to the formation of a coordination team to handle the transfer of operations specifically for Sarbanes-Oxley. The selling company, as a part of the agreement, agreed to maintain support and operations for the underlying information systems supporting the sold utility for several months post sale until the sold utility could be integrated into the other company's operations. Similarly, all nonautomated control structures were to be maintained by the selling company until final transfer of operations was feasible.

Overall, the findings indicate that effective ERM and an embracing of a risk management and control culture generally relieves the difficulty of compliance. Additionally, such a culture actually promotes organizational strategic flexibility (i.e., the ability to respond to changes in the marketplace) and facilitates enhanced supply chain performance. Simply meeting compliance requirements is insufficient and may just prolong problems. Rather, embracing a culture of risk management and control helps organizations meet regulatory mandates in a more efficient and effective manner while supporting organizational viability and competitiveness on an ongoing basis. Given the vital role that internal auditors play in the implementation and support of ERM processes, the findings also provide evidence of the strategic importance of a strong internal audit function to an organization's strategic goals.

INTRODUCTION

The study documented in this report has been designed to address many of the questions that have arisen during the course of the implementation of the U.S. Sarbanes-Oxley Act of 2002 provisions on effective systems of internal control and the mandates under Section 404. A broad view has been taken during the research in an effort to highlight why some organizations have had an easier time with implementation than others.

There also have been widespread concerns over how control systems are impacting organizations' competitiveness and their ability to meet business partners' expectations for supply chain performance. These issues have been argued to be of even greater concern to small- and SMEs.

The study approached these questions with a fairly open slate. While it was expected that the issues would revolve around organizational structure, top management response to the mandates, and the nature of control structures put in place to meet the new mandates, every effort was made to allow organizations' experiences to drive the evolution of the study. These efforts were initiated by originally seeking out two small and two medium-sized companies with each pair representing an organization that had a difficult time meeting compliance requirements and one that did not. These organizations' experiences highlight the critical roles of top management's attitudes, the integrated nature of enterprisewide information systems, and the strategic flexibility of the organization.

The lessons learned from these four companies were used to design a questionnaire that could be broadly disseminated to CAEs representing many different organizations to get a broad-based view on the relationships of the key factors identified in the case studies. The results provide substantial insight into the issues and concerns that have been raised in the business press. In short, we find that the strength of and support for ERM processes had a major influence on the organizations' difficulty in meeting compliance requirements and on the insulation of supply chain processes from negative effects.

While many SMEs are only now receiving their first audit opinions over management's assessment of their internal controls systems, many others have several years behind them. We look to these organizations to garner a better understanding of the other question that has received little attention to date: "What about tomorrow?" In asking this question, we turn not to organizations that are simply going through their third or fourth (or more) compliance year, but rather to those that provide a specific perspective. One organization successfully made it through the compliance process, but the reliance on manual controls was perceived to hinder its ability to compete in a supply chain environment where timing is critical. Making the decision to delist and go private, the original owner attempted to privatize the organization; however, a private equity firm outbid the original owner and took the organization private under its (i.e., the private equity firm's) control. Another organization struggled terribly during the compliance process, lost its auditor, and eventually merged with an international competitor that is benefitting from the hard lessons as the organizations are integrated. A third organization had a very successful compliance effort and was regarded as a model for compliance in earlier IIA reports, but unfortunately its financial growth was hindered by size and structure. We examine this organization's sharing of compliance models to facilitate the sale of business units to another organization.

There are many lessons to be learned from all of these organizations' experiences. In the remainder of this report, we elaborate on their experiences to allow other organizations to learn from them — particularly those SMEs that are just concluding their first years requiring an external auditor's report on their entitywide systems of internal controls.

PART I: CASE STUDIES

EARLY ADOPTER SMALL- AND MEDIUM-SIZED ENTERPRISES

Few corporate regulatory acts passed by the U.S. Congress have spurred as heated a debate in the public press and in speeches around the country (and the world) as has the U.S. Sarbanes-Oxley Act of 2002. Many have questioned whether the benefits outweigh the costs[1] while others have viewed Sarbanes-Oxley as one of the most important pieces of legislation related to financial reporting and corporate governance in terms of protecting the public interest.[2]

The debate has been most heated in weighing the impact on SMEs. This debate has revolved around the unanticipated consequences that compliance is projected to have on the operations of these smaller enterprises and their ability to remain competitive. These concerns arise mostly from the perceived restrictiveness of extensive internal control systems that may hinder SMEs that succeed based on fast-changing and flexible structures.[3] The restrictiveness of these control systems has been viewed as potentially impacting innovation, job creation, and global competitiveness.[4] However, despite all the outcry, these concerns have not been substantiated by prior research. Indeed, research focusing specifically on management control and its role in the strategic orientation of organizations has found that the more strategically oriented the organization, the stronger the managerial control processes required for such organizations to maintain their ability to strategically respond to marketplace changes.[5]

The purpose of Phase I of this study was to investigate the impact of Section 404 internal control reporting and assurance requirements on SMEs' ability to maintain competitiveness and to attain or maintain strong supply chain performance. Of particular interest were the processes implemented by various organizations to respond to compliance requirements and how these various processes impacted the flexibility of operations, the ability to strategically respond to market shifts, and overall supply chain performance.

I(a): Description of Participating Organizations

Given the focus of the research on understanding the Sarbanes-Oxley Section 404 internal control reporting and compliance experiences of organizations and putting together the pieces of the picture that help explain the interactive effect of organizational structures and compliance requirements on competitiveness and supply chain performance, we conducted a series of case studies. In each instance, we conducted interviews with the individuals representing the primary leaders in the Sarbanes-Oxley 404 compliance effort. Four targeted case studies were conducted with the goal of achieving diversity in the participating organizations across size, compliance experience, industry, processes, structure, and experience.

---

[1]Holstein, W.J. 2006. "Rethinking SOX." *Directorship*, (June): http://www.directorship.com/publications/oxley.aspx.

[2]Canada, J., J.R. Kuhn, and S.G. Sutton. 2008. "Accidentally in the Public Interest: The Perfect Storm That Yielded the Sarbanes-Oxley Act." *Critical Perspectives on Accounting*, 19(7): 987–1003.

[3]Katz, D.M. 2006. "Panels on 404 Skirt Small-company Woes." *CFO.com* (May 2).

[4]Reason, T. 2006. "Cry of Pain From Small Companies." *CFO.com* (May 10).

[5]Ditillo, A. 2004. "Dealing With Uncertainty in Knowledge-intensive Firms: The Role of Management Control Systems as Knowledge Integration Mechanisms." *Accounting Organizations and Society*, 29: 401–421.
Chenhall, R. H. and K.J. Euske. 2007. "The Role of Management Control Systems in Planned Organizational Change: An Analysis of Two Organizations." *Accounting Organizations and Society*, 32: 601–637.

Company A was an air and ocean freight company providing value-added logistics services to its customers. The company was relatively young, having been in business for only 40 years. Company A's logistics network includes 400 facilities located in 100 countries and employing more than 10,000 workers. In the year preceding our interviews, the company had US $3.1 billion in revenue, US $1.09 billion in assets, and a total market capitalization of US $1.5 billion. Its annual audit was conducted by a Big Four public accounting firm.

Company B was a defense and space systems manufacturer selling primarily to defense contractors and the U.S. military. The entirely U.S.-based company employs more than 3,000 workers. While this was our oldest company (nearing 100 years since its formation), its experience dealing with government regulatory compliance over the years left it well prepared to address Sarbanes-Oxley compliance mandates. Company B reported US $624 million in revenue and US $1.06 billion in assets for the year preceding our interviews. They had a market capitalization of US $1 billion and were audited by a Big Four public accounting firm.

Company Y was a manufacturer of corporate apparel, identification, and accessories for use in the healthcare, hotel, restaurant, public safety, industrial, transportation, and commercial markets. This company was also quite mature with more than 85 years of experience and a well-developed global network consisting of a broad array of offshore suppliers that produce more than 70 percent of the company's output. The managing arm and remaining 30 percent of production are all U.S. based with a total of 700 domestic employees. In the prior year the company reported US $144 million in revenue, US $106 million in assets, a market capitalization of US $104 million, and a 30-percent controlling interest by the founding family. Company Y employed a non-Big Four international public accounting firm to complete its audit.

Company Z was a supplier of durable medical equipment for homebound patients. The company has operations spread across 490 locations in 48 states and employs approximately 4,600 workers. This relatively young company had been in business for about 25 years and appeared to be operating solidly with prior year revenue of US $533 million and US $1.02 billion in assets. Company Z's market capitalization was US $426 million and they used a Big Four public accounting firm for their audit needs.

I(b): Company Sarbanes-Oxley Compliance Strategies

In evaluating the spectrum of experiences among our four organizations, it is clear that no single strategy was found to be preferable for all. Rather, in their compliance efforts we see a mix of strategies between external consultants, outsourced internal audit expertise, development of new internal audit capabilities, and an expanded role for internal audit. In general, the organizations that carefully built their own internal audit capabilities over time seemed to handle the transition to compliance most successfully.

Company A invested a substantial amount of funding into the compliance effort, having a Big Four firm as an auditor and two other Big Four audit firms as Sarbanes-Oxley compliance consultants to assist in planning, documenting, and testing internal controls. To facilitate the effort, Company A also invested in new workflow and document repository software requiring assistance from another external consultant. Additionally, two new employees were added to the IT staff to deal specifically with compliance issues. The company adopted a balanced scorecard approach to assessing risks that led to a myriad of new control procedures that at times appeared to hamper supply chain performance. The multifaceted strategy was viewed as providing the greatest opportunity for successful compliance as the company felt the lack of overall guidance by the U.S. Securities and Exchange Commission (SEC) and The Public Company Accounting Oversight Board (PCAOB) necessitated over-compliance. The expensive strategy adopted

was further exacerbated by rises in audit fees from pre-Sarbanes-Oxley levels of US $1.3 million to US $4.7 and US $4.9 million in the first two years of the compliance effort. Management's view was that the incorporation of very structured internal controls into the business processes hurt the company competitively in the global market as process time and costs increased. These changes made it difficult to compete for many jobs due to hampered speed of delivery and increased costs they felt they needed to pass on to their customers.

The stringent control guidelines placed on government contractors put Company B in a strong starting position for undertaking the compliance effort. Nonetheless, facing similar concerns to those of Company A in regards to the perceived ambiguity of the required control processes for achieving compliance, Company B decided to hire a Big Four accounting firm to provide consulting services to assure success. After two years of weighing and implementing a multitude of specific control processes, a new position, director of Sarbanes-Oxley 404, was hired in the third year of the compliance effort to streamline the effort and improve its overall effectiveness. Amidst the compliance effort, audit costs also rose significantly from pre- Sarbanes-Oxley levels of US $2.8 million to US $5.3 and US $4.9 million respectively in the first two years of the compliance effort. When asked whether the internal control compliance effort was a good investment of resources, the response was a clear no. Management viewed Sarbanes-Oxley 404 compliance as little more than a regulatory activity and the controller estimated that only about 20 percent of the total compliance cost had been productive. As a government contractor, Company B felt their internal control system was already in excellent condition and that the costs of compliance had simply been an additional regulatory cost.

Company Y was very proactive in its compliance efforts and appeared to take control of the situation very quickly. Top management was quick to jump on board the compliance effort and began documenting procedures very early on, hiring a boutique specialty consulting firm — which was later replaced — to facilitate the effort and assign related responsibilities to existing staff. However, most of this early documentation effort had to be scrapped and Company Y was set back in its effort. A new consulting firm was brought in and the process essentially restarted from scratch. The process was further hindered by early protest and noncooperation by the vice president of IT who was much more focused on a SAP software upgrade. Once the vice president got behind the effort, the IT staff also became engaged in the compliance effort and the process went very smoothly from that point forward. However, the early hiccup was costly because the auditors had to re-audit the new documentation, so this baseline cost was incurred twice. Audit fees rose from a pre-Sarbanes-Oxley level of US $154,000 to US $369,000 and US $409,000 in the first two years of the compliance effort.

Company Z also was proactive in its efforts to achieve compliance, but rather than try to achieve compliance through additional responsibilities being placed on existing personnel, an internal audit function was created. The company created the internal audit function to specifically handle financial-related processes and hired an outside specialty consulting firm to complement the internal audit function with IT specialists. The consulting firm also supported the implementation of content repository software to facilitate the documentation effort. The compliance process progressed well early on despite the chief financial officer's (CFO's) staunch opposition as the new director of internal audit understood the importance and pushed the effort forward. As a result, compliance costs were viewed as being well contained. The CFO's fierce opposition did prove costly, however, as a rift developed with the external auditor who was pushing for quick compliance. The audit cost also was costly because the auditor was forced to complete substantial additional testing late in the process to assure compliance. Thus, audit fees only rose the first year from US $332,000 to US $433,000 before quadrupling to US $1.2 million in the second year of compliance. Eventually, the CFO was replaced by the director of internal audit and the manager with the external consultant was hired as the new director of internal audit, bringing a cadre of

IT audit specialists with him to enhance the internal audit department's capability and self-sufficiency. Even after this change, the consulting firm continued to provide some controls testing support.

Our companies' experiences appear to be typical of the broad range of SMEs' experiences that have been briefly reported in the business press. The process has often been difficult as organizations stagger through new processes and mindsets. On the other hand, some organizations have complied much easier than others. In the following section, we integrate the various experiences of our case study companies to identify general patterns and critical factors that appear to impact compliance difficulty and the impact on business processes' efficiency and effectiveness.

I(c): Summary Research Findings

In evaluating the spectrum of experiences among our four companies, three fundamental areas stood out most prevalently: 1) ERM strategies, 2) the role of structural inertia and the corollary ability to adapt to change, and 3) organizational flexibility. We consider these three areas across the four companies participating in our case studies.

Improved ERM represents the biggest benefit of Sarbanes-Oxley 404 when considering our companies' experiences. Clearly, an objective of Sarbanes-Oxley was to push organizations toward better governance and stronger financial controls — key components of ERM. However, many organizations viewed the mandates as extending to robust ERM processes that are more strategic than operational, and each of our companies made significant strides in this direction. Likewise, the stronger the ERM processes in place pre-Sarbanes-Oxley, the easier time our case study companies had with the compliance process. This effect was perhaps best summarized by the chief information officer (CIO) at Company A who, despite the highly challenging experience in achieving compliance, still noted that "Sarbanes-Oxley does not ask for companies to do anything that they should not have been doing already."

Sarbanes-Oxley required organizations to stop and assess what were often long-neglected ERM processes that no longer were sufficient for their organizations. Company A, despite its bitterness about the Sarbanes-Oxley mandates, noted that new risk assessment processes were implemented and formalized to allow the company to match assessed risks with business priorities using a balanced scorecard-based approach. They further noted that Sarbanes-Oxley ". . . forces us to apply our practical pragmatic business approach to these types of issues and stop 'reacting' to perceived issues. We have improved in recognizing the importance to the company, as well as having a balanced approach." Company B instituted a training program to educate employees on risk-related issues with the intent to get employees to embrace control procedures, take ownership over control effectiveness, and recognize when risks threaten business process success. Company Y adopted a risk matrix that uses cross-functional teams to conduct annual risk analyses where potential risks are rated high or low in terms of consequence and probability with two high ratings requiring a written analysis report. Company Y further acknowledged that the formalization of policies and procedures provided a long-term impact on infrequent risks that might otherwise have been ignored. Company Z noted that one big benefit of Sarbanes-Oxley compliance was that it served to greatly improve the relationships between internal auditing and other departments. As internal auditing helped resolve complex compliance issues for the departments, department leaders gained a healthier appreciation for risk assessment and related internal control system processes. There was also little doubt that all of the companies' ERM processes were far more effective post-compliance.

Structural inertia[6] and companies' ability to cope with change provided another significant, contributing explanation to the companies' experiences. Structural inertia comes into play when assessing how organizations would react to Sarbanes-Oxley mandates. Theory suggests that older, more mature organizations will struggle far more to make the changes in their processes. On the other hand, organizations that have substantial experience in dealing with change as an ongoing part of their business model are able to use that experience to adapt much more quickly to new mandates. This held true with our companies. Company A, a medium-sized established enterprise, was most affected by Sarbanes-Oxley and struggled the most to comply. Its size and established structure, coupled with its far-reaching global operations, confounded the process. Company B, also a medium-sized enterprise but one that had dealt with government regulations in government contracting for an extended period, was quick to adapt and had a fairly smooth transition during the compliance process. Company Y, a smaller company, was able to react quickly; once the vice president of IT got behind the effort, size was an advantage and the "tone at the top" was a very effective driver of the compliance effort. Company Z benefitted perhaps the most of any of the organizations because of its size and the change experience it hired (i.e., while the organization itself was not highly experienced in change, they hired people from the outside — such as the IT audit director from the consulting firm — who had extensive experience with multiple organizations).

Organizational flexibility was the other prevalent factor impacting the companies' experiences. The loss of flexibility was frequently raised as a concern to all of the organizations. As noted earlier, Company A felt there were serious impacts on competitiveness due to loss of flexibility. More specifically, they noted that "time to process normal business transactions has increased an estimated 5 percent. In the transportation industry, any additional time the customer experiences can — and probably has — lost us business . . . . The time impact is greater as transactions increase in complexity." Company B's CFO noted that Sarbanes-Oxley "negatively impacted flexibility due to a fear that doing anything not in the documented procedures would result in a material weakness." The CFO also noted that while the strategic plan for the company was not altered, Sarbanes-Oxley compliance costs were now required to be included in every new project budget, thus making many strategic processes appear no longer cost beneficial. Company Y noted that Sarbanes-Oxley concerns influenced the decision to drop the SAP HR (human resources) module over concerns of the impact on overall compliance assessments. Company Z's head of internal audit acknowledged "there are specific areas where having to comply with Sarbanes-Oxley has made processes more involved, resulting in more time and effort required to perform a process for controls in that specific area to operate effectively." Company Z also noted that new information systems interfacing with the financial reporting system were delayed indefinitely until the associated Sarbanes-Oxley documentation was completed, which would clearly articulate the completeness of controls. Thus, Sarbanes-Oxley appeared to affect the companies' flexibility in many ways, but not necessarily all for bad reasons.

Also of note is the reverse influence of organizational flexibility. While often viewed as an attribute perceived to be hampered as an outcome of the Sarbanes-Oxley compliance process, organizational flexibility also proved to be a major input into its effectiveness. Overlapping to some degree with the

[6]Structural inertia is an organization's ability or inability to change under conditions of environmental turbulence. Age and size are considered to be the two largest impediments to changeability, while change experience can help overcome.
See: Hannan, M.T. and J. Freeman. 1984. "Structural Inertia and Organizational Change." *American Sociological Review,* (49) 2: 149–164; Amburgey, T.L and A.S. Miner. 1992. "Strategic Momentum: The Effects of Repetitive, Positional, and Contextual Momentum on Merger Activity." *Strategic Management Journal,* (13): 335–348; and Amburgey, T.L., D. Kelly, and W.P. Barnett. 1993. "Resetting the Clock: The Dynamics of Organizational Change and Failure." *Administrative Science Quarterly,* (38): 51–73.

structural inertia foundation for addressing change, the companies' flexibility was important in coping with change and adapting to the new mandates. Interestingly, it was the ready flow of information across the company that often dictated how well flexibility was able to help. Those companies with strong, integrated information technologies maintained higher flexibility and were better able to gather and assess the information needed for effective ERM. We see this in Company B with its size and maturity still able to react due to tight information integration and strong preexisting control structures that enabled it to react to changes. Companies Y and Z also were able to adapt more quickly once they embraced change and gained management's consistent support for the efforts, while automation of control processes influenced the ease of compliance. Company A's lack of integration across a dispersed global network coupled with surprising inflexibility for an organization that viewed itself as flexible in its business processes led to increased compliance difficulties.

Our team walked away from these four companies with a vision of the basic structures that impacted organizations' ability to address compliance mandates, maintain organizational flexibility, and maintain effective supply chain performance. Phase II of the study used this information in the design of a survey issued to a much broader set of organizations to test whether these observed phenomena held across a larger cross-section.

PART II: IIARF SURVEY
CHIEF AUDIT EXECUTIVES' EXPERIENCE
WITH SARBANES-OXLEY COMPLIANCE

Based on the case studies completed in the first portion of the study, several factors appeared to capture the major issues surrounding Sarbanes-Oxley compliance. The outcome issues of most concern generally focused on the difficulty in complying with Sarbanes-Oxley 404 mandates, supply chain performance, and the organization's ability to maintain flexibility and agility in its strategic operations. The enablers of these outcomes revolved around the effectiveness of ERM processes, strength of the control environment, and the compatibility and flexibility of IT systems in terms of bringing together the information necessary to support ERM, compliance documentation, well-controlled supply chain activities, and strategic flexibility.

The focus in Part II of the research study shifted to attaining a better understanding of whether the key issues identified in our sample of case study companies were representative of the experiences endured by a broader range of organizations. In conjunction with The IIARF, we launched a survey on The IIA's GAIN system and e-mailed solicitations for participation to members who are CAEs. The survey collected both pre- and post-Sarbanes-Oxley data on ERM process effectiveness, supply chain performance, IT flexibility from connectivity and compatibility perspectives, organizational strategic flexibility, and control environment. In addition, we collected data on Sarbanes-Oxley implementation processes and experiences, whether Sarbanes-Oxley 404 compliance was required, and a variety of demographic information related to the CAEs and their organizations. The remainder of the discussion in this part focuses on the execution of that portion of the study and our findings.

II(a): Methodology and Demographics

The IIARF's solicitation of CAE participation resulted in 251 members completing the survey (a response rate of 18.1 percent). The response rate is indicative of organizations' strong interest in Sarbanes-Oxley 404 compliance processes and challenges. Out of the 251 respondents to the survey, 139 (55.6 percent) were from organizations that had already completed the Sarbanes-Oxley 404 compliance process at least once and had issued both management and auditor's reports on internal controls. A different cross-section of the sample was analyzed for purposes of evaluating the impact of strategic ERM processes on supply chain performance. Of the 251 respondents to the survey, 155 (61.8 percent) of the CAEs provided information consistent with active involvement in a supply chain with 90 (58.1 percent) of those organizations having completed at least one Sarbanes-Oxley 404 compliance cycle. These two subsamples form the basis for our analyses in Phase II of the research study.

In the first subsample consisting of organizations having completed at least one Sarbanes-Oxley 404 compliance effort, 93.8 percent were publicly traded companies. A broad range of industries were represented in the sample with the largest groups coming from manufacturing (23 percent), financial services and real estate (16.8 percent), technology (10.6 percent), insurance (9.7 percent), and utilities (8.9 percent). (See Table 1 for details.)

Table 1
Demographics for Companies with
Completed Sarbanes-Oxley Section 404 Compliance

Category	Percentage
Gender	
Male	69.03%
Female	29.20%
Not answered	1.77%
Age	
25 to 40 years	24.78%
40+ years	74.34%
Not answered	0.88%
Experience	
3 to 10 years	18.58%
10+ years	81.42%
Industry	
Manufacturing	23.01%
Financial services and real estate	16.81%
Technology	10.62%
Insurance carriers and agents	9.73%
Utilities	8.85%
Wholesale and retail	5.31%
Transportation	5.31%
Communication	3.54%
Health	2.64%
All other	14.16%
Organizational Structure	
Publicly traded	93.81%
Not publicly traded	5.31%
Not answered	0.88%

In the second subsample consisting of organizations substantially involved in supply chain interactions, 58.1 percent were publicly traded companies. A broad range of industries also were represented in this sample with the largest groups coming from manufacturing (18.7 percent), insurance (16.8 percent), financial services and real estate (14.2 percent), wholesale and retail (8.4 percent), technology (7.7 percent), and utilities (7.1 percent). (See Table 2 for details.)

Table 2
Participant Demographics

Category	Percentage
Gender	
Male	70.3%
Female	29.0%
Not answered	0.7%
Age	
25 to 40 years	20.65%
40+ years	76.77%
Not answered	2.58%
Experience	
3 to 10 years	15.48%
10+ years	84.52%
Industry	
Manufacturing	18.71%
Insurance	16.77%
Financial and real estate	14.19%
Wholesale and retail	8.39%
Technology	7.74%
Utilities	7.10%
Health	4.52%
Communication	2.58%
Aerospace and defense	2.58%
Transportation	2.58%
All other	14.84%
Organizational Structure	
Publicly traded	58.06%
Not publicly traded	40.65%
Not answered	1.29%

A field survey method was used in the research to rapidly gather data on a broad range of organizations to examine the expected relationships among the various issues identified in the case studies. A field survey focuses on a key respondent who is in a position to observe the actual phenomena of interest in the study. In this case, we focus on CAEs based on their integral role in the Sarbanes-Oxley implementation process and their dual role in monitoring organizational efficiency and effectiveness. We adopted structural modeling techniques for the analysis of the data to both validate the overall measurement constructs (each

issue of concern was measured with multiple questions) and assess the overall fit of a conceptual model representing the expected relationships among the organizational attributes and the resulting outcomes.

II(b): Enterprise Risk Management and Sarbanes-Oxley Implementation Difficulty

The goal of our analyses on Sarbanes-Oxley implementation difficulty was to examine the drivers of our case study companies' experiences in an effort to better understand how they influenced the resulting compliance difficulty. Based on our earlier case studies, we viewed the critical relationships as focusing around the pre-Sarbanes-Oxley compliance state of an organization's ERM processes, control environment, IT flexibility in terms of compatibility, and strategic flexibility. As such, our research model examines these four factors as being predictive of an organization's difficulty in implementing effective Sarbanes-Oxley compliance procedures. However, we do not see these four factors as operating independently. Accordingly, our models consider the impact of factors on each other. Most notably, effective ERM necessitates the development of strong information flow across the organization (e.g., IT compatibility) and a strong control environment. Without the latter, it is unlikely that an organization will be able to easily implement effective Sarbanes-Oxley compliance procedures.

To develop measures of each of the factors within our responding organizations, we used a combination of questionnaire measures used in prior academic studies and measures developed by our team to address more contemporary factors where previously validated measures were not available. For ERM, we developed a five-question instrument based on the ERM framework prescribed by COSO.[7] Similarly, for the control environment, we developed a multi-question instrument based on COSO's[8] original framework description. For strategic flexibility we used a common measure from strategic management research first put forth by Cannon and St. John.[9] IT compatibility was a subcomponent of an overall IT flexibility instrument developed and validated by Byrd and Turner.[10] We focused on the compatibility component given its ability to capture the degree to which an organization's information systems are capable of sharing data from across the entire organization. As noted previously, the focus of these factors is on the difficulty an organization encountered in complying with Sarbanes-Oxley 404 mandates. We assess the efficiency of the Sarbanes-Oxley compliance implementation process through a set of questions we developed that focus on best practices for organizational and business process change. These questions were derived based on an amalgamation of related studies along with our original case studies.[11] The resulting model shown in Figure 1 supports our prediction of the influences of the various factors on the efficiency of the Sarbanes-Oxley compliance implementation process. Analyzed in its entirety, the model shows strong simultaneous fit among all of the various factors and relationships specified in the

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

[8]Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control — Integrated Framework.* American Institute of Certified Public Accountants.

[9]Cannon, A. R. and C. H. St. John. (2004). "Competitive Strategy and Plant Level Flexibility." *International Journal of Production Research,* 42(10): 1987–2007.

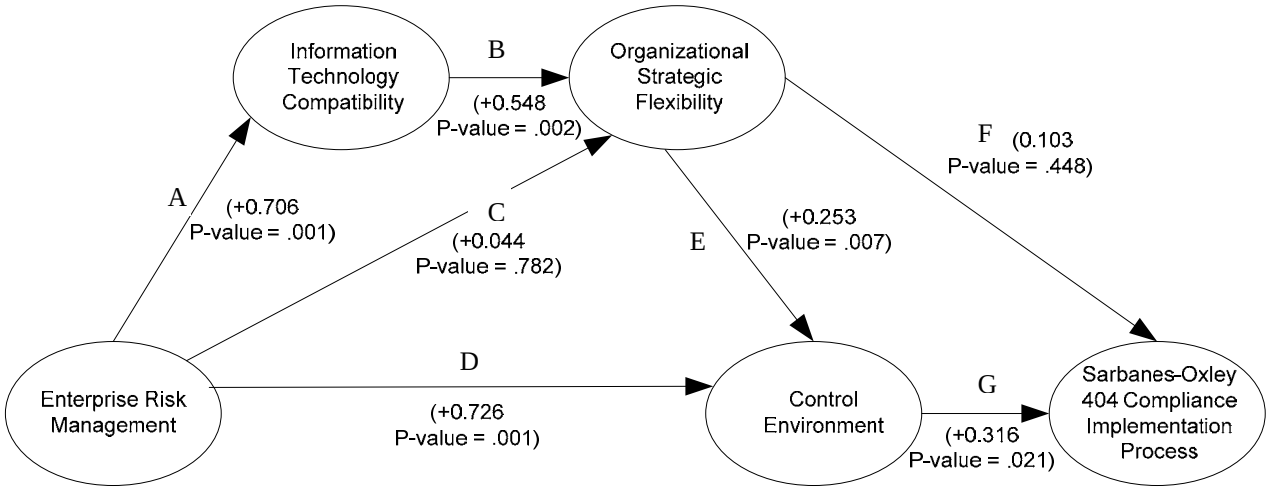
[10]Byrd, T. A. and D. E. Turner. 2000. "Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct." *Journal of Management Information Systems,* Summer Vol. 17, No. 1: 167–208.

[11]Kettinger, W. K. and V. Grover. 1995. "Toward a Theory of Business Change Management." *Journal of Management Information Systems,* Vol. 12. No. 1: 9–30.

Ungan, M. 2005. "Management Support for the Adoption of Manufacturing Best Practices: Key Factors." *International Journal of Production Research,* Vol. 43, No. 18: 3803–3820.

model.[12] To overview the model, we will quickly review the various relationships captured. The "A" path indicates that stronger ERM processes lead to higher levels of IT compatibility, a relationship that is highly significant in the model. The "B" path indicates that higher levels of IT compatibility support higher levels of strategic flexibility, a relationship that is also highly significant. On the surface, the "C" path appears to reflect the absence of a direct relationship between ERM and strategic flexibility. However, "C" is reflective of a *mediating* relationship indicating that the relationship between ERM and strategic flexibility is *fully mediated* by IT compatibility. In essence, the positive relationship between ERM and strategic flexibility is dependent upon strong IT compatibility.[13]

Figure 1
Predictive Model for Efficiency of Sarbanes-Oxley Section 404 Compliance Implementation Process



Chi-square = 141.726 df =111 p-value = .026
CFI = .972 RMSEA = 0.050

The "D" path indicates that strong ERM leads to a strong control environment, a basic COSO premise that not surprisingly is highly significant in the model. What may be less evident at first glance is that the inclusion of IT compatibility and strategic flexibility in the model results in an additional 15 percent of the relationship between ERM and the control environment. In other words, per the path weight on "D" of 0.726, ERM explains directly 72.6 percent of the control environment's strength. However, when IT compatibility and strategic flexibility are added into the model, a total of 83.5 percent of the control environment's strength is explained via direct and indirect effects of ERM.

[12]The model was tested using AMOS 7.0 (2006) software for structural equation modeling. The Comparative Fit Index (CFI) of 0.972 and the Root Mean Square Error of Approximation (RMSEA) of 0.050 provide solid support for concluding there is good overall model fit.

[13]If we extract ERM and strategic flexibility to only look at this relationship in isolation, there is a direct and significant relationship (p-value = 0.001). Similarly, when we add IT compatibility and look at the three factors in isolation together, the relationship between ERM and strategic flexibility lacks significance (p-value = 0.577), verifying that IT compatibility fully mediates the relationship.

The "E" path indicates that increased strategic flexibility leads to a stronger control environment, a relationship that is highly significant in the model. This is consistent with findings noted earlier that suggest organizations must build strong managerial control systems to sustain strategically flexible organizational structures over time. The "F" path indicates that a stronger control environment facilitates a more efficient Sarbanes-Oxley 404 compliance implementation process. The "G" path is reflective of a situation similar to that found with the "C" path. The "G" path is reflective of a *mediating* relationship which indicates that the relationship between increased strategic flexibility and a more efficient Sarbanes-Oxley 404 compliance implementation process is *fully mediated* by a strong control environment. In essence, the positive relationship between strategic flexibility and efficient Sarbanes-Oxley 404 compliance implementation processes is dependent upon a strong control environment.[14] This relationship highlights one possible explanation for many organizations' complaints that their flexibility was hampered by Sarbanes-Oxley 404 compliance processes — without strong ERM and a strong control environment, organizations have difficulty sustaining flexibility and reacting to new regulatory mandates such as those mandated by Sarbanes-Oxley.

II(c): Enterprise Risk Management and Supply Chain Performance

The goal of our analyses on supply chain performance was to better understand how ERM impacts performance. However, similar to our study of Sarbanes-Oxley 404 implementation difficulty, we recognize the intermediary effects of IT compatibility and strategic flexibility in facilitating ERM impacts on organizational performance. Based on our earlier case studies, we viewed the critical relationships as focusing on the current state of an organization's ERM processes, IT flexibility in terms of both compatibility and connectivity, and strategic flexibility. As such, our research model examines these three factors as being predictive of an organization's supply chain performance. As in the prior analyses, we do not see these three factors as operating independently, but rather we view them as highly interrelated. Accordingly, our model again considers the impact of the factors on each other. In particular, we view effective ERM as necessitating the development of strong information flow across the organization (e.g., IT compatibility and connectivity) to promote strategic flexibility and, in turn, supply chain performance.

To develop measures of each of the factors within our responding organizations, we used a combination of questionnaire measures, as noted earlier, used in prior academic studies and measures developed by our team. In this study, we used the same ERM measurement instrument based on the COSO ERM framework,[15] but this time we focused on current ERM processes as opposed to pre-Sarbanes-Oxley ERM as used in the earlier study. IT compatibility and connectivity are both subcomponents of the IT flexibility instrument developed and validated by Byrd and Turner.[16] In this part of the study we focus on the current state of both connectivity and compatibility to capture the intra-organizational information sharing capability necessary to support both strategic flexibility and supply chain activities. Our interest in this study is in understanding the intermediary effects on strategic flexibility and the overall effects on supply

[14]If we extract strategic flexibility and Sarbanes-Oxley Section 404 compliance implementation processes to only look at this relationship in isolation, there is a direct and significant relationship (p-value = 0.011). Similarly, when we add strength of control environment and look at the three factors in isolation together, the relationship between strategic flexibility and Sarbanes-Oxley 404 compliance implementation processes lacks significance (p-value = 0.678), verifying that strength of the control environment fully mediates the relationship.

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

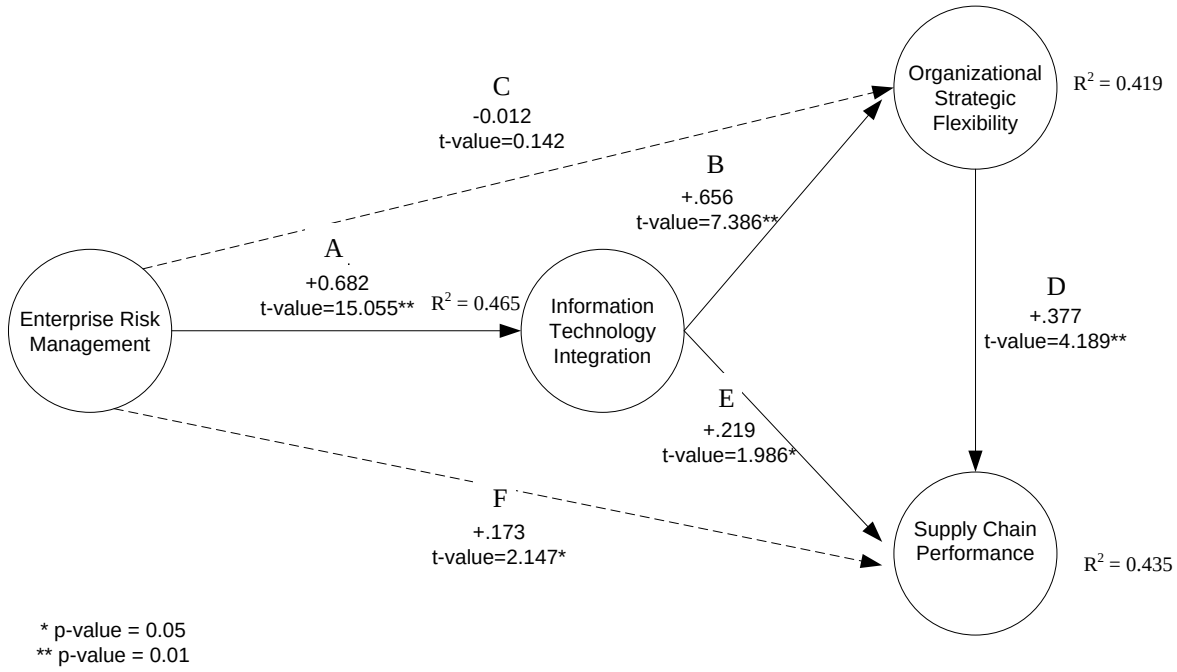
[16]Byrd, T. A. and D. E. Turner. 2000. "Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct." *Journal of Management Information Systems,* Summer Vol. 17, No. 1: 167–208.

chain performance that result from strong ERM processes in a post-Sarbanes-Oxley world. For strategic flexibility we again used the Cannon and St. John[17] measure, but similarly with a focus on the current state. For supply chain performance, our interests are on customer service goals and objectives and as such we adopt measures from Beamon[18] that are reflective of this interest.

The resulting model shown in Figure 2 supports our prediction of the influences of the various factors on both strategic flexibility and supply chain performance. Analyzed in its entirety, the model shows strong simultaneous fit among the various factors and relationships specified in the model. To overview the model, we will briefly review the various relationships captured. It should be noted that relationships in this model are quite complex recognizing the interrelationships of the particular factors of interest.

Figure 2

Predictive Model for ERM Effects on Strategic Flexibility and Supply Chain Performance



The "A" path indicates that stronger ERM processes will lead to higher levels of IT integration (i.e., compatibility and connectivity), a relationship that is highly significant in the model. The "B" path indicates that higher levels of IT integration support higher levels of strategic flexibility, a relationship that is also highly significant. On the surface, the "C" path appears to reflect the absence of a direct relationship between ERM and strategic flexibility. However, "C" is reflective of a *mediating* relationship, indicating that the relationship between ERM and strategic flexibility is *fully mediated* by IT integration. In essence, the positive relationship between ERM and strategic flexibility is dependent upon

[17]Cannon, A. R. and C. H. St. John. (2004). "Competitive Strategy and Plant Level Flexibility." *International Journal of Production Research*, 42(10): 1987–2007.
[18]Beamon, B. (1999). "Measuring Supply Chain Performance." *International Journal of Operations and Production Management*, 9(3): 275–292.

strong IT integration.[19] This finding is consistent with the relationships found in examining a similar set of factors in a pre-Sarbanes-Oxley environment in the previous analyses when testing the other subset of data.

The "D" path indicates that higher levels of strategic flexibility lead to better supply chain performance, a relationship that is highly significant in the model. On the surface, the "E" path is significant, but appears to not be as strong as some other relationships in the model. However, "E" is reflective of a *mediating* relationship, indicating that the relationship between IT integration and supply chain performance is *partially mediated* by strategic flexibility. In essence, the positive relationship between IT integration and supply chain performance is *partly* dependent upon higher levels of strategic flexibility that allow an organization to leverage information into performance.[20]

The "F" path represents a third *mediating* relationship where IT integration is viewed as *mediating* the relationship between ERM and supply chain performance. Similar to the "E" path, the "F" path represents a *partially mediating* relationship. This indicates that strong ERM processes have a positive impact on supply chain performance, but a portion of this relationship is dependent on the availability of strong IT integration that facilitates the necessary information flows to both efficiently control supply chain processes and facilitate monitoring of supply chain performance.[21]

II(d): Summary

On an overall basis, the results of the two models indicate that a strong ERM focus actually improves strategic flexibility and supply chain performance, contrary to many of the concerns voiced over the last few years in regards to potential negative effects of Sarbanes-Oxley 404. Further, the results suggest that organizations that had implemented strong ERM processes prior to Sarbanes-Oxley Section 404 and those organizations that similarly established strong control environments experienced significantly less difficulty in meeting compliance requirements. At the same time, the results highlight the critical role of strong IT integrated systems — a perspective that is consistent with COSO's long emphasis on information flow as being critical to strong control systems and is also consistent with the recent focus on automating Sarbanes-Oxley Section 404 compliance efforts to improve both efficiency and effectiveness of ERM processes. While not directly measured, the results also infer that a strong internal audit function can greatly benefit both an organization's flexibility and performance.

[19]If we extract ERM and strategic flexibility to only look at this relationship in isolation, there is a direct and significant relationship (p-value < 0.01). Similarly, when we add IT integration and look at the three factors in isolation together, the relationship between ERM and strategic flexibility lacks significance (t-value = 0.294), verifying that IT integration fully mediates the relationship.

[20]If we extract IT integration and supply chain performance to only look at this relationship in isolation, there is a direct and significant relationship (p-value < .01). Similarly, when we add strategic flexibility and look at the three factors in isolation together, the relationship between IT integration and supply chain performance decreases in significance (change in t-value from 11.545 to 3.211), verifying that strategic flexibility partially mediates the relationship.

[21]If we extract ERM and supply chain performance to only look at this relationship in isolation, there is a direct and significant relationship (p-value < .01). Similarly, when we add strength of IT integration and look at the three factors in isolation together, the relationship between ERM and supply chain performance decreases in significance (change in t-value from 7.810 to 1.576), verifying that strength of the control environment partially mediates the relationship.

PART III:
WHAT ABOUT TOMORROW?

While the first set of case studies and the follow-up survey provided a strong basis for understanding key issues surrounding initial compliance with Sarbanes-Oxley Section 404 internal control compliance mandates, the question that is left unanswered is how Section 404 affects organizations' business decisions in the future (i.e., What about tomorrow?). Our research team conducted three additional case studies designed to look at three specific situations with organizations facing ownership and control changes: 1) what are some of the risks and pitfalls that can occur when attempting to take a company private (i.e., delisting), perhaps to avoid Sarbanes-Oxley Section 404 mandates? 2) for companies that keep fighting the mandates but attempt to stay public, what are some of the business concerns? and, 3) what are the challenges that Sarbanes-Oxley Section 404 introduces to the mergers and acquisitions process? The first two situations relate to companies who fought the Sarbanes-Oxley compliance effort to various degrees. The latter is an almost reverse situation where a company that was a model for compliance encounters financial and business challenges that lead to divestiture of business units. We explore these three organizations to get some view of the challenges faced in each situation that go beyond the typical compliance efforts we had studied to date.

III(a): Ownership and Control Changes

The passage of Sarbanes-Oxley marked a significant change in corporate governance policies under the auspices of the public interest and altered the relationship be-ween shareholders and management. As a result, regulations have altered organizations' business models, and concerns have been raised regarding the impact on global competitiveness.[22] Companies feeling that Sarbanes-Oxley Section 404 mandates hamper their business activities fall into three groups: 1) acceptance, 2) denial, or 3) avoidance. Here we look at avoidance through an organization that chose a delisting option as a means of getting out of the requirements. Many firms have explored this option of not being traded on exchanges, instead choosing to avoid the corporate governance requirements prescribed by Sarbanes-Oxley. Consistent with this approach, there has been a significant increase in delisting activity on U.S. exchanges.[23] Publicly traded U.S. companies can delist by either *going dark* or *going private*. Firms that go dark can continue to trade on over-the-counter markets if they have less than 300 shareholders or if they have both less than 500 shareholders and less than US $10 million in assets. Going private requires the shareholders to sell all ownership interests to a private individual owner or group of owners. We were allowed to interview one such company as it endeavored to go private — albeit not in the manner originally intended.

Subsequent to our original study, one of our case study companies (reported about in Part I of this research report) decided to privatize to avoid the perceived negative effects of Sarbanes-Oxley Section 404 compliance structures on the firm's global competitiveness. Before the decision to privatize, the founder of the company held the positions of CEO and chairman of the board of directors, as well as being the single largest shareholder with an approximately 20 percent ownership interest. The founder and CEO put forth a proposal to make a leveraged buyout of the company with an explicitly stated concern that Sarbanes-Oxley Section 404 compliance was too costly. The board showed due diligence as it formed a special committee to review the offer, hire an investment banking firm to review the offer, and

[22]Katz, D.M. 2006. "Panels on 404 Skirt Small-company Woes." *CFO.com* (May 2).
Reason, T. 2006. "Cry of Pain From Small Companies." *CFO.com* (May 10).
[23]Leuz, C., A. Triantis, and T. Y. Wang. 2008. "Why Do Firms Go Dark? Causes and Economic Consequences of Voluntary SEC Deregistrations." *Journal of Accounting and Economics* (forthcoming).

had the investment banker solicit additional offers. Another suitor arose and outbid the CEO, placing the company under the ownership and control of a private equity firm. The CEO was subsequently dismissed. The private equity firm's successful pursuit of the company was inconsistent with prior research on acquisitions, as most of the normal motivators for acquisition were not present. First, the amount of free cash that was available to disperse to shareholders as dividends was very small, so excess cash reserves were not present. Second, there were no large blocks of stock held by institutional investors who might be more willing to facilitate an outside sale. Third, there was no unhappiness with the founder serving as CEO and chairman of the board; rather, the board actually chose the CEO's buyout offer over the private equity firm even though the CEO's price was lower. Fourth, other than the CEO, the remainder of the board consisted of independent directors.

However, there were alternative aspects of the organization that made it an attractive takeover target. First, it had performed very well and had high growth up until the last two quarters. The slowdown was blamed on the effects of Sarbanes-Oxley Section 404 compliance on the company's global competitiveness. Second, the slowdown over the last two quarters had led the company to be undervalued by approximately 25 percent based on its stock price. The CEO's failed offer was 20 percent over the current stock price at the time. Finally, when the board accepted the CEO's lower offer, a shareholder sued and required the deal to be nullified so as to maximize the value to shareholders.

The active involvement of a private equity firm in the bidding for the company and its ultimate success was only predictable if the impact of Sarbanes-Oxley Section 404 compliance was considered. First, a private equity firm had no requirement to obtain Sarbanes-Oxley compliance, so this perceived impediment to competitiveness was nullified. Second, the private equity firm held another similar company that was U.K.-based and viewed the acquisition of the company's industry expertise as valuable. Third, the private equity firm wished to take the U.K. company public on the U.S. exchanges, but needed to prepare for Sarbanes-Oxley Section 404 compliance before going public. The private equity firm, it turned out, was intentionally acquiring in part the company's expertise in Sarbanes-Oxley compliance, but at the same time backed off some processes in the acquired U.S. company to focus on a more risk-based approach for both companies. The risk-based focus that was encouraged under revised SEC interpretations of Sarbanes-Oxley Section 404 mandates allowed the firm to leverage what worked well in the acquired U.S. company to improve controls in both companies while eliminating a number of unnecessary manual processes that hampered competitiveness. The intent is to eventually go public with both companies.

III(b): Still Out of Control?

Sarbanes-Oxley Section 404 requires extensive strengthening of governance structures and reporting systems. The intense scrutiny of internal control systems has led many organizations to invest in IT to improve the reliability of such systems. However, maintaining the same corporate culture may inhibit an organization's ability to achieve operational and internal control synergies despite heavy investments in IT.

The organization examined in this case study specializes in developing cutting-edge Internet marketing solutions. The organization grew exponentially during 2000 to 2004, but that changed in 2005. Internal control issues surrounding their billing processes and the accuracy of billings contributed to customer attrition and accordingly the organization's performance suffered. The interview, as well as the Sarbanes-Oxley Section 404 management and auditor's reports, revealed that the organization lacked adequate controls, documentation, and automation. Attempting to satisfy Sarbanes-Oxley Section 404, the organization created an internal audit function and a Sarbanes-Oxley Section 404 compliance team, and

invested heavily in IT. Further complicating their Sarbanes-Oxley compliance, the organization merged with a European competitor and changed auditors from a Big Four firm to a local firm.

The major difference between this organization and the others that were examined lies in the failure of top management to embrace the goal of better corporate governance and enhanced risk management. The organization's founder and CEO had an entrepreneurial spirit that pushed the envelope as he developed and provided cutting-edge marketing solutions to the organization's customers. While this maverick attitude served the organization well in its early years as it navigated through its less travelled niche in the marketing sector, the same attitude and entrepreneurial spirit became a hindrance in the more control-oriented post-Sarbanes-Oxley regulatory environment. The interview revealed that the organization's top management viewed Sarbanes-Oxley compliance as a nuisance task that interfered with their market flexibility and business operations. In short, the organization did not embrace ERM as a facilitator of strategic flexibility and, not surprisingly, the focus on strategic responsibility caused the organization to unravel in the absence of managerial control processes.

Although the organization competed in a technology-driven market, it focused its investments in IT on external reporting processes, which were neither intended nor designed to be integrated into the organization's business processes. Many of the controls that were designed to meet Sarbanes-Oxley Section 404 compliance mandates were superficial and intentionally designed to minimize any impact on operations. Top management was adamant about continuing business in its unfettered reactionary form despite Sarbanes-Oxley compliance and had no desire to create synergy between the system of internal controls and the business operations. The goals for the new IT systems were so narrowly defined that, in many cases, due diligence simply was not performed. For example, a popular system integration software (Hyperion) was purchased, but would not work because one of the major systems (SAP 1) was customized. Top management's attitude toward Sarbanes-Oxley compliance can be summed up as "Hire some people, buy some software, and make this thing go away."

Notwithstanding the investments in technology, the organization still manually extracted financial data from different systems and compiled them to produce organizationwide financials. With heavy investments in IT and very little Sarbanes-Oxley Section 404 compliance progress, the organization subsequently outsourced the majority of its accounting functions. Only the compilation of financial data was performed by the organization's in-house accountants. Eventually, their problems with IT led the firm to outsource their operating systems as well. Unfortunately, outsourcing operating systems in a technology-driven market can lead to a shedding of tacit knowledge that provides the organization's competitive advantage. The organization eventually downsized 20 percent of its employees in 2007 and another 15 percent in 2008. The CEO and founder has since been relieved of his position and the organization began to sell off certain core operating units while acquiring other small organizations. Not surprising, today the organization is very different than it was when it started the Sarbanes-Oxley Section 404 compliance process in 2004. It has spun out of control by trying to achieve performance while employing pre-Sarbanes-Oxley designed business processes without post-Sarbanes-Oxley ERM processes that would monitor and enable strategic flexibility.

III(c): Maintaining Compliance During Acquisitions and Mergers

For many organizations, the Sarbanes-Oxley Section 404 compliance process was a very inward focused approach that was tailored to their specific organization. But what happens when an organization that has achieved compliance wants to add to their business through an acquisition or a merger? How does the organization handle the transition without risking an exception or qualification on their management and audit reports on controls? To look at answers to these questions, our team turned to a utility company that had been previously documented in a prior IIARF study on ERM as a model organization. The key was

that the organization we studied was now selling off operations to other organizations who were acquiring the business.

The U.S. Midwestern utility was relatively small and attempting to compete in an environment dominated by large players. It became increasingly clear that the logical business decision was to sell off some smaller business units that fell under specific state regulatory frameworks and required different tracking and control from other business units. However, the acquiring organizations were concerned with the specific issue addressed in this section — how to assure that the acquiring organization's overall Sarbanes-Oxley Section 404 compliance was not jeopardized by the merger. Our case study company used their expertise in Sarbanes-Oxley Section 404 compliance and ERM as a selling point during the process. A little history might help.

The utility was an accelerated adopter of Sarbanes-Oxley Section 404 internal control mandates and accordingly, like most organizations in that era, they focused on a bottom-up approach to controls, identifying key controls in all major processes. The result was an extensive documentation and testing of close to 600 control procedures. With the release of AS 5, the Q&A released by the PCAOB, and the clear message that a top-down approach is what was really desired, the organization took on a retooling of the control processes. At the same time, the CAE undertook an extensive ERM implementation plan. The ERM strategy worked in synergy with the top-down risk-based focus on controls that was desired after the first year of Sarbanes-Oxley compliance. Additionally, the utility purchased software to help automate the documentation and monitoring of control processes. As a result, the utility became a model of how the Sarbanes-Oxley Section 404 compliance process should be handled and how ERM can help make the process more efficient through a risk-based orientation.

The effectiveness with which the utility handled the compliance process was an asset during the business sell-off process. The utility agreed during the sale and acquisition process to provide transition services to maintain the controls over the processes. As transition teams were set up with the acquiring organization to handle the transition across a broad range of business issues, a transition team also was set up to specifically handle Sarbanes-Oxley Section 404 compliance processes. The utility agreed to maintain control processes and procedures, and monitor them for the first three months after the sale. As noted by the CAE, this transition process was not viewed as a Sarbanes-Oxley issue, but rather as a business issue and a part of effective ERM.

One other aspect of interest was the use of SAS 70s for relationships with trading partners. The utility used SAS 70s extensively in the first year of compliance to make sure the bases were covered. With the transition to a risk-based approach, the trading partners were re-scoped and many of the SAS 70s were dropped in the third and fourth years of compliance. This experience and knowledge attained in risk-based compliance was also applied during the transition. When the acquiring organization insisted on a SAS 70 from the utility to cover the three-month transition period, the utility countered that under a risk-based approach, there was no way that the relationship should be considered material and it was therefore an unnecessary control procedure and expense. The acquiring organization reviewed the counterarguments and relented on the requirement of a SAS 70 from the utility.

Review of the sale and acquisition process demonstrates an effective strategy for the transition period that alleviates concerns from a compliance perspective. The process provides a good best practices example for use by other organizations both in terms of considering the process from a risk-based orientation and determining how to handle transition processes smoothly. Just as organizations would do for other aspects of the business, a transition team to facilitate both maintenance of control processes and the integration of ERM strategies should be an integral part of the overall transition process.

IMPLICATIONS AND CONCLUSION

The results from the research conducted provide an array of insights into the Sarbanes-Oxley compliance process. The Phase I case studies provided insights into the key role that ERM, IT systems and data availability, organizational adaptiveness to change, and the control environment established by the "tone at the top" all played in the difficulty of the Sarbanes-Oxley implementation process and the perceived impediments to supply chain performance. The Phase II survey of a broad range of organizations added clarity to the overall picture as the results confirm the importance of the factors identified in the initial case studies, but also demonstrate that strength across the factors on a whole both eased the difficulty of implementation and actually led to improved supply chain performance. Effective ERM in particular appears critical to making compliance processes work efficiently while at the same time enhancing performance. The Phase III case studies focused on issues surrounding ongoing compliance and provided perspectives on a variety of dimensions — most notably challenges to delisting organizations to avoid regulatory oversight, approaches to protecting compliance during mergers and acquisitions, and negative impacts from failing to both address control deficiencies and embrace control processes as an integral part of critical business processes.

In Phase I, we conducted four case studies with a range in size among SMEs and with both difficult and non-difficult experiences in meeting compliance. All of our organizations adopted a perspective that Sarbanes-Oxley Section 404 compliance was really a focus on improving overall ERM. As such, all four organizations substantially improved their ERM procedures and felt that they benefited from the compliance process. However, the organizations that relied more on manual controls and did not have strong information systems in place to facilitate information sharing struggled through the process. The organizations with stronger information systems had an easier time complying and more effective ERM processes at the end of their first-year experiences. A focus on further automating control processes was a prevalent theme during the subsequent year's compliance focus. It was also notable that firms that developed stronger ERM processes maintained a better culture in terms of adapting to change — a key component of strategic flexibility. Thus, while the organizations broadly felt their supply chain performance was hampered by lost flexibility (only Company A provided evidence of such an effect), in the team's discussions with the organizations the lost flexibility was not apparent for the other companies.

Based on these findings, Phase II of the study focused on a broad-based survey of organizations to better understand the relationships among these various factors. We collected survey responses from more than 250 CAEs to learn more about their experiences. The initial analyses focused on organizations' structures and processes prior to Sarbanes-Oxley Section 404 compliance and the relationship with the difficulty of meeting compliance mandates. The data supports the view that ERM was fundamental to easing the process and also shows that effective ERM drives better integration of information systems with enterprisewide data sharing, enhances strategic flexibility, and leads to a stronger control environment. It is worth noting, however, that the integrated information systems were a critical bridge for effective ERM to drive enhanced strategic flexibility. The analyses also showed that strategic flexibility coupled with a strong control environment were critical to efficient Sarbanes-Oxley compliance efforts.

The survey data also covered organizations' post-Sarbanes-Oxley organizational structures and processes along with performance. Analysis of this data shows that organizations with stronger ERM post-Sarbanes-Oxley exhibit higher levels of strategic flexibility and better supply chain performance. However, in this post-Sarbanes-Oxley environment, it was clear from the study results that strong, integrated information systems were critical to this positive effect of ERM on strategic flexibility and supply chain performance.

The Phase III case studies focused on specific concerns of interest in a post-Sarbanes-Oxley compliance world. We looked at a company that struggled but made it through the Sarbanes-Oxley process, an organization that failed to achieve control at a level appropriate for a positive Sarbanes-Oxley, and a company who very successfully handled the Sarbanes-Oxley Section 404 compliance process, but due to business and industry issues needed to sell off certain business units while helping the acquiring companies avoid any risk of control weaknesses developing during the transition.

The first company that struggled through the process attempted to delist by going private. The CEO and founder of the company attempted to buy the company back. The board was favorable, but the CEO and founder was blindsided by a private equity firm that came in and outbid the founder to essentially acquire the company's expertise from both a business and a compliance perspective. The events suggested that compliance processes can be an important factor that should be considered when weighing business acquisitions.

The second company basically disdained the compliance process and tried to keep it separate from the actual business processes. This failure to view controls as an integral part of business operations and business processes predictably led to more problems. The company had to report material weaknesses in controls and subsequently the uncontrolled business processes began to unravel and the company's market share dipped substantially. The company eventually merged with a competitor and the joint company continues to struggle to bring processes under control and to reverse the business spiral downward. The business issues can be directly tied to control weaknesses and failures to integrate business processing with effective control procedures.

The third company strongly reinforced a view of compliance process value. This utility sold off several of its units to competitors in the same region. An integral part of the transition process as units transferred to the acquiring companies was the existence of a transition team specifically focused on Sarbanes-Oxley Section 404 compliance issues and the maintenance of controls over processes. The company agreed during the sale to continue managing business processes for the sold-off units for three months post-sale while the units were integrated into the new company's systems and processes.

On an overall basis, our results indicate that effective ERM processes should be an integral part of an organization's strategic vision and operations. Well-controlled companies that manage their risks are shown to have better strategic flexibility, better performance, and enhanced value. Ultimately, the results of this study suggest that the Sarbanes-Oxley Section 404 compliance process helped most organizations and that better controls lead to more successful businesses. As one of our case participants noted, "Sarbanes-Oxley does not ask for companies to do anything that they should not have been doing already."

UNDERSTAND, SHAPE, ADVANCE

The IIA Research Foundation is a 501(c)(3) corporation formed to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.

Through its research reports, Bookstore products, and GAIN Knowledge Services, The Foundation provides resources that help understand, shape, and advance the global profession of internal auditing by initiating and sponsoring intelligence gathering, innovative research, and knowledge-sharing in a timely manner.

To learn more, visit www.theiia.org/research

ISBN 978-0-89413-671-9
Item #2019.dl
Free to IIA Members
Non-members: US$40

The Institute of Internal Auditors Research Foundation

Anexo V – Terceiro estudo – "*Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-organizational Settings*", de Shannon W Anderson, Margaret H. Christ e Karen L. Sefatole.

Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-organizational Settings

by

Shannon W. Anderson
Rice University

Margaret H. Christ
The University of Texas at Austin

Karen L. Sedatole
The University of Texas at Austin

January 2006

The Institute of Internal Auditors
RESEARCH FOUNDATION
Understanding. Guiding. Shaping
www.theiia.org/research

Disclosure

The IIARF publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors' (IIA) International Professional Practices Framework for Internal Auditing (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The mission of The IIARF is to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN 978-0-89413-649-8
01/06 First Printing

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This document reports on the findings of an academic study funded by The Institute of Internal Auditors Research Foundation (Anderson et al. 2006). Contact the authors for the complete study. The authors are grateful to The Institute of Internal Auditors and its membership for their participation in this project. This research benefited from the helpful suggestions of Urton Anderson.

ABOUT THE AUTHORS

Shannon W. Anderson, Ph.D., served on the faculty of the University of Michigan Business School for nine years before joining the Jones School of Management at Rice University in 2001. She earned a doctorate in Business Economics at Harvard University and a B.S.E. in Operations Research at Princeton University. Her research focuses on designing and implementing performance measurement and cost control systems to support management decision-making and has been published in the *Accounting Review*, *Accounting Organizations and Societies*, *Accounting Horizons*, *Production and Operations Management*, the *International Journal of Flexible Manufacturing Systems, Management Science,* and the *Journal of Management Accounting Research.* She is also co-author of the book *Implementing Management Innovations*. Before returning to school to pursue her doctorate, Professor Anderson worked as an engineer for General Motors Corporation. As a part of her research program, Professor Anderson has worked with firms in a wide variety of industries, including: automotive, pharmaceuticals, machine tools and industrial equipment, defense contractors, commercial construction, textiles, and industrial glass.

Margaret H. Christ, CIA, CPIM, is a doctoral student of Accounting at the McCombs School of Business, The University of Texas at Austin. Margaret earned her BS in accounting with a concentration in internal auditing at Louisiana State University. Prior to her doctoral work, she worked as an internal auditor for a Big Five public accounting firm and an independent risk consulting firm. She is a certified internal auditor (CIA) and is certified in production and inventory management (CPIM). As an internal auditor, her clients included Fortune 500, multinational and local firms in a variety of industries, including energy services, retail, manufacturing, banking, hospitality, and waste management.

Karen L. Sedatole, Ph.D., is an Assistant Professor of Accounting at the McCombs School of Business, The University of Texas at Austin. Karen earned her BSE in computer engineering from Baylor University, her MBA from The University of Texas at Austin, and her Ph.D. from The University of Michigan. Prior to her doctoral work, she worked as a systems consultant, designing and implementing customized client information systems used in forecasting, planning, and decision-making. Professor Sedatole's research interests are in management control systems, including issues related to performance measurement and rewards. Her current research examines the role of non-financial performance measures in predicting future financial performance, and the determinants and consequences of the use of financial and non-financial performance measures in managerial incentive contracts and in inter-organizational settings. Her research, which includes experimental, archival, and field research methodologies, has been published in *The Accounting Review*, *Accounting Horizons, Journal of Services Marketing,* and *Accounting, Organizations and Society*.

ABSTRACT

Using data from a survey administered to 151 chief audit executives and internal audit consultants, this research seeks to identify, categorize, and quantify common and systematic risks associated with the formation and performance management of innovative inter-organizational forms, control practices currently being implemented, and effectiveness of chosen control practices.

EXECUTIVE SUMMARY

Firms are increasingly using collaborative organizational arrangements (e.g., joint ventures, strategic alliances, and strategic supply chains) to complete transactions that require a high level of inter-organizational involvement and coordination. The adoption of these organizational forms has created a need for new management control practices that comprehend the risks of transacting with self-interested parties when complete contracts cannot be written or when the cost of doing so is prohibitive. This study seeks to identify, categorize, and quantify:

1. The common and systematic risks associated with the formation and performance management of innovative inter-organizational forms, and
2. The control practices currently being implemented by firms engaged in these activities.

Using a Web-based survey, we obtained responses from 151 chief audit executives and internal audit consultants regarding the inherent level of specific risks their firms face as a result of their critical strategic alliances, as well as the specific control mechanisms they use to manage these risks. Specifically, we identify and collect data from respondents regarding risk and controls associated with four specific types of strategic partnerships:

1. Upstream partnerships,
2. Downstream partnerships,
3. Marketing partnerships, and
4. Research and development partnerships.

We use the COSO Enterprise Risk Management (ERM) framework (COSO 2004) to guide our investigation of the processes by which firms identify, assess, and manage business risks as related to these four types of strategic alliances. We focus on two of the COSO ERM risk management components (risk assessment and control activities) and provide additional insight into the control activities component by integrating into our analysis the “Levers of Control” framework as proposed by Simons (1995). In the framework, Simons describes four control levers – beliefs systems, boundary systems, interactive control systems, and diagnostic control systems – each with a distinct purpose for controlling business activities while maintaining an innovative work environment.

Results indicate that most of the risks faced by firms as a result of strategic alliances are not highly probable; however, many of the risks would be highly detrimental to the firm if they were to occur. Therefore, careful management of these risks is critical to the success of the alliance partnership and the strategic objectives of the firm. Further, consistent with the theory underlying the Levers of Control framework, firms use all four levers to control the risks raised by strategic alliances, regardless of the type of alliance. However, the specific control mechanisms that firms use differ for the different types of alliances. Finally, respondents indicate that the use of SAS 70 reports as a control mechanism has increased greatly as a result of the U.S. Sarbanes-Oxley Act of 2002.

INTRODUCTION

Recent evidence indicates that firms have dramatically increased the use of strategic collaborations for transactions that require a high level of involvement and coordination between alliance partners (Anderson and Sedatole 2003). These collaborations may take the form of arrangements that align the interests of participating parties through formal profit-sharing rules (e.g., franchises, licensing agreements, and joint ventures). Alternatively, they may take a more amorphous form, using few mechanisms from contract law to structure their interactions or allocate the gains from trade (e.g., strategic alliances, consortia, and strategic supply chains). However, it is important to recognize that collaborative organizational forms are inherently risky and, in fact, it is this additional risk which offers many of the important strategic advantages, as long as those risks can be "safely managed" (Buehler and Pritsch 2003).

In this study, we suggest that the adoption of collaborative organizational forms has created a need for new management control practices that comprehend and effectively manage the risks of transacting with self-interested parties when complete contracts cannot be written or when the cost of doing so is prohibitive. Historically, many of the risk identification and risk management tasks have fallen to managers who work in the area of strategy. However, as collaborative organizational forms are adopted as equilibrium forms of organizing, inter-organizational control must devolve to those in the role of internal auditor.

This research is important to managers and internal auditors of firms that utilize strategic alliances to enhance their business practices. The results of this study provide valuable insights into the types of risks that can be expected when entering into an inter-organizational collaboration, as well as the level of impact (magnitude) and the likelihood of the occurrence (probability) of specific risks. Further, the results can be used as guidance for firms that strive to effectively manage inter-organizational collaborations, as it describes the practices commonly used by a diverse cross section of firms.

The primary contribution of this study is to provide descriptive evidence of the different types of risks that affect firms that engage in strategic alliances and the management control practices these firms use to manage those risks. To do so, we conducted an online survey of chief audit executive (CAE) and consultant members of The Institute of Internal Auditors (IIA). Participants were solicited through e-mail communication from the Institute of Internal Auditors Research Foundation (IIARF) and provided responses to a Web-based survey. The survey consisted of questions regarding the management of strategic alliance networks in general, as well as specific questions regarding the type of strategic alliance with which the respondents were most familiar.

Using the COSO Enterprise Risk Management (ERM) framework (COSO 2004), we provide data describing the risks faced by firms when operating within each of the major alliance categories: upstream partnerships, downstream partnerships, marketing partnerships, and research and development partnerships. As we discuss below, many firms currently use, or are in the process of implementing, the COSO ERM framework. Therefore, the use of this framework provides a meaningful and practical context for our results. Further, we integrate the Levers of Control framework (Simons 1995) to provide a basis for organizing and understanding the types of control mechanisms commonly used by firms to manage the risks that arise as a result of their participation in strategic alliances.[1] The four control levers identified by Simons (1995) are:

1. Beliefs systems – organizational standards used to reinforce the firms' core values,
2. Boundary systems – regulations regarding what partners are *not* to do,
3. Diagnostic control systems – traditional feedback systems,
4. Interactive control systems – formal information systems that allow management to involve themselves regularly and personally in the partner's activities.

[1] In Anderson et al. (2006), we further analyze the correlations between risks facing firms engaging in strategic alliances and the control practices implemented to manage these risks. In addition, that study includes descriptive evidence of control practices used by three large companies and one national consulting company that specializes in risk management based on extensive interviews.

Finally, we provide preliminary evidence regarding the changes to control practices firms have undertaken in response to the enactment of the Sarbanes-Oxley Act , which requires that firms assess the risks and internal control practices of certain strategic partners.

Our results indicate that while most of the risks introduced by strategic alliances are not highly probable, many would be highly detrimental to the firm if they were to occur. Further, we find that firms rely on many types of control mechanisms to manage their strategic partner risk. Specifically, we find that firms tend to rely on each of the four Levers of Control (Simons 1995) equally. Finally, respondents indicate that they are making significantly greater use of SAS 70 reports as a means of demonstrating that key strategic partners have adequate internal control practices than they did prior to the enactment of Sarbanes-Oxley.

In the following sections, we provide a brief review of prior academic literature. We then describe the management risk and control frameworks used to guide our survey development. We use the COSO ERM framework to organize and examine the risks faced by firms using strategic alliances and the Levers of Control typology, designed by Robert Simons (1995), to organize and describe the relevant control practices utilized by these firms. After describing the research methodology and participant demographics, we provide the results of our survey regarding risks faced by firms using strategic alliances and the control mechanisms used to manage those risks, respectively. We conclude this report by describing implications of the Sarbanes-Oxley Act on strategic alliance risks and control systems followed by some concluding remarks.

REVIEW OF RELEVANT ACADEMIC LITERATURE

Strategic alliances account for a large and increasing segment of the global economy today. Since the 1980s, the number of alliances has increased by approximately 20% per year and account for as much as 25% of firm revenue for many U.S. companies (Ernst 2002). As alliances have become a dominant force in the world economy, they have also received substantial attention in academic research. Extensive research on transaction cost economics addresses the determinants of firm boundaries.[2] Further, there is increasing research on when and how firms choose "hybrid" organizational forms (e.g., Menard 1995, 1996; Williamson 1985, 1991), on the specific type of hybrid chosen (Buvik and Reve 2001; Gulati 1995; Gulati and Singh 1998; Osborn and Baughn 1990; Pisano 1989, 1990; Pisano et al. 1988) and on the determinants of hybrid success (e.g., Anand and Khanna 2000; Baum et al. 2000; Dekker 2003; Lorenzoni and Lipparini 1999; Stuart 2000; Wolff and Reed 2000; Zaheer et al. 1998). However, there is little research on the day-to-day controls used by firms in managing collaborative arrangements.

The high incidence of failure of collaborative arrangements – reportedly, 60 percent of alliances fail – (Anonymous 2000), is typically linked to the *risks* associated with collaborative organizational forms; risks associated not only with the lack of cooperation among partner firms, but also with performance failure *despite full cooperation* (Das and Teng 1996, 2000, 2001). Indeed, collaborative arrangements are subject to severe "business process" and "information risks" (as defined by Kinney 2000). *Business process risks* include the risks associated with "hold-up" by a partner firm and risks associated with the inequitable allocation of collaboration returns in the absence of complete contracts. The measurement of partner performance and overall collaboration performance is difficult in many of these settings in which performance quality is not clearly defined (e.g., R&D alliances). This represents a significant *information risk* to individuals (e.g., internal auditors) attempting to monitor and control such collaborations.

There is a fairly extensive literature on collaborative arrangements examining the role of individual and organizational *trust* in enabling economic transactions that appear to be subject to severe risks (i.e., hazards of opportunistic behavior) (e.g., Granovetter 1973; Lewis 1999; Ring and Van De Ven 1992; Ring and Van De Ven 1994; Zaheer et al. 1998; Zaheer and Venkatraman 1995). Although empirical studies generally confirm trust as an important determinant of strategic alliance success, it is not clear to

[2] See Anderson and Sedatole (2003) for a brief review of this literature as it relates to managerial and accounting controls.

what extent trust serves as a complement to or substitute for other forms of control in collaborative settings. Nor is it clear how firms create or even measure trust levels in these settings.

Previous research on control practices in collaborative arrangements (Anderson and Dekker 2005; Anderson et al. 2000; Christ et al. 2005; Coletti et al. 2005) has attempted to provide initial evidence on the relationship between transaction characteristics, the design of inter-organizational control practices, the trust levels created, and the performance achieved under alternative control design choices. The current study adds to extant literature by identifying the common and systematic risks associated with various forms of collaborative arrangements and the control practices currently being used by firms to manage those risks. Further, based on data obtained by CAEs and internal audit consultants, we are able to quantify the pervasiveness and magnitude of the risk management and control problems in a large cross section of firms.

MANAGEMENT RISK AND CONTROL FRAMEWORKS

COSO (2004) Enterprise Risk Management-Integrated Framework

In reviewing the literature, and based upon discussions with practicing internal auditors, we identified several commonly used risk frameworks. We selected one, the COSO Enterprise Risk Management-Integrated Framework (hereafter, COSO ERM) developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO 2004) for providing a useful structure for our survey.[3]

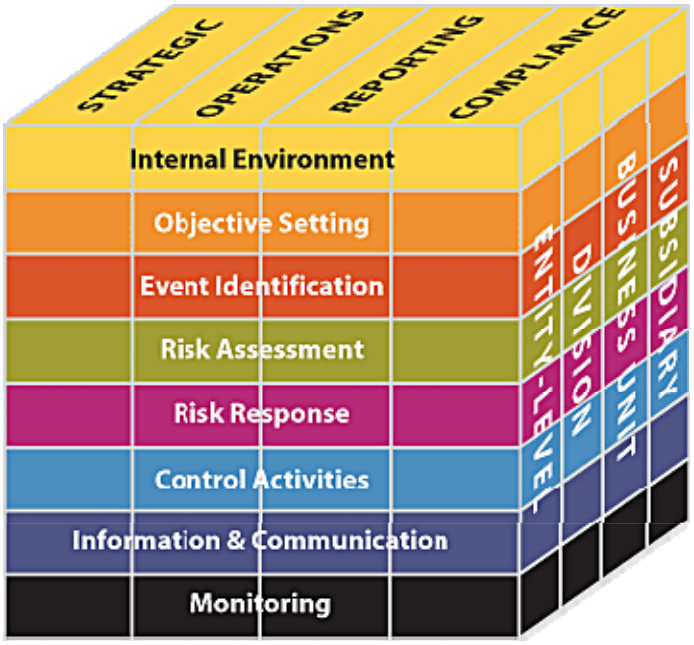
COSO ERM, released in 2004, was developed to provide a robust framework to guide firms through the identification, assessment, and management of business risks. The framework is designed to be implemented by management during strategy setting, during which management considers the risks inherent in each of the strategic alternatives. These alternatives may include, but are not limited to, the decision to form new strategic alliances. The key purpose of the framework is to "help managements of businesses and other entities better deal with risk in achieving the entity's objectives" (COSO 2004). Further, the framework seeks to integrate various risk management models and develop a common tool for enterprise risk management.

COSO ERM recognizes that first, and foremost, companies strive to increase shareholder value. However, greater shareholder value is not achieved without increased business risk, which is defined as "the possibility that an event will occur and adversely affect the achievement of objectives" (COSO 2004, p. 4). COSO ERM establishes four classes of business objectives: (1) strategic, (2) operations, (3) reporting, and (4) compliance. Strategic objectives are those which relate to high-level goals and are aligned with and supporting the firm's mission. Operations objectives relate to the effective and efficient use of firm resources. Reporting objectives are those that relate to the reliability of a firm's reporting and compliance with relevant laws and regulations (COSO 2004, p. 9). By organizing business objectives into these classifications, firms are able to focus specifically on the separate aspects of enterprise risk management and concentrate on achieving performance and profitability objectives while preventing losses.

[3] The other frameworks considered were the Australian Standards and Basel II. However, results from discussions with practicing internal auditors, survey responses, and current practitioner literature suggest that the COSO ERM framework is currently the most widely used framework. For example, results from an IIA GAIN survey conducted in 2004 indicate that 84% of respondents expected that the issuance of the COSO ERM framework would have at least a little impact on their current ERM practices. Further, 60% of respondents indicated that their firm had already implemented a formal ERM system to some extent. In addition, while the PCAOB does not expressly require that management use the COSO ERM framework for its assessment of the adequacy and effectiveness of internal controls, it does indicate that this is a suitable framework. Further, Auditing Standard No. 2, issued by the PCAOB in 2004, uses the COSO ERM framework as a basis for directing management's internal control assessment activities because of the "frequency with which management of public companies are expected to use the framework for their assessments" (Public Company Accounting Oversight Board (PCAOB) 2004, p. 9).

COSO ERM also identifies eight interrelated components of enterprise risk management: (1) internal environment, (2) objective setting, (3) event identification, (4) risk assessment, (5) risk response, (6) control activities, (7) information and communication, and (8) monitoring, which are represented by the horizontal rows of the COSO ERM three-dimensional cube as shown in Exhibit 1. Each component of risk management is applicable to all four objective categories for the firm. Finally, the organization and its units (subsidiaries, business units, and divisions) are represented on the third side of the cube to indicate that enterprise risk management may pertain to the enterprise as a whole, or any of its business units or segments. The COSO cube is intended to illustrate the direct relationship between the objectives (what the firm strives to achieve), enterprise risk management components (how the entity will achieve the objectives),and the business units of the firm.

Exhibit 1
COSO ERM Three-dimensional Matrix (COSO 2004)*



*This cube-shaped, three-dimensional matrix illustrates the direct relationship between objectives and the enterprise risk management components (COSO 2004).

Our research focuses on the risk assessment and control activities components of COSO ERM. The risk assessment process allows management the opportunity to consider the extent to which potential events may have an effect on the achievement of firm objectives. Generally, management assesses each potential event based upon the expected likelihood of occurrence and the potential impact of the event using a combination of qualitative and quantitative methods. Control activities are the policies and procedures implemented to ensure that management's risk responses are carried out as intended (COSO 2004).

Based upon interviews with practicing internal auditors we have identified a set of risks that often develop or intensify when a firm enters into strategic alliance relationships. We have classified these risks as they affect the four business objectives identified by the COSO ERM framework (see Exhibit 8 below).[4]

[4]It is important to note, however, that our classification is based on a general understanding of these risks. As noted in the COSO framework, "no two entities will or should apply enterprise risk management in the same way" (COSO 2004, p. 11). Therefore, risk classifications may vary between firms. Further, for simplicity, we restrict our

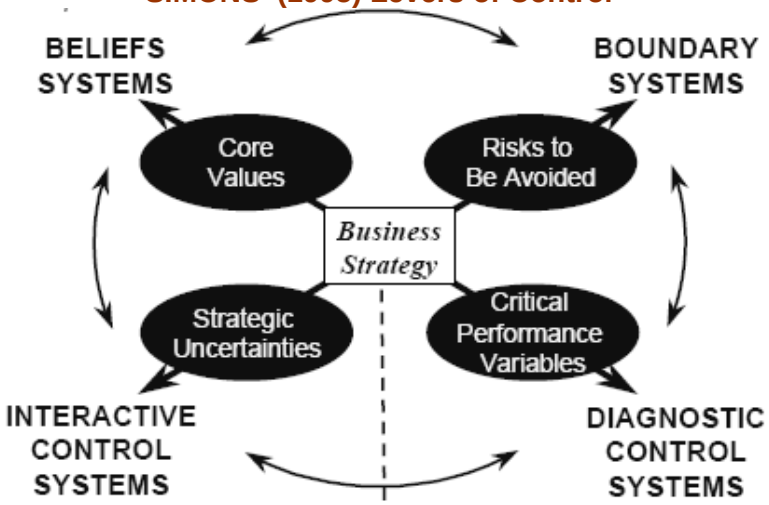
Typically, the risk assessment process includes consideration of both inherent and residual risk. However, in our survey respondents were instructed to focus on inherent risk only so that we could gain an understanding of the extent to which these risks exist in the absence of any control techniques management may implement. Therefore, respondents provided their assessments of the inherent probability and magnitude of each of these risks. Finally, we have identified the control mechanisms used by firms to address these risks.

SIMONS' (1995) LEVERS OF CONTROL FRAMEWORK

Firms that use inter-organizational collaborations require flexibility and typically embrace innovation. As such, these firms cannot be effectively controlled using traditional control methods alone. Instead, management must empower employees to initiate process improvements and respond to opportunities in a manner that is consistent with the overall objectives of the firm. To do so, management must strike a balance between opportunity and control. The Levers of Control framework, designed by Robert Simons (Simons 1995), provides a structure for finding this balance (see Exhibit 2 below).

In the framework, Simons describes four control levers, each with a distinct purpose for controlling business activities while maintaining an innovative work environment. While the original intent of the Levers of Control framework is to provide a control structure for managing internal activities of firm employees, we suggest that the framework is applicable to firms managing their strategic alliance relationships as well. In a strategic partnership, it is imperative that firms use an appropriate combination of controls and trust. Prior research suggests that a main cause for alliance failure is uncertainty of partner cooperation, also known as "relational risk" (Das and Teng 1996; Das and Teng 1998; Das and Teng 2001). Formal control systems help to mitigate relational risk by reducing the opportunities and/or incentives for opportunistic behavior. However, prior research also suggests that implementation of control systems may have negative signaling effects that result in reduced trust and decreased cooperation (Christ et al. 2005; Das and Teng 2001). Because cultivating and maintaining high levels of trust between alliance partners is vital to strategic alliance success, the choice of controls in strategic alliances is of paramount importance. By utilizing the Levers of Control framework, firms can strike a balance between more traditional, formal control mechanisms as well as more abstract control systems, such as corporate norms and interactive feedback. This balance is necessary to facilitate the innovations sought by the alliance formation while maintaining adequate control.

Exhibit 2
SIMONS' (1995) Levers of Control



Reprinted from: Simons (1995)

---

categorization to only one objective per risk; however, under COSO ERM risks may be classified under multiple objective categories.

The first lever of control described in the framework is *belief systems.* These are the organizational standards that are used to reinforce the core values, purpose, and direction of the organization. Examples of belief systems include corporate credos and mission statements. *Boundary systems* comprise the second lever of control. Boundary systems indicate the minimum standards of a company and indicate what partners are *not* to do. The third control lever, *diagnostic control systems,* is defined as feedback systems and include the most traditional control practices used by management. Diagnostic control systems are designed to: (1) measure the outputs of a process, (2) identify the existence of a predetermined benchmark to which results can be compared, and (3) enable the manager to correct deviations from these benchmarks. Finally, the fourth lever, *interactive control systems*, is formal information systems that allow management to involve themselves regularly and personally in the partner's activities.

Based upon discussions with professional internal auditors, we developed a comprehensive list of control mechanisms commonly used by firms for controlling the risks related to their strategic partnerships. In Exhibit 3, below, we have categorized those controls within the Levers of Control framework. We use this categorization when describing the control practices most often used by our survey respondents for managing their strategic alliance risks. We further categorize these controls by the more familiar categories utilized by internal auditors of preventive, detective, and monitoring controls.

Exhibit 3
Control Practices Commonly Used in Strategic Partnerships
Classified by Simons' (1995) Levers of Control Framework

Lever 1: Belief Systems	
Preventive	• Written and agreed-upon code of ethics or code of conduct • High level of trust between partners
Lever 2: Boundary Control Systems	
Preventive	• Written policies and procedures regarding alliance operations • Strategic identification of suppliers • Standard contract template • Contract terms detailing specific payment terms, delivery dates, etc. • Contract terms specifying cost sharing arrangements • Contract provisions to assign property rights • Contract terms regarding handling of failure to meet contract terms • Other contract terms • Segregation of duties within the alliance • Authorization levels for investment decisions (within the alliance) • Physical safeguards of alliance assets • Physical safeguards of firm assets • Controls to protect proprietary information

Exhibit 3, cont.

Lever 3: Diagnostic Control Systems	
Preventive	• Formal review process for supplier selection • Require partners to provide SAS 70 reports • Contract terms specifying how performance will be measured for contract fulfillment • Contract terms related to dissolution of or exit from relationship • Interactive feedback for continuous learning between partners • Interactive feedback within the firm with respect to partner selection, alliance management, etc.
Detective	• Periodic announced audits • Periodic unannounced audits • Periodic review of your partner's financial information
Monitoring	• Ongoing review of non-financial performance indicators • Ongoing review of financial performance measures
Lever 4: Interactive Control Systems	
Preventive	• Accountability w/in firm for partner selection • Formation of formal profit-sharing entity (e.g., joint venture) • Composition of alliance management team • Accountability of alliance personnel for alliance performance
Monitoring	• Informal monitoring of partner operations

RESEARCH METHODOLOGY AND PARTICIPANT DEMOGRAPHICS

Research Methodology and Participant Demographics

With the assistance of The Institute of Internal Auditors Research Foundation (IIARF), we surveyed chief audit executive (CAE) and consultant members of The IIA. The survey was completed in spring 2005. We received 151 responses (98 CAEs and 53 consultants). CAE respondents represented internal audit departments of varying sizes as shown in Exhibit 4.

Exhibit 4
Descriptive Statistics for the Firms Represented by Respondents

Panel A: Size of Internal Audit Department

Size	Number of Respondents	Percentage of Respondents
1 auditor	12	12%
2 auditors	15	15%
3 – 10 auditors	43	44%
11 – 20 auditors	6	6%
21 – 30 auditors	5	5%
31 – 50 auditors	3	3%
51 – 100 auditors	1	1%
> 100 auditors	3	3%
Did not respond	10	10%

CAE respondents had an average of 13 years performing internal audit work and 5 years performing external audit services. Approximately 73% of respondents indicated that they were either chief audit executives or internal audit directors, with the balance indicating that they were internal audit managers or seniors. Approximately half of the respondents were from U.S.-based companies. About 62% indicated that they performed all internal audit services in-house, while 37% co-source some internal audit services and only 1% outsource the entire internal audit function.

Consultant respondents represent a variety of service firms, including Big Four public accounting firms (23%), other CPA firms (26%), and internal audit/risk management boutique firms (28%). Consultant respondents also hold a range of positions within their firms with 48% of respondents holding the title of partner or director at their respective firms, 19% managers,and 15% internal audit seniors. The respondents have an average 8 years of internal audit experience and 7 years of external audit experience. Additionally, they indicate that they have an average of 4 years of experience working with strategic alliances. Of the consultant respondents, 43% are certified internal auditors (CIA) and 36% are CPAs. Further 19% indicated that they are certified in Information Systems Audit (CISA) and 2% are certified in production and inventory management (CPIM). Finally, 25% of consultant respondents have been involved in performing SAS 70 reviews for their clients.

Both CAE and consultant respondents were asked a series of questions regarding the management of strategic partner networks. Further, the CAE respondents were asked to identify one critical partner with which they are knowledgeable and to classify that partner as one of four partner types: (1) upstream partners (53%) (e.g., such as raw materials suppliers, or product or service providers), (2) downstream partners (21%) (e.g., final assembly, transportation, and distribution partners or franchisees), (3) marketing partners (13%) (e.g., co-branding), or (4) research and development partners (13%). Participants were then asked a series of questions regarding the risk and controls used to manage that specific partner relationship.

Similarly, consultant respondents were asked to first identify one of the four types of strategic partnerships – upstream, downstream, marketing, or R&D – with which they had the greatest familiarity. They provided assessments of the risks and controls relevant to managing that specific type of partnership. Importantly, although CAE respondents were asked about their experience with the one critical partner who they identified, consultant respondents were asked to provide their overall impressions of the risks and controls in strategic alliances gained from their experiences with client firms.

Use of formal control and risk frameworks

Many companies adopt (or develop) formal control frameworks to provide guidance and structure to the control assessment process. Furthermore, in its final rule on management's report on internal controls over financial reporting, the SEC requires that companies include a "statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting" (SEC 2003 – www.sec.gov/rules/final/33-8238.htm). While the SEC does not specify which internal control frameworks are preferred, it does state that "a suitable framework must: be free from bias, permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting."

We asked respondents to identify the control framework currently in use by their company (or clients).[5] Based on discussions with internal audit practitioners and academics we identified the following control frameworks as the most commonly used: (1) COSO, (2) COCO, (3) COBIT, and (4) Turnbull Report. As shown in Exhibit 5, the largest percentage of respondents (46%) uses the COSO Internal Control-Integrated Framework to evaluate their internal control system. COBIT (Control Objectives of Information

[5] Responses may include partial implementation of control framework.

and Technology) was the second most frequently listed control system (20%). Only 18% of respondents indicated that their company (or clients) did not use a formal control framework of some kind.[6]

Exhibit 5
Use of Formal Control Frameworks

COSO	COCO	COBIT	Turnbull	Other	None
46%	2%	20%	3%	10%	18%

Risk frameworks provide a logical and often visual representation of the business risks faced by a company and are designed to be easily understood by personnel at all levels of the organization (McNamee 2000). Over the past several decades, various risk frameworks have been developed and widely adopted – the most recent being the COSO ERM framework which was released in September 2004.

Based on discussions with practicing internal auditors and academics, we determined that the following formal risk frameworks were the most commonly used: (1) COSO ERM, (2) Australian Standards, and (3) Basel II. We asked respondents to indicate whether their companies (or their clients' companies) had implemented one of these formal risk frameworks. Alternatively, if applicable, participants identified any other frameworks currently used by their company to assess business risk. As shown in Exhibit 6, COSO ERM is the most commonly used formal risk framework (37%). Only a slightly smaller percentage of firms, 32%, indicate that they use a formal risk framework classified as "other," possibly indicating the use of an internally developed framework. Further, we find that only approximately 10% of respondents have not implemented some sort of formal risk framework.[7]

Exhibit 6
Use of Formal Risk Frameworks

COSO ERM	Australian Standards	Basel II	Other	Type Unknown	None
37%	4%	12%	32%	4%	10%

[6] Many of the CAE respondents (63%) indicated that their companies were not required to comply with Sarbanes-Oxley; therefore, they would not be subject to the SEC's final rule requiring a statement identifying the control framework used by management.
[7] The survey question permitted participants to respond positively to this question if their firm was in the process of implementing part or all of any formal risk framework.

STRATEGIC ALLIANCE RISK ASSESSMENT

Management of the Strategic Partner Network

The benefits associated with strategic alliances are great; however, strategic alliances are inherently risky endeavors that require careful and methodological risk management throughout their lives – from partner selection, through the dissolution of the partnership. In general, firms must effectively manage: (1) selection risk, (2) monitoring risk, and (3) failure identification risk.

Selection risk is defined as the risk that the firm has nonexistent, irrelevant, or unreliable processes by which to select viable strategic partners. *Monitoring risk* is the risk that the firm lacks the appropriate financial and/or non-financial measures for evaluating the progress of the alliance. Finally, *failure identification risk* is the risk that the firm will have nonexistent, irrelevant, or unreliable processes by which to identify when a partnership should be terminated.

CAE and consultant respondents provided their evaluations of the magnitude and probability of occurrence for each of the three risk types as they relate to the entire strategic partner network of the firm. Their responses, displayed in panels A – C of Exhibit 7, indicate that for most firms, these risks have a moderate to high expected impact. Expected impact is calculated as the magnitude of the risk multiplied by the probability of occurrence for that risk. CAEs and consultants provided their evaluations of magnitude and probability using a 7-point Likert scale (1 indicates no magnitude or likelihood and 7 indicates very high magnitude or likelihood). Thus, an impact score of 16 indicates that the CAE rated both magnitude and likelihood to be moderate and an impact score of 49 indicates the highest possible rating, 7, was provided for both magnitude and likelihood. As can be seen in Exhibit 7, over 35% of respondents indicate that each of the three risk types have a moderate impact on the operations of the firm. It is also important to note that a large number of respondents (greater than 20% for each risk type) indicate that the potential impact for each of these three risk types is much greater than moderate. Several respondents also indicated that the manifestation of these risks would have a critical impact on the operations of their firm, as evidenced by responses yielding the upper bound of 49 (untabulated).

Exhibit 7
Strategic Alliance Network Risk Assessment**

Panel A: Net Impact of Selection Risk

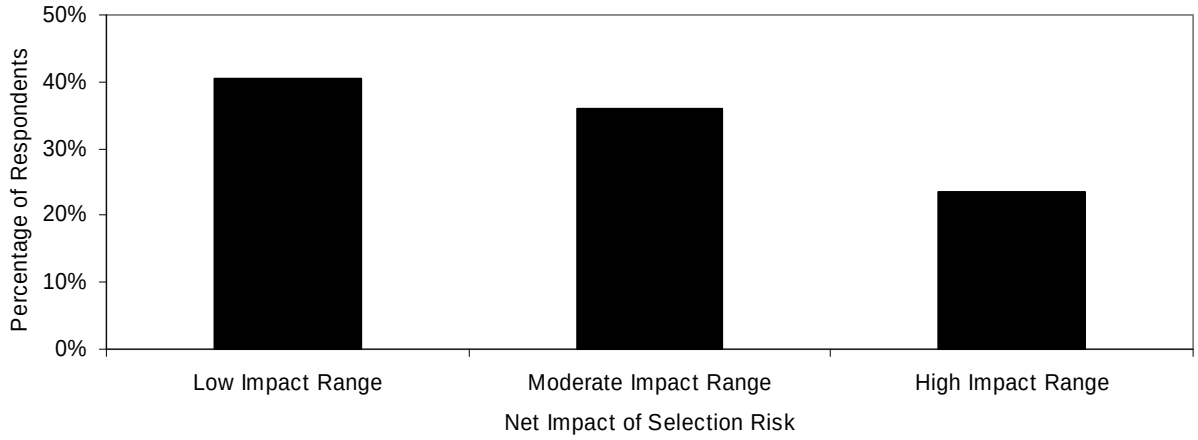
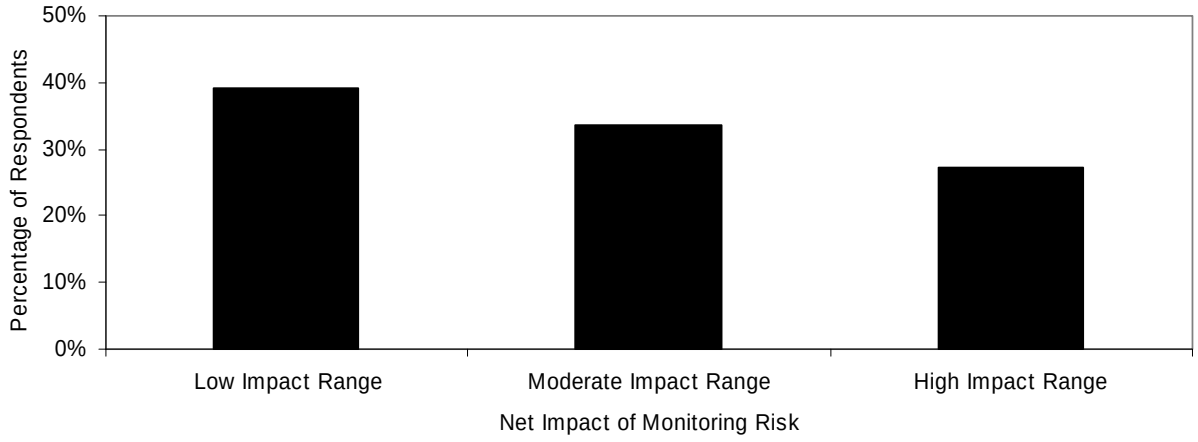
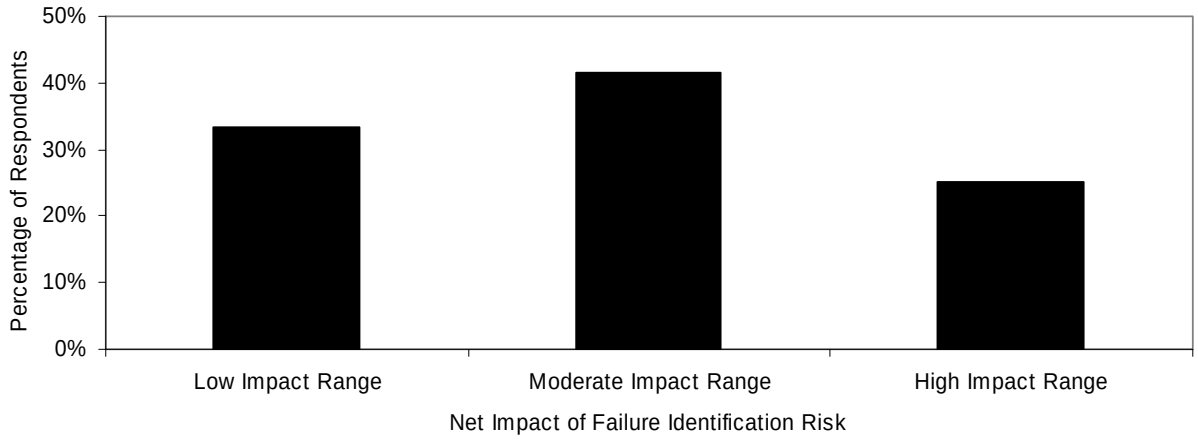


Exhibit 7, cont.

Panel B: Net Impact of Monitoring Risk



Panel C: Net Impact of Failure Identification Risk



** Low impact range includes net effects scores from 1 – 9
Moderate impact range includes net effects scores from 10 – 19
High impact range includes net effects scores greater than (or equal to) 20.

Specific Strategic Alliance Risks

As firms strive to increase stakeholder value, they set goals and objectives and develop strategies that will enable them to achieve those objectives. COSO ERM suggests classifying the objectives into four distinct categories – (1) strategic, (2) operations, (3) reporting, and (4) compliance. By distinguishing these objectives from one another, firms can focus directly on the specific risks that may prevent the company from achieving its objectives in each of the areas. Further, this classification facilitates the development of effective internal control mechanisms that will lead to success in each category.

We have used the classification of objectives suggested by COSO ERM to categorize the risks most commonly occurring in strategic alliance relationships. These risks, and their COSO ERM classifications, are defined in Exhibit 8, below.[8]

[8] Risk definitions are consistent with those used by DeLoach (2000).

Exhibit 8
Risk Classification

Strategic – relating to high-level goals, aligned with and supporting the entity's mission	
Innovation risk	The risk that strategic partners will not maintain adequate levels of innovation to support the firm's needs.
Intellectual property risk	The risk that your strategic partner will make inappropriate use of proprietary information in a manner that could negatively affect the firm.
Product/ service failure risk	The risk that faulty or non-performing products or services from your strategic partners expose your company to sanctions from endcustomers.
Misalignment of incentives risk	The risk that strategic partners have incentives to take actions that would negatively affect the firm (e.g., relationships with your competitors, incentives for their employees to take action which are not in the best interest of the firm).
Partnering lock-in risk	The risk that the choice of a specific strategic partner locks the firm into a relationship with negative long-term consequences for the firm.
Outside scope risk	The risk that the alliance will create products or services outside the scope of the original agreement.
Operations – relating to effective and efficient use of the entity's resources	
Input supply risk	The risk that the strategic partner is unable or unwilling to supply key commodities, raw materials, or component parts in a timely manner to meet the firm's regular demand patterns.
Surge capacity risk	The risk that the strategic partner is unable or unwilling to supply key commodities, raw materials, or component parts in a timely manner to meet unusually high, unexpected demand.
Quality performance risk	The risk that the strategic partner is unable or unwilling to supply key commodities, raw materials, or component parts according to the quality and reliability standards of the firm.
Cost/price renegotiation risk	The risk that the strategic partner will take advantage of its position at a later date and seek unexpected increases in the price of key commodities, raw materials, or components.
Coordination risk	The risk that the firm and its strategic partner will fundamentally misunderstand one another's needs due to complexity or uncertainty associated with the task or difficulty of coordinating complex actions.
Financial viability risk	The risk that the strategic partner will experience financial distress that limits its ability to meet the firm's consumption needs.
Contribution valuation risk	The risk that the firm's non-monetary contribution to the partnership will be undervalued by the partner.
Financial commitment risk	The risk that entering into a strategic partnership may expose the firm to credit risk
Reporting – relating to the reliability of the entity's reporting	
Verification and evaluation risk	The risk that the firm will be unable to verify, monitor, or evaluate its strategic partner's performance in an accurate or timely manner.
Misalignment of incentives risk	See above.
Compliance – relating to the entity's compliance with applicable laws and regulations	
Compliance and regulatory risk	The risk that the strategic partner's failure (intentional or unintentional) to comply with customer requirements, firm policies, or government laws and regulations may expose the firm or its employees to sanctions.

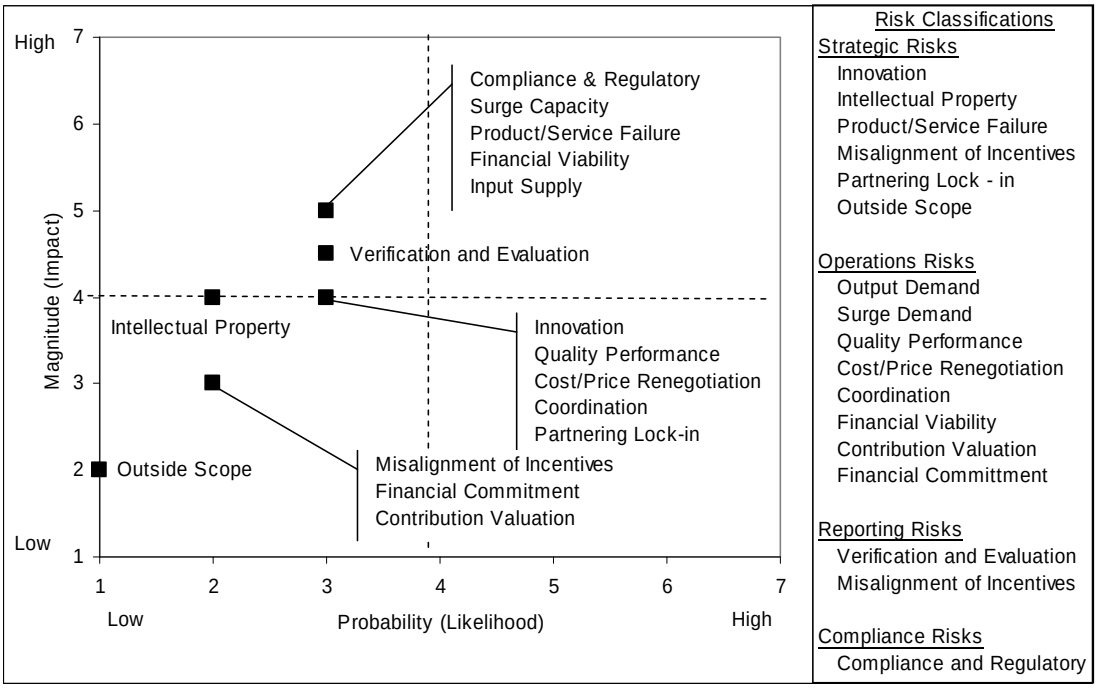
As described by COSO ERM, the risk assessment process provides an opportunity for firms to consider the events which might occur and which would prevent the firm from achieving its objectives. During the risk assessment process internal auditors typically consider the impact (or magnitude) of the potential events as well as the likelihood (or probability) of the occurrence of those events. Assessing the expected impact and likelihood of each risk allows management the ability to determine the appropriate level of resources to focus on mitigating those risks. For example, if the firm determines that the impact and likelihood that the alliance will create products that are outside the scope of the partnership (outside scope risk) are both low, then they will focus only minimal attention on that event. Instead, management will direct resources toward events with a high impact and likelihood of occurrence.

We asked CAE respondents to assess both the perceived impact and likelihood of each of the previously described risks for their critical partner. Further, we asked consultant respondents to assess the perceived impact and likelihood of each risk for the strategic partner type with which they are most familiar. The risk maps, shown below, illustrate the median responses for each partner type (see Exhibit 9, Panels A - D).[9]

As evidenced by Exhibit 9, the magnitude and likelihood of occurrence for each risk type varies by strategic alliance partner type. However, for each partner type, most risks fall into the upper left quadrant of the risk maps. While risks in this quadrant are not the most critical to the firm, they do warrant close attention.[10] These are the risks that may have a low likelihood of occurrence, but will have a significantly detrimental effect on the firm in the event of occurrence. It is imperative that management develop and maintain effective control mechanisms to minimize these risks, and that internal auditors routinely evaluate these risks and assess the applicable controls.

Exhibit 9
Inherent Risk Assessment by Partner Type

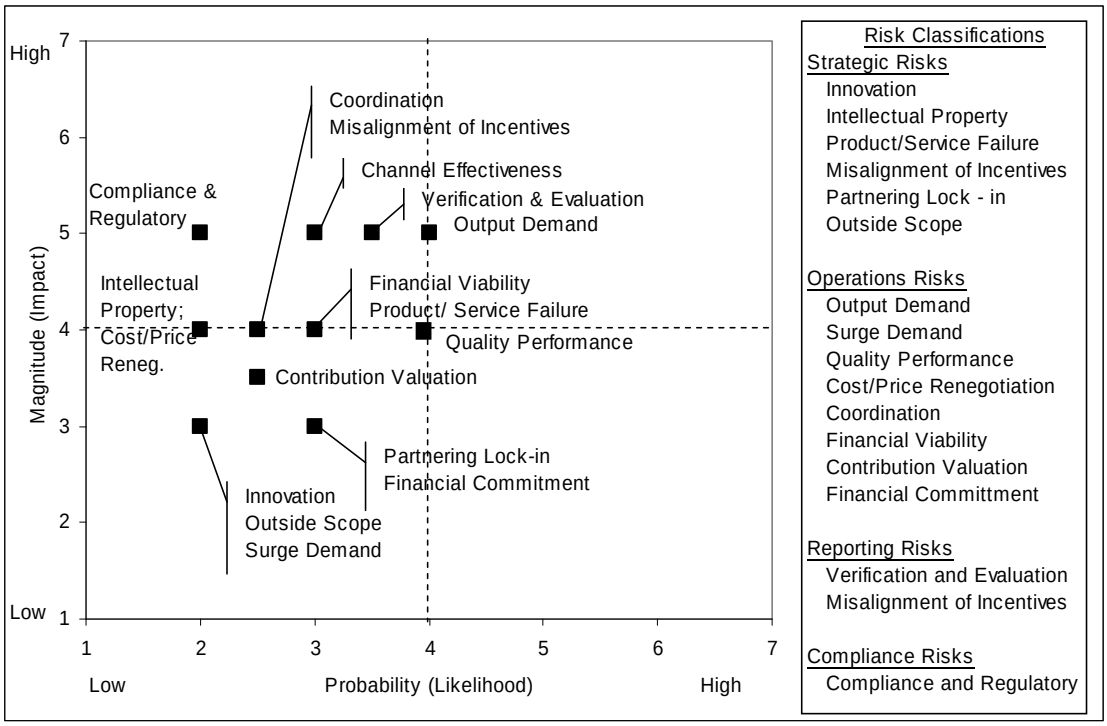
Panel A: Upstream Partnerships



[9] CAE and consultant responses have been combined for analysis of risks and control mechanisms.
[10] Risks determined to be in the upper right quadrant are considered to be the *most* critical. If uncontrolled, risks in the upper right quadrant would be devastating to the firm.

Exhibit 9, cont.

Panel B: Downstream Partnerships



Panel C: Marketing Partnerships

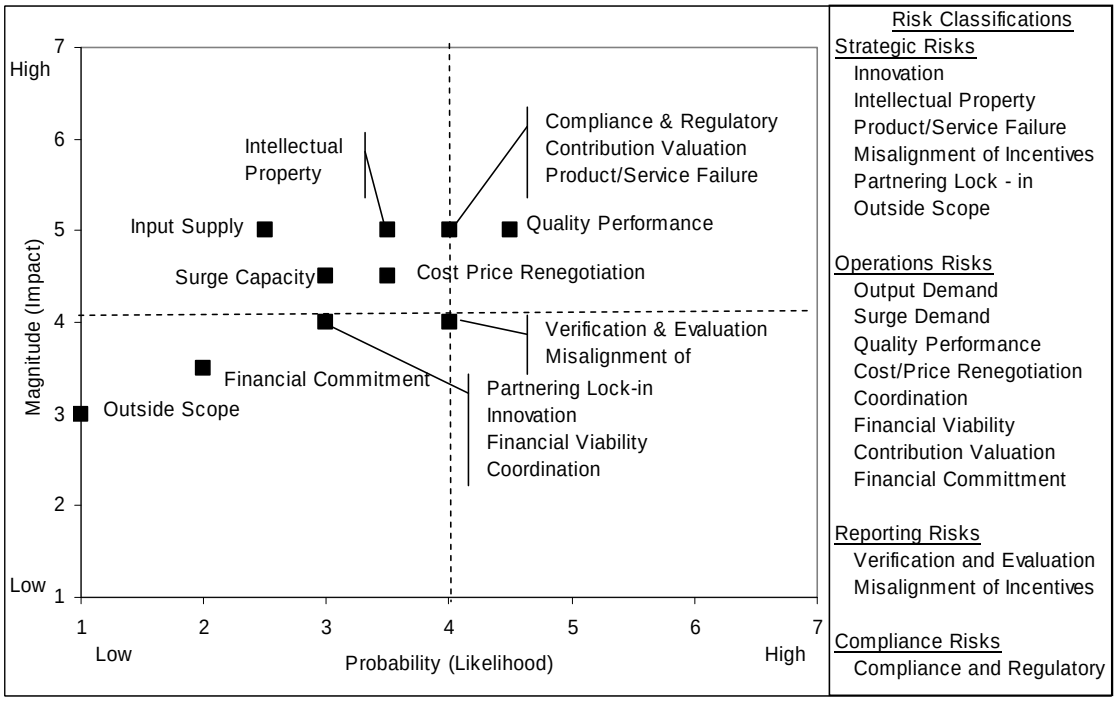
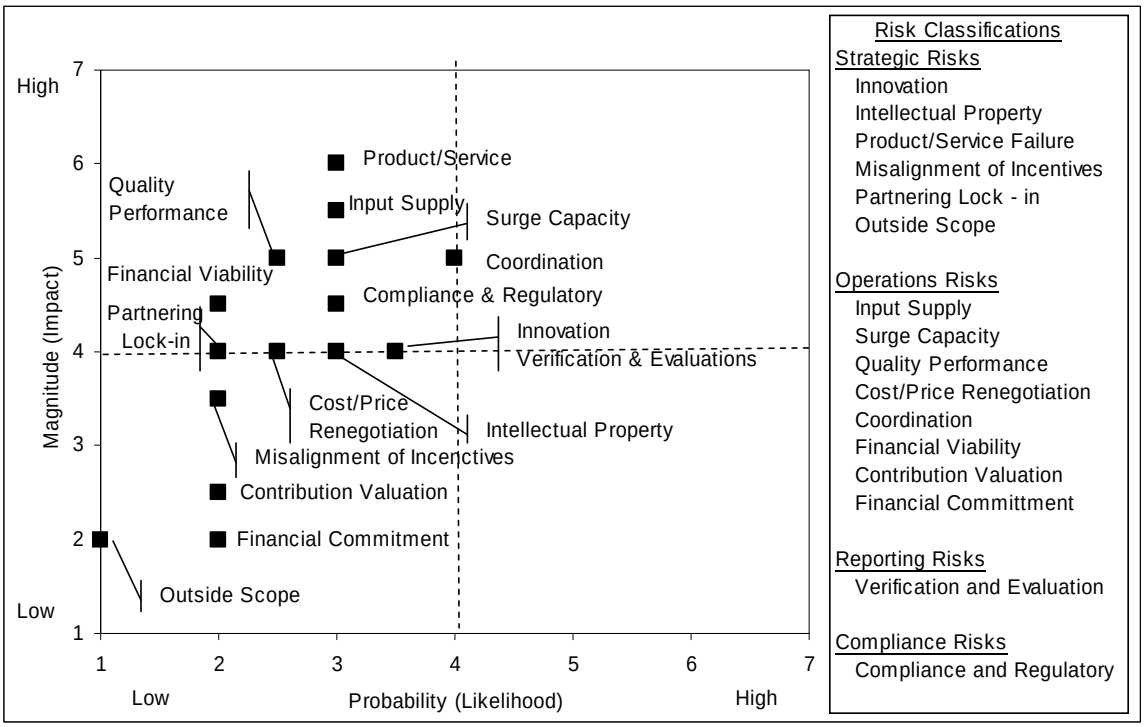


Exhibit 9, cont.

Panel D: Research and Development Partnerships



In general, CAE and consultant respondents assessed the likelihood of all risk to be less than or equal to the midpoint (somewhat probable).[11] While the risk assessments for each risk type vary, and are most clearly evident by reviewing Exhibit 9, several interesting results are worth mentioning here. For all (applicable) partner types, compliance and regulatory risks are assessed to be within the upper right quadrant of the risk maps, indicating that these risks are both highly probable and would have a large negative impact on the firm if they were to occur. This is consistent with the increased scrutiny that most firms are experiencing as a result of the Sarbanes-Oxley Act (see below for further discussion on the implications of the Act). Further, risks such as: (1) product/service failure, (2) input supply, (3) financial viability, and (4) quality performance, are also included in the upper right quadrant, indicating an elevated need for effective control mechanisms.

Outside scope risk, the risk of engaging in activities not included in the scope of the original partnership is consistently rated the most unlikely of all risks to occur, as evidenced by its median probability ranking of 1 for three of the partner types. Financial commitment risk is also assessed to have both a low probability of occurrence and low impact by all partner types.

[11] The sole exception is the risk of poor quality performance by a strategic marketing partner. CAEs and consultants with expertise in handling marketing alliances indicated that the likelihood of this was greater than moderate (4.5 on a scale from 1 – 7).

CONTROL ACTIVITIES USED TO MANAGE STRATEGIC ALLIANCE RISKS

Consistent with the Levers of Control framework, CAE and consultant respondents providing responses for each partner type indicate equal reliance on each of the four types of control systems: belief systems, boundary systems, diagnostic control systems, and interactive control systems. Median responses indicate that firms rely upon each lever of control to a moderate extent.[12] Therefore, firms seek a balance in their control practices to enhance the overall control environment. By utilizing all four levers, firms are able to reveal the core values of the business, empower strategic alliance partners to strive for goal achievement, and encourage long-term success.

Although the data suggest that firms rely equally on each of the four broad categories of the Levers of Control regardless of the partner type, further investigation suggests that the *specific* control mechanism used differs depending upon strategic partner type, as evidenced in Exhibit 10, below.

In general, firms place moderate reliance on written codes of conduct (see Panel A, Exhibit 10), regardless of the type of strategic alliance in which they are involved (although the reliance is somewhat lower for R&D alliances). Importantly, all firms indicate a relatively high reliance on trust between partners, as evidenced by a score of 4 on a 5-point Likert scale. This result is consistent with the widely held belief that effective strategic alliance management is dependent upon both control and trust (Das and Teng 2001).

Panel B of Exhibit 10 shows survey responses regarding reliance on boundary systems. All firms seem to rely significantly on various contract terms. Specifically, regardless of the partner type, respondents indicate greater than average reliance on contract terms detailing specific payment terms, delivery dates, etc. as evidenced by a score of 4 on a 5-point Likert scale. Firms with strategic marketing partners indicate greater reliance on contract terms to assign property right and to address the handling of failure to meet contract terms than do other firms.

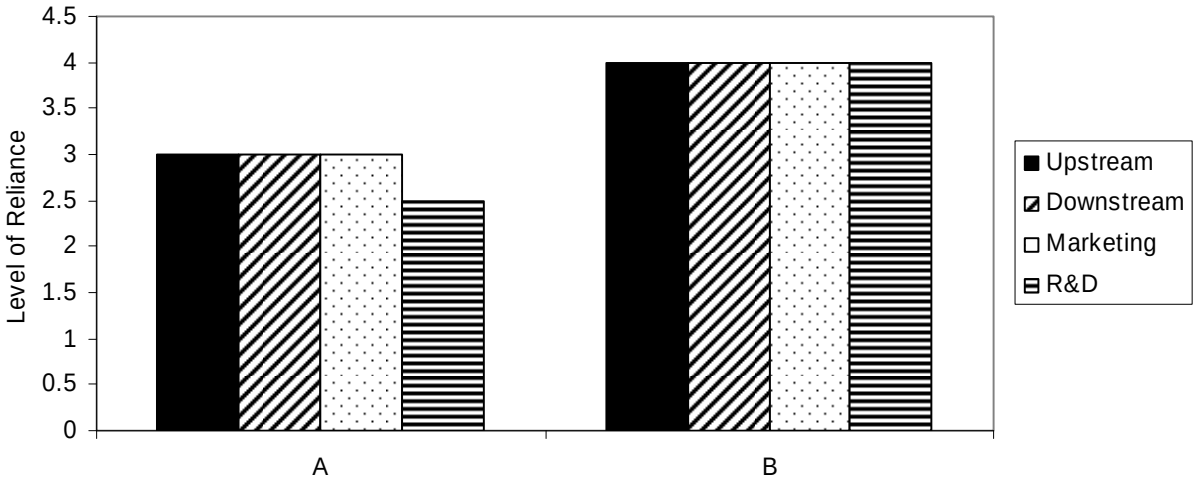
Panel C of Exhibit 10 illustrates survey responses regarding reliance on diagnostic control systems. Interestingly, firms with marketing partners indicate a greater reliance on SAS 70 reports than do other firms. Further, firms with upstream and downstream partners indicate that they place very little (if any) reliance on SAS 70 reports. Also noteworthy is the greater reliance on periodic unannounced audits by firms engaged in research and development partnerships than other firms, who indicate greater reliance on periodic *announced* audits. In addition, research and development partners indicated less reliance on formal review process for partner selection, contract terms specifying performance measurement, and contract terms for partnership dissolution than did other firms.

Finally, Panel D of Exhibit 10 illustrates survey responses regarding reliance on interactive control systems. Firms with marketing partnerships appear to be more likely to form formal profit-sharing entities (such as joint ventures) than do other firms. Further, firms with downstream partnerships indicate very little reliance upon formal profit-sharing entities. Instead, these firms indicate a greatest reliance upon accountability for partner selection. Finally, firms with upstream partnerships place little reliance upon the composition of the alliance management team.

[12] The median response for all partner types is 3 on a 5-point scale for each of the four partner types.

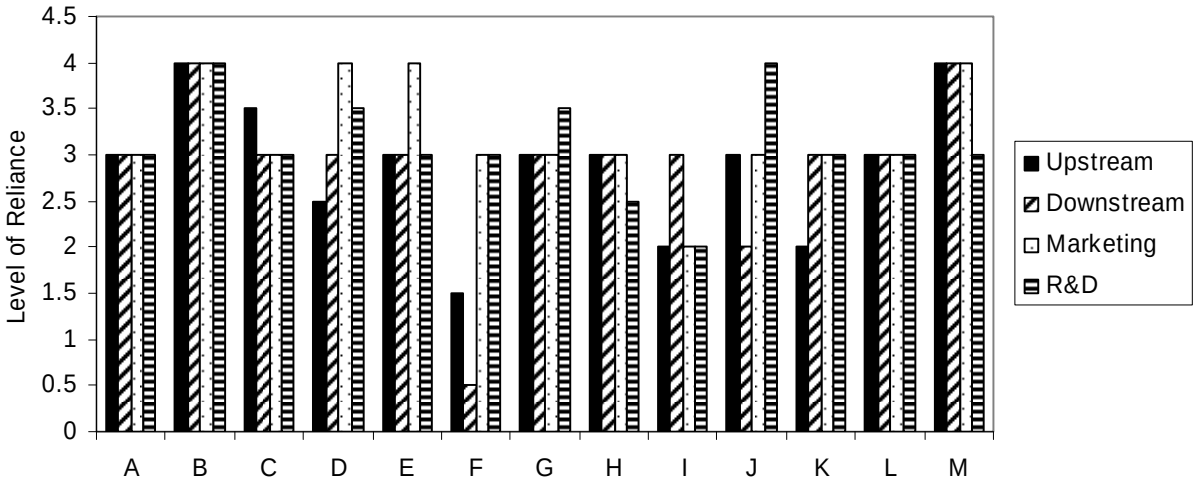
Exhibit 10
Level of Reliance on Simons' Levers of Control

Panel A: Belief Systems



A - Written and agreed-upon code of ethics/ code of conduct
B - High level of trust between alliance partners

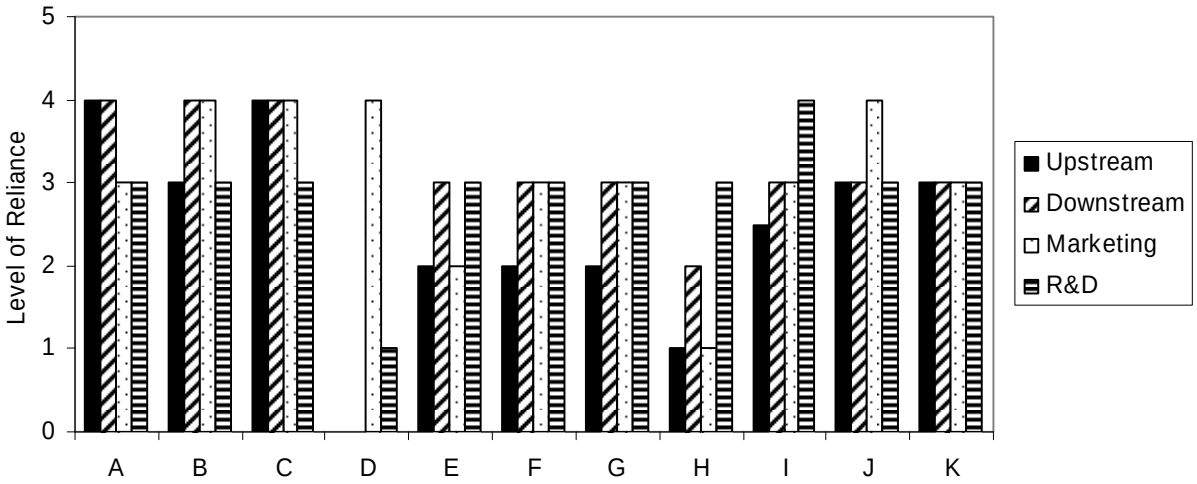
Panel B: Boundary Systems



A - Standard contract template
B - Contract terms detailing specific payment terms, delivery dates, etc.
C - Contract terms specifying cost sharing arrangements
D - Contract provisions to assign property rights
E - Contract terms regarding handling of failures to meet contract terms
F - Other contract terms
G - Written policies and procedures
H - Strategic identification of suppliers
I - Segregation of duties within the alliance
J - Authorization levels within the alliance
K - Physical safeguards of alliance assets
L - Physical safeguards of firm assets
M - Controls to protect proprietary information

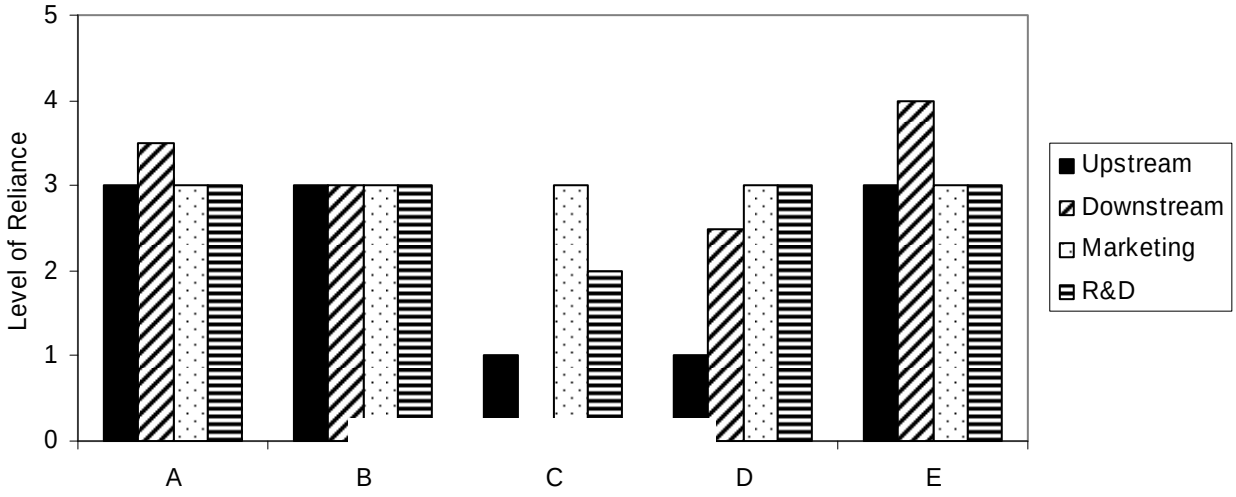
Exhibit 10, cont.

Panel C: Diagnostic Control Systems



A - Formal review process for supplier selection
B - Contract terms specifying how performance will be measured for fulfilling the contract
C - Contract terms for dissolution of partnership
D - Require partners to provide SAS 70 reports
E - Interactive feedback for continuous learning between partners
F - Interactive feedback within firm with respect to partner selection, alliance management, etc.
G - Periodic announced audits
H - Periodic unannounced audits
I - Periodic review of partner's financial information
J - Ongoing review of non-financial performance indicators
K - Ongoing review of financial performance measures

Panel D: Interactive Control Systems



A - Informal monitoring of partner's operations
B - Accountability of alliance personnel for alliance performance
C - Formation of formal profit-sharing entity
D - D – Composition of alliance management team
E - E – Accountability w/in firm for partner selection and alliance partners

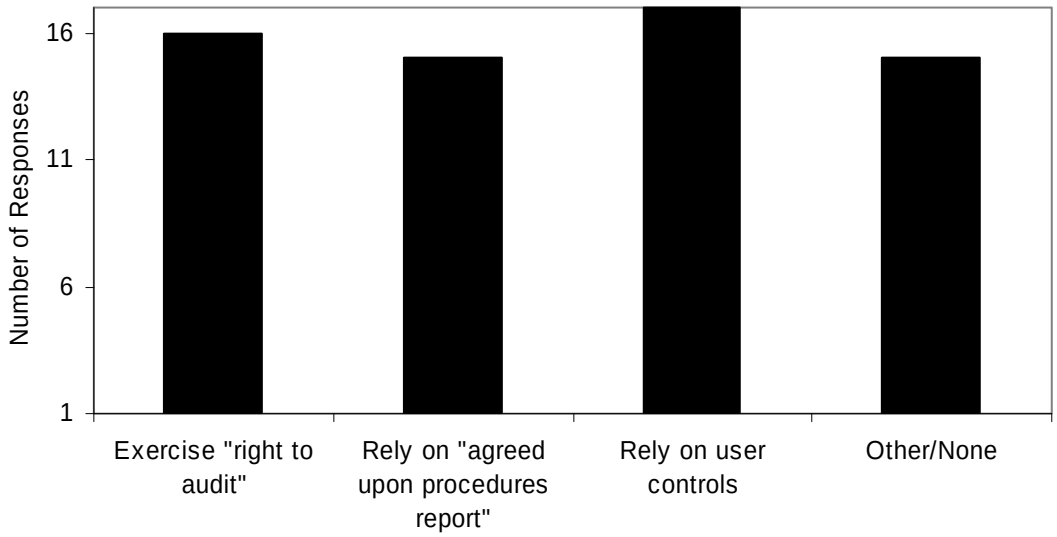
IMPLICATIONS OF THE SARBANES-OXLEY ACT

Firms with strategic alliance partnerships expose themselves to additional business risk as a result of the partnership. The Sarbanes-Oxley Act, which requires firms to perform an annual assessment of their internal controls systems, has led many companies to increase scrutiny of the internal control mechanisms of their strategic partners.

We asked CAE and consultant respondents with experience implementing Sarbanes-Oxley how their firms (or clients) have changed their control systems in response to the Sarbanes-Oxley requirements. Twenty-five (25) CAE respondents and 23 consultants responded to the Sarbanes-Oxley portion of the survey. Five of 25 CAEs (20%) work for companies that had filed statements of internal control weaknesses with the Securities and Exchange Commission (SEC) at the time of our survey.[13] Further, 3 of 23 consultants (13%) indicate that their clients filed statements with the SEC.

Approximately half of CAEs and 57% of consultants indicate that their firms (clients) have implemented new control systems over their strategic partners in response to Sarbanes-Oxley.[14] Further, participants were asked which of the following commonly used control mechanisms their firms intended to rely upon to ensure partners' Sarbanes-Oxley compliance: (1) exercise the right to audit clause from contract, (2) rely upon an "agreed-upon procedures" report, and/or (3) rely on partner controls. As Exhibit 11 illustrates, most firms rely on more than one of those specific control mechanisms. Further, both CAE and consultant respondents indicate that approximately 67% of firms intend to exercise their right-to-audit clause included in the original contract terms of the partnership.

Exhibit 11
Control Mechanisms Used to Ensure Partners' Sarbanes-Oxley Compliance

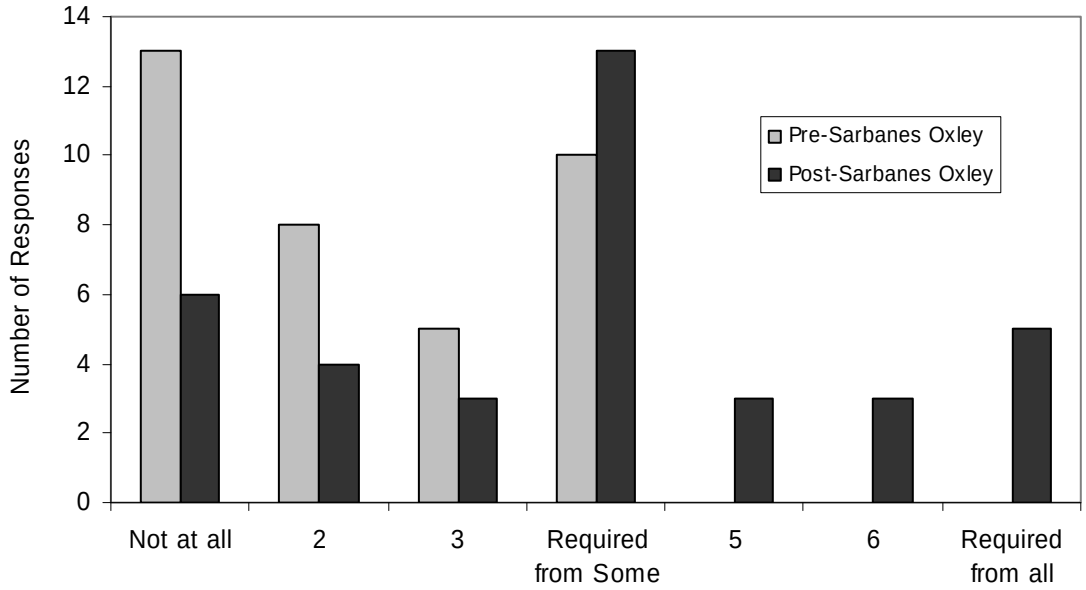


[13] Only one of the five CAEs who indicated that their firm had filed statements of internal control weaknesses with the SEC indicated that the internal control weakness was partially attributable to their strategic partnerships. This CAE indicated that its partner was minimally responsible (rating of 2 on a 7-point Likert scale with 1 indicating not at all attributable and 7 indicating completely responsible).

[14] 11/24 CAEs indicated that new controls had been implemented, two indicated that they "did not know" whether new controls had been implemented.

We also asked respondents to describe the extent to which their firms' strategic partners are requiring *them* to amend their existing internal control structure (untabulated). Approximately 29% (12/42) indicate that no internal control changes are required of their firms by their strategic partners. However, 40% (17/42) indicate that their partners (clients' partners) are requiring changes to varying degrees.[15]

Exhibit 12
Use of SAS 70 Reports Pre- and Post-Sarbanes-Oxley



Finally, we asked CAE and consultant respondents to indicate the level of reliance their firm and their partner firms were placing on SAS 70 reports to ensure adequate internal control mechanisms were in place. Exhibit 12, above, indicates that the number of firms that placed little or no reliance on SAS 70 reports has diminished as a result of Sarbanes-Oxley. Further, the number of firms that place moderate to high reliance on SAS 70 reports has increased in the post-SOX era and several respondents (approximately 14%) indicated that their firms or clients now require SAS 70 reports from all strategic partners.

CONCLUSION

While strategic alliances offer firms opportunities for growth and innovation, they also present unique challenges to these firms. These alliances are inherently risky, as evidenced by the high incidence of alliance failure. Therefore, firms that utilize strategic alliances need to develop and maintain new management control practices that effectively mitigate the risk of transacting with self-interested parties.

We collected survey responses from CAE and internal audit consultant members of The Institute of Internal Auditors to identify, categorize, and quantify the risks that firms face when entering into strategic alliances. Further, we examined the control practices used by firms to mitigate these risks.

When considering the management of their strategic alliance network as a whole, respondents indicated that (1) selection risk, (2) monitoring risk, and (3) failure identification risk each have a moderate to high impact on the operations of the firm, suggesting that the magnitude and likelihood of each is greater than average. Further, when assessing specific risks (as they apply to a critical partner or specific partner

[15] Four CAE and three consultant respondents indicated that they did not know of any internal control changes required by partners.

type), survey respondents indicated that the manifestation of most risks would have a significant impact on firm operations, although the likelihood of the manifestation was low. However, these assessments indicate that careful consideration and evaluation of these risks is necessary.

Using the Levers of Control framework, we categorized and examined the control practices firms use to mitigate the risks raised by strategic partners. Consistent with the framework, firms appear to use control mechanisms from each control lever equally. This indicates that firms use a variety of complementary control mechanisms to minimize strategic partner risks. The data also suggest that firms rely on high levels of trust between partners to preserve the alliance and minimize the fear of opportunistic behavior. Further, respondents indicate a reliance on contract terms to manage the partnership.

As strategic alliances continue to be a dominating force in the business community, their effective management and control is critical. Internal auditors are in a unique position, as risk and control experts, to evaluate strategic alliances before their formation, throughout their lifecycle, and through their dissolution. Risk frameworks, such as COSO ERM, can aid internal auditors in these assessments. Effective risk management during all stages of the strategic partnership can increase the likelihood of alliance success and propel the organization toward the achievement of its strategic goals.

REFERENCES

____. 2000. Alliance management: Five destructive myths. *CMA Management*, Vol. 73: 14-15.

Anand, B. N. and T. Khanna. 2000. Do firms learn to create value? The case of alliances. *Strategic Management Journal* 21 (3): 295-315.

Anderson, S. W., K. L. Sedatole, and D. Glenn. 2000. Sourcing parts of complex products: Evidence on transactions costs, high-powered incentives and ex-post opportunism. *Accounting, Organizations and Society* 25 (8): 723-750.

Anderson, S. W. and K. L. Sedatole. 2003. Management accounting for the extended enterprise: Performance management for strategic alliances and networked partners. In A. Bhimani (Ed.), *Management accounting in the digital economy*: 36-73. London: Oxford Press.

Anderson, S. W. and H. C. Dekker. 2005. Management control for market transactions: The relation between transaction characteristics, incomplete contract design, and subsequent performance. *Management Science* 51 (12): 1734-1752.

Anderson, S. W., M. H. Christ, and K. L. Sedatole. 2006. Field and survey evidence on the state of management control for risks associated with strategic alliances. Working Paper.

Baum, J. A. C., T. Calabrese, and B. S. Silverman. 2000. Don't go it alone: Alliance network composition and startups performance in canadian biotechnology. *Strategic Management Journal* 21 (3): 267-294.

Buehler, K. S. and G. Pritsch. 2003. Running with risk. *McKinsey Quarterly* (4): 40-49.

Buvik, A. and T. Reve. 2001. Asymmetrical deployment of specific assets and contractual safeguarding in industrial purchasing relationships. *Journal of Business Research* 51 (2): 101-113.

Christ, M. H., K. L. Sedatole, and K. L. Towry. 2005. All control is not equal: The effect of control system type on trust and cooperation in strategic alliances. Working paper.

Coletti, A., K. Sedatole, and K. Towry. 2005. The effect of control systems on trust and cooperation in collaborative environments. *The Accounting Review* 80 (2): 477-500.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise risk management – integrated framework*.

Das, T. K. and B. Teng. 1996. Risk types and inter-firm alliance structures. *Journal of Management Studies* 33 (6): 827-843.

Das, T. K. and B. Teng. 1998. Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review* 23 (3): 491-512.

Das, T. K. and B. Teng. 2000. Instabilities of strategic alliances: An internal tensions perspective. *Organization Science: A Journal of the Institute of Management Sciences* 11 (1): 77-101.

Das, T. K. and B. Teng. 2001. Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies* 22 (2): 251-283.

Dekker, H. C. 2003. Control of information technology transactions: An empirical test of appropriation concerns, coordinations requirements and social embeddedness. *Accounting, Organizations & Society* (forthcoming).

Deloach, J. W. 2000. *Enterprise-wide risk management: Strategies for linking risk and opportunity*. New York: Financial Times Management.

Ernst, D. 2002. Give alliances their due. *McKinsey Quarterly*: 4.

Granovetter, M. S. 1973. The strength of weak ties. *American Journal of Sociology* 78 (6): 1360-1380.

Gulati, R. 1995. Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal* 38 (1): 85-113.

Gulati, R. and H. Singh. 1998. The architecture of cooperation: Managing coordination costs and appropriation concerns in strategic alliances. *Administrative Science Quarterly* 43 (4).

Kinney, W. R. 2000. *Information quality assurance and internal control for management decision making*. Boston: Irwin McGraw-Hill.

Lewis, J. D. 1999. *Trusted partners: How companies build mutual trust and win together*. New York: The Free Press.

Lorenzoni, G. and A. Lipparini. 1999. The leveraging of interfirm relationships as a distinctive organizational capability: A longitudinal study. *Strategic Management Journal* 20 (4): 317-338.

McNamee, D. 2000. Targeting business risk. *Internal Auditor* 57 (5): 46-50.

Menard, C. 1995. Markets as institutions versus organizations as markets? Disentangling some fundamental concepts. *Journal of Economic Behavior & Organization* 28 (2): 161-182.

Menard, C. 1996. On clusters, hybrids, and other strange forms: The case of the french poultry industry. *Journal of Institutional and Theoretical Economics* 152 (1): 154-183.

Osborn, R. N. and C. C. Baughn. 1990. Forms of interorganizational governance for multinational alliances. *Academy of Management Journal* 33: 503-519.

Pisano, G. P., M. V. Russo, and D. Teece. 1988. Joint ventures and collaborative agreements in the telecommunications equipment industry, *Book section*: 23-70. Cambridge, MA: Ballanger.

Pisano, G. P. 1989. Using equity participation to support exchange: Evidence from the biotechnology industry. *Journal of Law, Economics, and Organization* 5 (1): 109-126.

Pisano, G. P. 1990. The R&D boundaries of the firm: An empirical analysis. *Administrative Science Quarterly* 35 (1): 153-176.

Public Company Accounting Oversight Board (PCAOB). 2004. *Auditing standard no. 2: An audit of internal control over financial reporting performed in conjunction with an audit of financial statements*.

Ring, P. S. and A. H. Van De Ven. 1992. Structuring cooperative relationships between organizations. *Strategic Management Journal* 13 (7): 483-498.

Ring, P. S. and A. H. Van De Ven. 1994. Developmental processes of cooperative interorganizational relationships. *Academy of Management Journal* 19 (1): 90-118.

Simons, R. 1995. *Levers of control: How managers use innovative control systems to drive strategic renewal*. Boston, MA: Harvard Business School Press.

Stuart, T. E. 2000. Interorganizational alliances and the performance of firms: A study of growth and innovation rates in high-technology industry. *Strategic Management Journal* 21 (8): 791-811.

Williamson, O. E. 1985. *The economic institutions of capitalism*. New York: The Free Press.

Williamson, O. E. 1991. Comparative economic organization: The analysis of discrete structural alternatives. *Administrative Science Quarterly* 36 (2): 269-297.

Wolff, J. A. and R. Reed. 2000. Firm resources and joint ventures: What determines zero-sum versus positive-sum outcomes? *Managerial and Decision Economics* 21 (7): 269-284.

Zaheer, A. and N. Venkatraman. 1995. Relational governance as an interorganizational strategy: An empirical test of the role of trust in economic exchange. *Strategic Management Journal* 16 (5): 373-392.

Zaheer, A., B. Mcevily, and V. Perrone. 1998. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science: A Journal of the Institute of Management Sciences* 9 (2): 123-142.

UNDERSTAND, SHAPE, ADVANCE

The IIA Research Foundation is a 501(c)(3) corporation formed to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.

Through its research reports, Bookstore products, and GAIN Knowledge Services, The Foundation provides resources that help understand, shape, and advance the global profession of internal auditing by initiating and sponsoring intelligence gathering, innovative research, and knowledge-sharing in a timely manner.

To learn more, visit www.theiia.org/research

ISBN 978-0-89413-649-8
Item #2007.dl
Free to IIA Members
Non-members: US$15