UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

MESTRADO EM: GESTÃO DE SISTEMA DE INFORMAÇÃO

CONFORMIDADE COM A S404 DA LEI *SARBANES OXLEY* NO CONTEXTO NACIONAL

DAVID ELISIÁRIO DE MATOS CARDOSO OLIVEIRA

Orientação: Professor Doutor Pedro Teixeira Isaías

Júri:

Presidente: Professor Doutor Mário Fernando Maciel Caldeira

Vogais: Professor Doutor José António Ferreira Porfírio

Professor Doutor Pedro Teixeira Isaías

Professora Doutora Maria Fernanda Abreu Sampaio

NOVEMBRO / 2008

UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

MESTRADO EM: GESTÃO DE SISTEMA DE INFORMAÇÃO

CONFORMIDADE COM A S404 DA LEI *SARBANES OXLEY* NO CONTEXTO NACIONAL

DAVID ELISIÁRIO DE MATOS CARDOSO OLIVEIRA

Orientação: Professor Doutor Pedro Teixeira Isaías

Júri:

Presidente: Professor Doutor Mário Fernando Maciel Caldeira

Vogais: Professor Doutor José António Ferreira Porfírio

Professor Doutor Pedro Teixeira Isaías

Professora Doutora Maria Fernanda Abreu Sampaio

NOVEMBRO / 2008

[Esta página foi intencionalmente deixada em branco]

CONFORMIDADE COM A S404 DA LEI *SARBANES OXLEY* NO CONTEXTO NACIONAL

David Elisiário de Matos Cardoso Oliveira

Mestrado em: Gestão de Sistemas de Informação

Orientador: Professor Doutor Pedro Isaías

Resumo

A presente dissertação de mestrado expõe uma revisão bibliográfica sobre os antecedentes e os principais fundamentos da Lei *Sarbanes Oxley* (SOX), culminando com a apresentação de um caso de estudo sobre a conformidade com a secção com maior impacto nas organizações sujeitas a este normativo, a s404.

São analisados os factos que conduziram à falência – e incentivaram a criação da Lei SOX – de duas das mais conceituadas empresas Norte Americanas, nomeadamente a adopção de práticas fraudulentas pela Gestão de Topo, e da eventual conivência entre estes e os auditores externos responsáveis pela certificação do reporte financeiro.

As principais secções da lei são apresentadas quanto ao seu teor e impacto nas empresas, com especial enfoque na necessidade destas ajustarem o seu *modus operandis* de forma a responderem às novas exigências impostas pela lei.

O caso de estudo, descreve a forma como uma empresa Multinacional sedeada em Portugal respondeu às exigências da s404 e em que medida converteu essa obrigação em valor acrescentado para a empresa e seus colaboradores, através da adopção de uma estratégia efectiva de gestão de risco.

A conclusão expõe os principais aspectos do modelo de conformidade com a s404 da Lei SOX adoptado pela empresa em estudo, nomeadamente os relacionados com a gestão de projecto, metodologia seguida, *General IT Controls e transição para Business as Usual*

Palavras-chave: *Sarbanes-Oxley*, Reporte Financeiro, Gestão de Risco, *General IT Controls*, Controlo Interno, *Business as Usual.*

COMPLIANCE WITH THE S404 OF THE *SARBANES OXLEY* ACT IN THE PORTUGUESE CONTEXT

David Elisiário de Matos Cardoso Oliveira

Master's degree in: Information systems Management

Orientation: Pedro Isaías (PhD)

Abstract

The present master's degree exposes a bibliographical revision about the record and the main provisions of the *Sarbanes Oxley* Law (SOX), culminating with the presentation of a case study about the conformity with the section with bigger impact in the companies which are subject to this law, the s404.

The facts that drove to bankruptcy – and encouraged the creation of the SOX Law – of two of the most respected American North companies are analysed, namely the adoption of fraudulent practices by the Top Management, and of the eventual connivance between these and the external auditors responsible for the attestation of the financial report.

The main sections of the law are presented in what regards its content and impact in the companies, with a particular concern about how the companies need to adjust their way of work to the new requirements imposed by the law.

The case study, describes how a Multinational company with an office in Portugal answered the requisites of the s404 and how it transformed the obligation to be compliant in an increased value for the company and its staff, through the adoption of an effective strategy of risk management.

The conclusion exposes the main aspects of the model of conformity with the s404 of the SOX Law adopted by the company in study, namely the related with project management, chosen methodology, General IT Controls and transition to Business the Usual

Key-words: Sarbanes-Oxley, Financial Reporting, Risk Management, General IT Controls, Internal Control, Business as Usual.

ÍNDICE

Lista de Figuras

Lista de Tabelas

Acrónimos

AS Nº2 – Auditing Standard Nº2

AS Nº5 – Auditing Standard Nº5

BAU – Business as Usual

CAO – Chief Accounting Officer

CEO – Chief Executive Officer

CFO – Chief Financial Officer

CIO – Chief Information Officer

CObIT – Control Objectives for Information Tecnology

COSO – Committee of Sponsoring Organizations of the Tradeway Commission

CPA – Certified Public Accounts

GAAP – Generally Accepted Accounting Principles

GAAS – Generally Accepted Auditing Standards

GITC – General IT Controls

KPI's – Key Performance Indicators

PCAOB – Public Company Accounting Oversight Board

s404 – Secção 404 da Lei Sarbanes Oxley

SEC – Securities and Exchange Commission

SLA – Service Level Agreements

SOX – Lei Sarbanes Oxley

SRO – Self-regulated organizations

TelCos – Empresas de Telecomunicações

Agradecimentos

Gostaria de deixar uma mensagem de agradecimento às seguintes pessoas:

Em primeiro lugar à minha mulher, Rute, meu “porto seguro” há vários anos, por ter escutado os meus desabafos, ideias, dificuldades e que esteve sempre ao meu lado dando-me o apoio e a força que necessitava.

À minha filhota, Catarina, que no final do trabalho, me deu a motivação extra para concluir a dissertação.

Aos meus pais, Francisco Oliveira e Maria Hermínia Oliveira que me trouxeram a este mundo, que fizeram de mim a pessoa que sou hoje e que sempre me incentivaram a atingir patamares mais elevados na minha vida académica e profissional.

Aos meus colegas de equipa pelas ideias e sugestões que partilharam comigo no decorrer da presente dissertação.

Finalmente, ao meu orientador Prof. Doutor Pedro Isaías pelo apoio e disponibilidade que demonstrou para comigo no decorrer do presente trabalho.

1 Introdução

Enron, Arthur Andersen, WorldCom, Tyco e Adelphia. Estas organizações, já de si bastante conhecidas, ganharam uma maior notoriedade por força de um passado recente fraudulento, ganancioso e de práticas contabilísticas impróprias. Embora as más práticas deste pequeno grupo de empresas não seja representativa da maioria das 15.000 cotadas em bolsa nos EUA, o resultado das suas acções tiveram uma repercussão significativa nos mercados. Quando os detalhes sobre a corrupção emergiram e os preços das acções e poupanças de reforma caíram abruptamente, a população americana ficou estupefacta e exigiu uma reforma. Em 30 de Julho de 2002 o congresso respondeu a estes factos com a criação da Lei *Sarbanes Oxley* de 2002 (também conhecida como o "Acto"). O "Acto" foi assinado com o objectivo de melhorar a transparência e a exactidão dos relatórios financeiros e das divulgações financeiras das organizações, bem como para reforçar a importância dos padrões éticos destas. Como resultado, a *Securities and Exchange Commission* (SEC) emitiu regras para definir os requisitos do Acto. Muitos consideram que as exigências de Controlo Interno sobre o reporte financeiro do Acto (Secção 404) e o facto da Gestão de Topo ser obrigada a certificar as Demonstrações Financeiras (Secção 302) como dolorosas, de elevado custo de implementação e com pouco valor acrescentado. Outros vêem estes requisitos como uma oportunidade de implementar as melhores práticas de negócio, melhorar o desempenho das organizações e potenciar a confiança dos investidores (Marchetti, 2004).

Conforme defende Roth (2007), a abrangência global da Lei *Sarbanes Oxley* faz com que as organizações procurem novas formas de responder aos seus apertados requisitos ou cumulativamente ao de qualquer outra lei que tenha surgido entretanto. Existe, contudo, uma preocupação crescente em fazê-lo de uma forma eficiente e eficaz, proporcionando benefícios às organizações, permitindo-lhes recuperar os recursos investidos nestas matérias. Por estes motivos muitas empresas consideram expandir a certificação com a Lei *Sarbanes Oxley* para uma estratégia efectiva de Gestão de Risco. Esta evolução é aparentemente natural; a Lei *Sarbanes Oxley* endereça os riscos e controlos sobre o reporte financeiro e a Gestão de Risco endereça de forma lata todos os riscos e controlos da organização.

Com a criação da Lei *Sarbanes Oxley* as empresas cotadas em bolsa nos EUA depararam-se, subitamente, com desafios novos, diferentes e mais exigentes. Embora não exista uma definição de "melhor estratégia" para atingir a conformidade com a Lei – nomeadamente a Secção 404 – existe um conjunto de boas práticas no mercado, sugeridas por vários autores, que as empresas têm adoptado de forma crescente.

A presente dissertação de mestrado procura evidenciar, através de uma revisão bibliográfica, os pontos fundamentais – e com maior impacto nas organizações – da Lei *Sarbanes Oxley*, bem como propor um modelo de conformidade com da Secção 404.

1.1 Objectivos

Os objectivos da presente dissertação são os seguintes:

- Analisar os factos que conduziram á criação da Lei *Sarbanes Oxley*;
- Apresentar as principais secções da Lei *Sarbanes Oxley*;
- Definir um modelo de gestão para atingir a conformidade com a s404 da Lei *Sarbanes Oxley*;
- Propor uma *framework* de controlo para gerir o risco associado aos sistemas de informação;
- Sugerir um modelo de governo para a sustentabilidade da certificação.

1.2 Motivação para o estudo do tema

A motivação para a dissertação do tema prende-se com o facto da actividade profissional do autor ter evoluído associada a matérias relacionadas com Auditoria e Gestão de Risco. É igualmente considerado um desafio ter a possibilidade de evidenciar, de que forma as crescentes necessidades legais das organizações se cruzam com as melhores práticas existentes no mercado nestas matérias.

No actual contexto das organizações existe uma competitividade cada vez mais acentuada. As empresas procuram sistematicamente formas e factores que as diferenciem da concorrência, de forma a assumirem uma posição dominante. A necessidade de ter de responder aos requisitos da Lei *Sarbanes Oxley* – em particular da secção 404 – não é, por si só, um factor de destaque. Contudo os seus fundamentos e objectivos vão ao encontro das motivações acima mencionadas, na medida em que abrangem um leque alargado de questões relacionadas com controlo interno e uma gestão efectiva dos riscos das organizações.

Poder partilhar com o mundo académico, a forma como a organização em estudo respondeu aos requisitos apertados da Lei *Sarbanes Oxley*, adoptando uma estratégia de efectiva de Gestão de Risco é, sem dúvida, um desafio extremamente motivante, nomeadamente por ter a possibilidade de evidenciar como as melhores práticas existentes auxiliaram e potenciaram a implementação de requisitos tão apertados como os relacionados com a s404.

1.3 Metodologia

A metodologia seguida neste estudo está alinhada com os objectivos propostos para a dissertação:

- Realização de uma revisão bibliográfica sobre o estado do conhecimento sobre a Lei *Sarbanes Oxley*;
- Análise e apresentação de um caso de estudo sobre a conformidade com a s404 da Lei *Sarbanes Oxley* numa empresa Multinacional sedeada em Portugal.

A investigação não teve como objectivo aprofundar os fundamentos legais da Lei ou os aspectos técnicos de implementação. A principal motivação foi abarcar os principais temas e impactos que a lei trouxe para o panorama internacional, procurando dar uma visão global sobre o tema. Para o efeito foram utilizadas obras de referência que englobavam os aspectos obrigatórios impostos pela Lei e que incidiam, igualmente, sobre ângulos práticos de estabelecimento da conformidade

desta em diversos contextos. Foram, também, utilizadas bases de dados *online* como a *Proquest, b-on e EBSCO* para seleccionar artigos cujas temáticas se focassem essencialmente sobre: *Sarbanes Oxley*, s404, Secção 302, *Audit Committee*, *Auditor Independence, Whistleblowers, Securities and Exchange Commission (SEC) e Public Company Accounting Oversight Board (PCAOB).*

Para o caso de estudo apresentado foi recolhida diversa informação da empresa em estudo e entrevistados alguns dos principais intervenientes. Ainda que as pessoas em causa e determinados documentos analisados não possam ser identificados/citados de forma explícita – por motivos relacionados com confidencialidade – considerou-se toda a informação relacionada com o planeamento do projecto de implementação da s404, estrutura de risco e *framework* de controlos da empresa. Adicionalmente, incluiu-se nessa pesquisa a informação relacionada com os métodos utilizados para promover a sustentabilidade da conformidade com a Lei *Sarbanes Oxley* e a forma como esta se integra na empresa.

No sentido de evidenciar de forma mais clara os métodos de pesquisa utilizados, o autor da dissertação apresenta, em seguida, o método utilizado para desenvolver cada um dos objectivos propostos:

- **Analisar os factos que conduziram à criação da Lei Sarbanes Oxley:**

  Este objectivo foi atingindo na sua plenitude através da revisão bibliográfica realizada, nomeadamente através da colecção de factos incorporados em obras de referência e/ou artigos publicados em revistas conceituadas.

- **Apresentar as principais secções da Lei Sarbanes Oxley:**

  Em linha com o primeiro objectivo, também o segundo foi alcançado totalmente através da revisão da bibliografia realizada. Dado que o caso de estudo incide sobre uma componente específica, a conformidade com a s404, houve uma preocupação especial do autor em aprofundar as matérias relacionadas com esta secção, nomeadamente ao incorporar normativos recentemente aprovados, i.e., AS5.

- **Definir um modelo de gestão para atingir a conformidade com a s404 da Lei Sarbanes Oxley**

  A apresentação do caso de estudo foi fundamental para responder a este objectivo. Foram recolhidos testemunhos e realizadas entrevistas às pessoas chave na organização, no sentido de obter informação não residente em documentação. Os documentos de suporte ao projecto (e.x.: organigramas e planos de projecto) foram igualmente importantes, na medida em que potenciaram a identificação das pessoas chave, estruturação das entrevistas e, finalmente, a consolidação do conteúdo no capítulo 3 da presente dissertação.

- **Propor uma framework de controlo para gerir os riscos associados aos sistemas de informação**

  O propósito do presente objectivo é apresentar aquela que foi a *baseline* dos *General IT Controls* utilizados pela organização em estudo para responder aos requisitos da s404. Para o efeito foi recolhida toda a documentação relacionada com a estrutura de processos, controlos e riscos (nesta estão incluídos os documentos relacionados com as auditorias)

- **Sugerir um modelo de governo para a sustentabilidade da certificação**

  Em linha com o método utilizado para o terceiro objectivo, também para este foram utilizadas diferentes técnicas. O recurso a entrevistas e a documentação da organização foi essencial, pois permitiu entender os fundamentos e as motivações que levam uma organização desta dimensão a adoptar este tipo de estratégia.

1.4 Estrutura da dissertação

A dissertação de mestrado é composta por quatro capítulos.

No primeiro capítulo é apresentado o tema da dissertação, os objectivos propostos, a motivação para o estudo do tema e a metodologia seguida.

O segundo expõe, através de uma revisão bibliográfica, os factores que levaram à criação da Lei *Sarbanes Oxley*, descrevendo igualmente as secções mais relevantes e com maior impacto nas empresas sujeitas a este normativo.

O terceiro capítulo apresenta um caso de estudo sobre a implementação da s404 – a secção da Lei com maior impacto nas empresas – analisando a forma como uma empresa Multinacional sedeada em Portugal respondeu aos requisitos impostos.

No quarto capitulo são apresentadas as principais conclusões da dissertação, limitações impostas e que trabalhos futuros podem ser desenvolvidos tendo por base o presente trabalho.

2 Revisão de Bibliografia

2.1 Antecedentes da Lei Sarbanes Oxley de 2002

No início do milénio, os EUA assistiram a alguns dos maiores escândalos corporativos e financeiros da sua história. Práticas empresariais corruptas, movimentos contabilísticos fraudulentos e jogos de poder/influência foram repentinamente descobertos, trazidos para público e os responsáveis identificados.

Conforme é do domínio público os acontecimentos, relatados de forma sumária em baixo, envolveram algumas das maiores organizações empresarias dos EUA (e.g.: *Enron, WorldCom*) e provavelmente a maior empresa de Auditoria a nível mundial na altura (desapareceu do mercado como consequência): a *Arthur Andersen*.

2.2 ENRON

2.2.1 Caracterização da Empresa

Em 31 de Dezembro de 2000 o valor unitário das acções da *Enron* ascendia a $83.12 e tinha uma capitalização bolsista que ultrapassava os $60 biliões, 70 vezes os lucros e 6 vezes o valor contabilístico, indicando claramente altas expectativas de projecçãofutura. Num estudo levado a cabo pela revista *Fortune*, sobre as empresas mais admiradas, a *Enron* foi classificada como a empresa mais inovadora dos EUA (Healy et al, 2003).

Antes de apresentar o pedido de falência no final de 2001 a *Enron* tinha receitas na ordem dos 101 mil milhões de dólares e era uma das maiores empresas do sector de energia do mundo, disponibilizando electricidade e gás natural. A revista *Fortune* tinha referenciado a *Enron* durante seis anos consecutivos como a “Empresa americana mais inovadora (Welytok, 2006).

Em 2001 a *Enron* tinha-se tornado num conglomerado que detinha e operava oleodutos para transporte de gás, centrais eléctricas, fábricas de papel e que negociava fortemente nos mercados financeiros no mesmo tipo de produtos (Healy et al, 2003)**.**

A imagem de inovação e solidez que a *Enron* transparecia era igualmente partilhada pelos seus Gestores de Topo. Citando várias excertos dos media Sherman (2002) retratava os Gestores de Topo da *Enron* da seguinte forma: "Em Janeiro de 2000 a *Business Week* mostrou Kenneth Lay como um dos 25 Gestores de Topo desse ano. Lay e Skiling saíram igualmente no estudo anual preconizado pela *Worth* como estando incluídos nos 50 melhores CEO's. Em 2001 Skiling era classificado pela *Worth* como "uma pessoa inteligentíssima e repleto de confiança", arrecadando a segunda posição. Quando a *Worth* questionou Ken Lay acerca do seu colega este não hesitou em afirmar que "não tenho a certeza se ele tem algum osso não estratégico no corpo". A Impressa tratava a gestão de topo da *Enron* como puros santos. De acordo com a *Fortune*, Kenneth Lay era revolucionário enquanto que os pontos fortes de Lay eram descritos na *Worth* através de uma citação de uma analista como "a melhor combinação entre visão e execução que alguma pessoa tinha visto em alguém". Jeffrey Skiling, na *Fortune* foi declarado como o "executivo mais brilhante no negócio do Gás Natural". De acordo com esta mesma revista Skiling era igualmente uma pessoa modesta e um homem de família".

2.2.2 O Modelo Salarial

Como na maior parte das empresas dos EUA, a Gestão de Topo da *Enron* era fortemente remunerada através da utilização de *Stock Options*. A aplicação abusiva deste tipo de prémios ligada ao preço das acções, no curto prazo, pode explicar em parte o focos da Gestão de Topo da *Enron* na criação de expectativas de crescimento rápido, bem como nos seus esforços em inflacionar os lucros reportados, no sentido de responder às expectativas da Bolsa de Wall Street. Em 2001 no *proxy statement* **([1])** a *Enron* comunicou que passados 60 dias os seguintes planos de *Stock Options* seriam disponibilizados para serem exercidos: Kenneth Lay 5.285.542 acções, Jeff Skilling 824.038 acções e 12.611.385 acções para os restantes Directores e Gestores (Healy et al, 2003).

[1] Documento que a SEC exige que seja disponibilizado pela Organização aos accionistas por forma a estes tomarem decisões informadas aquando da reunião anual

O mesmo autor refere, citando Hall e Knox em 2002, que "o objectivo de ter *Stock Options* como forma de compensação da Gestão de Topo é alinhar os objectivos destes com os dos accionistas. Contudo, muitos destes programas de incentivos concedem elevadas porções de acções de curto prazo baseadas em manobras contabilísticas, e poucos promovem a existência de planos de longo prazo. A experiência da *Enron*, bem como de outras empresas ao longo dos últimos anos, levanta a possibilidade de os actuais programas de incentivos que, utilizam *Stock Options*, conduzirem a Gestão a tomar decisões que fomentam os resultados de curto prazo em detrimento das de longo prazo".

2.2.3 O Motivo da Falência

De acordo com Healy em 2003, o modelo de negócio da *Enron* era complexo – composto por uma grande variedade de produtos, incluindo bens físicos, negócios na bolsa e além fronteiras – e os limites da contabilidade foram levados ao máximo. A *Enron* aproveitou ao máximo as limitações contabilísticas na gestão do lucro e reporte financeiro para esconder e dar uma visão cor-de-rosa do seu desempenho performance. A *Enron* utilizou centenas de *Special Purpose Entities*[2] para se financiar e gerir o risco associado a determinados activos até 2001. O objectivo de grande parte destas entidades era puramente para efeitos de reporte financeiro. Por exemplo, em 1997 a *Enron* pretendeu comprar a parte de um dos seus parceiros numa das muitas *Join Ventures* que detinha, porém não pretendia mostrar na sua folha de balanço débitos relacionados com o financiamento para realizar a compra. Para o efeito criou um Entidade, chamada *Chewco*, que solicitou um empréstimo na ordem dos $383 milhões, garantido pela *Enron*. A transacção foi estruturada de tal forma que a *Enron* não teve necessidade de consolidar a *Chewco* ou a *Join Venture* nas suas contas, tendo, desta forma, adquirido o parceiro sem ter necessidade de reconhecer qualquer custo adicional.

[2] *Special Purpose Entities* são entidades de curta duração muitas vezes criadas como subsidiárias ou parcerias. Estas entidades têm objectivos muito bem definidos, nomeadamente avaliar a receptividade do mercado a produtos derivados do *Core* da empresa principal. Caso o mercado reaja negativamente o impacto na empresa principal é minimizado.

Em Outubro de 2001 a *Enron* revelou, igualmente, que tinha violado o princípio contabilístico que forçava que pelo menos 3% dos activos das *Special Purpose Entities* fossem detidos por investidores independentes. Ao ignorar este requisito a *Enron* conseguiu evitar ter de consolidar estas entidades não evidenciando nas demonstrações financeiras todas as responsabilidades e enaltecendo os lucros e ganhos dessas mesmas empresas.

No dia 16 de Outubro de 2001 a *Enron* anunciou a necessidade de corrigir as Demonstrações Financeiras relativas ao período compreendido entre 1997 e 2000. Estas violações implicavam, no final de 2000, reduzir os lucros em cerca de $613 milhões, aumentar as responsabilidades no final do exercício em $628 milhões e reduzir o valor accionista em cerca de $1.2 biliões.

2.2.4 A Empresa Auditora

Os Auditores da *Enron*, *Arthur Andersen*, foram acusados de aplicar os standards contabilísticos de auditoria levianamente, devido a problemas de conflito de interesses, uma vez que também prestavam serviços de consultoria à *Enron*. Em 2000 a *Arthur Andersen* lucrou cerca de $25 milhões em serviços de auditoria e $27 milhões em consultoria. É difícil determinar se os problemas da *Arthur Andersen* resultaram do conflito de interesses que a empresa tinha ao prestar serviços de Consultoria e Auditoria à mesma empresa. Todavia, dados os valores envolvidos nos serviços de auditoria, é provável que estes tenham tido impacto nas negociações entre a *Enron* e o *Partner* Local da *Arthur Andersen*. O cliente *Enron* representava cerca de 27% do valor total de facturação do escritório da *Arthur Andersen* em Houston.

Independentemente dos auditores da *Andersen* terem tido conflitos de interesse, ou pura e simplesmente não terem tido o conhecimento suficiente para avaliar uma complexidade financeira tão elevada, a verdade é que falharam no exercício de identificar as transacções que foram desenhadas pura e exclusivamente para efeitos de reporte e não para o negócio. De notar igualmente que, quando o risco de crédito nas *Special Purpose Entities* foi descoberto, os auditores da *Enron* aparentemente sucumbiram à pressão exercida por parte da Gestão da *Enron* e permitiram que a

organização diferisse o reconhecimento de responsabilidades. Os controlos internos desenhados pela *Andersen* para se proteger contra os conflitos de interesses dos *partners* locais falharam. Por exemplo, foi permitido que o escritório de Houston da *Andersen* fosse auditar as contas da *Enron* com o objectivo de refutar as conclusões da revisão executada pela *Andersen* de Chicago, cujo conteúdo continha notas criticas escritas pelo *Partner* (Healy, 2003).

No dia 10 Janeiro de 2002 a *Arthur Andersen*, auditora da *Enron*, admitiu perante o congresso que tinha destruído e rasgado um número incalculável de documentos, relacionados com a utilização de *Special Purpose Entities* pela *Enron,* com o intuito de esconder os prejuízos em que esta tinha incorrido. Nessa altura, ninguém na *Andersen* questionou e/ou impediu tais acções (Welytok, 2006).

2.2.5 Consequências:

- Dezembro de 2001 - A *Enron* apresenta a sua declaração de falência e deixa no desemprego milhares de trabalhadores;
- Março de 2002 – A empresa de auditoria da *Enron*, *Arthur Andersen* LLP, é indiciada de destruição de documentação relacionada com a *Enron*
- Junho de 2002 – A *Andersen* é condenada por obstrução de justiça e multada pelo montante máximo previsto na lei, $500.000;
- Fevereiro de 2004 - O antigo CEO Jeffrey Skilling é indiciado de 35 crimes, nomeadamente conspiração, fraude e tráfico de influências;
- Julho de 2004 - O CEO da *Enron* Kenneth Lay é acusado de conspiração, manipulação dos resultados financeiros e de proferir declarações inexactas acerca do estado financeiro e da performance da *Enron* (Welytok, 2006).

2.3 WorldCom

2.3.1 Caracterização da empresa

Zekany (2004) relata que um dos executivos mais importantes da *WorldCom*, Jonh Sidgmore, referia que a empresa desempenhava um papel importantíssimo na infra-

estrutura de telecomunicações norte americana devido ao facto de:

- Ser uma empresa inovadora que detinha um número extremamente elevado de activos. As suas receitas ascenderam a mais de $30 biliões e empregaram mais de 60 mil empregados;
- Ter mais de 20 milhões de clientes;
- Ser a maior empresa de fornecimento de Internet do mundo. As suas operações chegaram a mais de 100 países;
- Disponibilizar serviços de Internet a aplicações críticas para o governo dos Estados Unidos da América

Este gestor concluía mesmo referindo que "a *WorldCom* era uma componente chave para a economia e estrutura de telecomunicações dos EUA".

De acordo com a imprensa o desempenho da *WorldCom* devia-se fundamentalmente à gestão realizada pela Gestão de Topo da *WorldCom*, cuja cotação estava, igualmente em alta. Zekany refere em 2004, no mesmo artigo, que "o CEO da *WorldCom* Bernard Ebbers era percepcionado pela revista *Fortune* como uma das pessoas a seguir no ano 2001 (…) e que Scott Sullivan não se ficava atrás em termos de notoriedade, tinha sido intitulado como "puto maravilha" e recebido da revista CFO *Magazine* o prémio de CFO *Execellence* em 1998 (…)". Além disso, Ebber era um líder extremamente poderoso e capaz de atrair admiradores não só para Conselho de Administração e para a sua equipa, como também investidores, membros de comunidades de investimento (consórcios) e, ainda, reunir o apoio da imprensa. Na primeira pessoa, Ebbers refere a um repórter da *Fortune* que "o nosso objectivo não é capturar o mercado de capitais e ou ser global. O nosso objectivo é sermos a acção nº1 em Wall Street".

2.3.2 O Modelo Salarial

A remuneração de determinados Gestores da *WorldCom* assentava, regra geral, em três vectores: o salário, o bónus e um plano de acções. A partir dos anos 90, contudo, ficou demonstrado que o processo através do qual certos membros da

empresa eram remunerados dependia, significativamente, da posição do empregado ou do estatuto que detinha dentro da organização. Mais importante é que a teoria de compensação decidida para a empresa nem sempre reflectia aquela que estava implementada. Apesar de existir um Comité de Compensações, cuja função supostamente era a de monitorar as decisões sobre a estratégia de compensação, os seus membros abdicaram dessas responsabilidades e delegaram em Ebbers o cargo efectivo de decidir.

A gestão de topo, contudo, seguia a linha de salário definida acima. De acordo com Thornburg (2003), "entre Janeiro de 1999 e Dezembro de 2001, as compensações para estes indivíduos eram substanciais. O Sr. Ebbers, por exemplo, recebeu um total de $20.5 milhões em dinheiro e mais de 4 milhões em planos de acções, perfazendo no total (com todos os tipos de remuneração) cerca de $55 milhões durante este período".

2.3.3 O Motivo da Falência

O crescimento da *WorldCom* não foi orgânico e estruturado. A *WorldCom* cresceu através de aquisições sucessivas. Zakani (2004) menciona que Ebber comprou o maior número de empresas que pôde, através da utilização das acções da *WorldCom* como moeda. No seu todo ele organizou e promoveu a integração de 75 empresas, incluindo a maior delas, a MCI.

Em jeito de prenúncio para o que haveria de suceder, Metha (2001) refere que o desejo da *WorldCom* em adquirir novas empresas era maior que a sua capacidade de fazer com que as aquisições anteriores fossem consolidadas. Alguns observadores questionaram mesmo se as capacidades que tinham sido utilizadas por Ebber na construção da *WorldCom* o iriam ajudar a liderar a organização pelo forte/volátil mercado de telecomunicações.

Como o objectivo de Ebbers era atingir o topo de Wall Street, a ligação entre a *WorldCom* e o Mercado de capitais era extremamente próxima. A empresa aparentava respirar saúde financeira e batia todas as expectativas dos analistas (Charan e Useem, 2002).

No início do ano 2000 as despesas da *WorldCom* como percentagem das receitas começaram a aumentar e os lucros da empresa a decrescer. Este facto representava um risco extremamente elevado, caso o desempenho da empresa não subisse e os lucros voltassem a superar as expectativas dos analistas, o valor das acções caía. Devido a este facto, Zekany (2004) defende que existia uma pressão muito elevada para que o valor das acções da *WorldCom* não caísse. Esta pressão vinha não só dos investidores externos e dos analistas, mas também do próprio CEO, cuja saúde financeira pessoal dependia directamente do valor das acções da *WorldCom*. Ebbers tinha dado uma vasta fatia das acções da *WorldCom* como garantia de empréstimos pessoais[3]. Caso o preço das acções da *WorldCom* caísse substancialmente as garantias prestadas seriam insuficientes para assegurar os empréstimos contraídos. Pressões adicionais vinham igualmente do facto da *WorldCom* se ter caracterizado a si própria como uma organização altamente rentável, com o crescimento das receitas a ter um papel fundamental no sucesso inicial da *WorldCom*. Os analistas maravilhavam-se com a capacidade que a *WorldCom* tinha de crescer mais que uma indústria que, por si só, já crescia mais que a economia. Na opinião de Zekany, o crescimento contínuo era crucial para aumentar o valor das acções da *WorldCom*, de forma a estas poderem ser utilizadas como moeda nas aquisições. Adicionalmente, como a remuneração da Gestão da *WorldCom* também dependia dos resultados da empresa e era necessário atingir um aumento da receita na casa dos dois dígitos percentuais. O desempenho da empresa tinha de ser alcançado. Miraculosamente, mesmo com o mercado em condições adversas no sector das telecomunicações a *WorldCom,* continuou a crescer de uma forma impressionante.

[3] Bereford (2003) refere que no relatório o seguinte relativamente aos empréstimos de Ebbers "após examinarmos os factos e as circunstâncias destes empréstimos e garantias, incluindo as justificações para cada um deles, concluímos que são contrários aos interesses da *WorldCom* e dos seus accionistas. De facto, não percebemos como é que o Comité de Compensação e o Conselho de Administração concluíram que estes eram do interesse da organização e aceitaram a utilização de milhões de USD dos accionistas. Estas decisões reflectem uma atitude não crítica relativamente aos interesses financeiros de Ebbers e um foco insuficiente relativamente aos interesses dos accionistas."

A gestão dos custos de ligação era extremamente relevante para o lucro da *WorldCom*, pois representavam, aproximadamente, metade dos custos da empresa. Este facto fazia com que os analistas e a Gestão da *WorldCom* acompanhassem com muita atenção estes custos, bem como a sua tendência. Uma medida chave utilizada para medir o desempenho da *WorldCom*, e das *TelCos* em geral, é o rácio entre o custo e despesas de ligação e as receitas. Um aumento neste rácio indica que o desempenho da empresa se está a deteriorar, seja pela utilização deficitária da sua rede, seja pela utilização abusiva da rede de terceiros.

No sector das telecomunicações as comunicações podem passar por redes que podem pertencer ou não à empresa que presta o serviço ao cliente final. Por norma, a *WorldCom* adoptava uma estratégia de utilização dos seus próprios meios físicos para estabelecer as ligações dos seus clientes. Devido a esta estratégia, detinha uma rede de comunicação física extremamente alargada pelo mundo fora. Contudo, sempre que era necessário fornecer serviços a um cliente não conectado na sua rede, a *WorldCom* tinha de pagar uma taxa pelo aluguer da linha, o custo de interligação.

Mensalmente a *WorldCom* preparava uma estimativa de custos de interligação. Como algumas das facturas apenas eram recebidas e/ou pagas alguns meses após a sua utilização efectiva, a *WorldCom* preparava mensalmente os ajustamentos contabilísticos necessários ao reconhecimento imediato dos custos estimados como despesas do período, para efeitos de reporte financeiro. Deste modo, até pagar as facturas, os respectivos montantes permaneceriam numa conta de acréscimos de custos (*liability account*) na contabilidade. À medida que as facturas iam chegando dos fornecedores a *WorldCom* pagava reduzindo assim aquilo que havia provisionado (Zakany et al 2004).

Este seria o procedimento correcto, contudo Bereford et al (2003) refere que, durante o período compreendido entre 1999 e 2000, a *WorldCom* reduziu os custos de interligação em aproximadamente $3.3 biliões de dólares. Este feito foi conseguido através da libertação indevida de provisões ou de montantes postos de lado do reporte financeiro da *WorldCom,* para pagar facturas postecipadas. As

provisões deveriam, supostamente, reflectir os custos associados à utilização das linhas e/ou outros meios físicos de fornecedores que a *WorldCom* ainda não tivesse pago. Libertar uma provisão, quando se verifica que é necessário um montante menor para pagar facturas, tem um efeito positivo, pois vão ser considerados menos custos do que os esperados, diminui as despesas reportadas e aumenta os rendimentos antes de impostos.

No mesmo relatório podemos verificar que a *WorldCom* manipulava o processo de ajustamento de provisões das seguintes formas:

- Em algumas situações as provisões eram libertadas sem justificação (não respeitando GAAP (*Generally Accepted Accounting Principles*)). Além disso, os custos de interligação eram reduzidos (aumentando os rendimentos antes de impostos) sem qualquer razão aparente;

- Quando a *WorldCom* teve provisões em excesso, a empresa por norma não libertava as provisões no período em que estas eram identificadas. Certas provisões relacionadas com custos de interligação eram mantidas como "almofada" e libertadas para melhorar os resultados quando a gestão considerava mais oportuno.

No final do ano 2000, a *WorldCom* praticamente tinha esgotado todas as provisões disponíveis no sentido de continuar a manipular os custos de interligação á escala referida. Por esse motivo, do primeiro trimestre de 2001, até ao primeiro de 2002, reduziu indevidamente os seus custos de ligação em $3.8 biliões, nomeadamente através da capitalização de custos com a rede própria no valor de $3.5 biliões – por ordem de Sullivan – violando a política e os princípios contabilísticos estabelecidos.

Através da capitalização das despesas operacionais, a *WorldCom* adiava estes custos da sua declaração de rendimentos para a folha de balanço e, por conseguinte, aumentava o valor reportado antes de impostos por acção.

Caso a *WorldCom* não o tivesse feito, tinha reportado prejuízo antes de impostos em três dos cinco trimestres, nos quais impropriamente capitalizaram custos e nunca teria alcançado o desempenho de 42% no rácio entre despesas e receitas;

aliás, o resultado teria sido muito mais elevado, i.e, teria excedido os 50%.

No campo das receitas, a pressão para atingir os objectivos também era muito elevada.

No início de 1999, alguns colaboradores da *WorldCom* começaram a realizar movimentos contabilísticos após o fecho de contas com o objectivo de atingir as percentagens de crescimento definidas por Ebbers e Sullivan.

A maior parte das receitas que poderiam ser postas em causa durante as investigações foram identificadas em contas de receita intituladas de "*Corporate Unallocated*". Estas contas estavam separadas das contas que tinham os registos financeiros da *WorldCom* nos outros canais e eram reportadas num anexo ao *MonRV*[4], sendo conhecidas como "*Corporate Unallocated*" *Schedule*. Estes ajustamentos normalmente apareciam no final dos trimestres e não eram registados durante o mesmo, mas sim várias semanas após este ter terminado, fazendo com que o valor total reportado nestas contas fizesse disparar os fechos trimestrais. Os mais elevados (entre $136 milhões e $257 milhões) deram-se durante os trimestres que a *WorldCom* teve as receitas abaixo das expectativas, i.e., segundo e terceiro trimestres de 2000 e segundo e terceiro trimestres de 2001 (Thornburg, 2003).

A investigação levada a cabo em 2003 identificou mais de $958 milhões de receitas que tinham sido indevidamente contabilizadas entre o primeiro trimestre de 1999 e o primeiro de 2002. Adicionalmente, os auditores que avaliaram as contas, encontraram ainda $1.107 biliões de registos durante esse mesmo período que consideraram como questionáveis, e que, baseado nas circunstâncias em que foram registados não têm suporte disponível e/ou adequado (Bereford et al, 2003).

2.3.4 A Empresa Auditora

A *Andersen* reconheceu a *WorldCom* como uma empresa de máximo risco. Nos

[4] Relatório que identificava as receitas trimestrais e anuais da organização. Existiam, porém, uns relatórios especiais que continham dados manipulados com o objectivo de manipular os valores da receita que a organização reportava.

seus papéis de trabalho a *Andersen* verificou que a *WorldCom* tinha aplicado de forma errada os GAAP em certos investimentos. Os auditores independentes mencionaram ainda que "no passado tinham notado que os gestores (da *WorldCom*) tinham adoptado posições contabilísticas extremamente agressivas" (Thornburg, 2003).

Contudo e apesar de haver preocupações sérias, os auditores reportaram para o *Audit Committee* e para o Conselho de Administração da *WorldCom* que não tinham qualquer preocupação. O trabalho de auditoria nos balanços e relatório de rendimentos estava encerrado, enquanto que o relacionado com o reporte financeiro de final de ano a ser incluído no reporte anual a ser enviado para a SEC, ainda estava a ser revisto. A opinião formal reportada pela *Andersen* em 2001 foi de que os balanços e o relatório de rendimentos "apresentavam, em todos os aspectos materiais, a posição financeira da *WorldCom* e estavam em conformidade com os princípios contabilísticos geralmente aceites nos EUA. (Zekany et al, 2004)

Para Bereford (2003), a *Andersen* empregou nesta auditoria uma abordagem que ela própria caracterizou como diferente das utilizadas normalmente. Focou-se, essencialmente, na identificação de riscos e em avaliar se a organização tinha os controlos adequados para os mitigar, em vez de se centrar nos habituais testes substantivos, relacionados com os registos contabilísticos constantes nos reportes financeiros. Esta abordagem não era única da *Andersen*, e foi partilhada com o *Audit Committee*. Porém, a consequência foi que a *Andersen* falhou na identificação dos riscos significativos ou confiou nos controlos da empresa sem determinar adequadamente que estes poderiam ser dignos de confiança, por forma a poder demonstrar que não necessitavam de um teste exaustivo para detectarem situações fraudulentas (Bereford et al 2003).

2.3.5 Consequências

Em Julho de 2002, o segundo maior operador de telecomunicações de longa distância e fornecedor de Internet foi afectado por um escândalo financeiro. A SEC investigou e descobriu que a *WorldCom* tinha reconhecido receitas a mais no valor de $3.8 biliões. A SEC intitulou esta descoberta como um dos maiores casos de

fraude e “contabilidade forjada” de sempre e lamentou a sua magnitude sem precedentes (Welytok, 2006). Em Julho de 2002 a empresa pediu protecção de falência.

Na sequência do escândalo, as acções da empresa, avaliadas em cerca de 60 dólares em 1999, foram desvalorizadas e muitos dos ex-administradores foram indiciados pelo promotor Federal. O Sr. Bernard Ebbers, ex-CEO da empresa, foi considerado culpado e condenado a 25 anos de prisão. O ex-CFO (Administrador Financeiro), Sr. Scott Sullivan e o ex-contabilista David Myers foram presos.

2.4 A Lei Sarbanes Oxley

2.4.1 Introdução

Os escândalos corporativos de 2001 e 2002 têm sido referidos como a “tempestade perfeita”. Tudo o que poderia correr mal em algumas das mais prestigiadas empresas dos EUA correu. Aos olhos dos analistas os acontecimentos derivaram de um problema clássico: o risco dos Gestores e Directores não sujeitarem os seus interesses aos das empresas e dos accionistas que, supostamente, representam. Esse risco tornou-se ainda mais patente, pelo facto de não existirem pressões dos auditores externos, departamento legal, analistas e afins (Green, 2004).

A Lei *Sarbanes Oxley* de 2002 foi promulgada após os escândalos da *Enron* e da *WorldCom*, como resposta às perdas dramáticas de confiança nos gestores das organizações cotadas em bolsa. Implementada como medida correctiva a lei afecta as funções diárias de todos os gestores de topo e executivos das empresas cotadas em bolsa, nomeadamente o CEO, o CFO e o CIO. A lei criou a *Public Company Accounting Oversight Board* (PCAOB), que tem a autoridade de estabelecer e impor auditorias, certificação, controlos de qualidade e standards éticos nas organizações cotadas em bolsa. A lei concede ao PCAOB o direito de impor sanções disciplinares como resposta às violações das directivas desta entidade, leis relacionadas com a gestão de títulos e standards de auditoria. A SEC adoptou uma série de provisões da Lei *Sarbanes Oxley*, estas fazem com que os CEO’s, CFO’s e CIO’s tomem uma atenção especial ao sistema que a empresa definiu para reportar e auditar toda a

informação financeira relevante e as transacções de títulos (Anand, 2006).

2.4.2 A Independência dos auditores

2.4.2.1 Enquadramento

Raiborn e Schorg (2004) referem que a questão de independência incluída na lei *Sarbanes Oxley* não é nova. Um artigo publicado no *Jornal of Accountancy*, em 1957, tinha incluído o seguinte comentário: "na questão de manter a independência no trabalho de auditoria para um cliente que procura regularmente aconselhamento para problemas de gestão ou para quem outro tipo de trabalhos é feito, é provável que nem todas as dúvidas relativamente à independência do auditor possam ser evitadas".

Para Wright e Booker (2005), a publicidade negativa motivada pelos pedidos de falência da *Enron* e da *WorldCom,* aumentou o nível de desconfiança e cepticismo da opinião pública sobre a prática das organizações contratarem indivíduos que prestaram serviços nas auditorias e/ou para as empresas auditoras. Citando o *Washington Post,* esse mesmo autor refere que a *Enron* contratou para *Chief Accounting Officer* (CAO) um auditor da *Arthur Andersen*.

Com o objectivo de colmatar os pontos acima mencionados, a secção 208(a) da lei *Sarbanes Oxley* estabelece um conjunto de imposições. Segundo Lander (2004), a SEC adoptou, com a Secção 208(a), novas regras com o objectivo de alargar os requisitos relativamente à independência dos auditores. Estas endereçam um período de "arrefecimento" após um relacionamento profissional com o auditor, o âmbito dos serviços que podem ser prestados pelos auditores independentes, a rotação obrigatória de *partner* responsável pela auditoria e outros assuntos relacionados com a independência do auditor. Estas regras devem ser aplicadas a todos os auditores, mesmo os pertencentes a empresas de auditoria fora dos EUA.

2.4.2.2 Actividades interditas aos auditores

Segundo Rieger (2006), a Lei *Sarbanes Oxley* corrigiu a secção 10A da lei *Securities* Exchange de 1934 ao adicionar uma secção acerca de actividades proibidas. Estas regras não são inconsistentes com as regras de independência do

auditor, mas clarifica o tipo de actividades proibidas. O Auditor não pode realizar:

- Serviços de contabilidade ou outros serviços relacionados com registos contabilísticos que afectem as demonstrações financeiras do cliente;
- Serviços de avaliação, racionais de justificação, ou qualquer tipo de contribuições para os relatórios;
- Serviços de avaliação de fundos de pensões e seguros;
- Serviços de Auditoria Interna em regime de *Outsourcing*;
- Exercer funções de Gestão ou de Recursos humanos;
- Serviços de corretagem, consultor de investimentos ou investimentos em serviços bancários;
- Serviços de aconselhamento legal ou outros especializados não relacionados com a auditoria;
- Qualquer outro serviço que a comissão determine, pela regulação, como não permitido.

Qualquer serviço não relacionado com o de auditoria tem de ser precedido, obrigatoriamente, de uma pré aprovação pelo *Audit Committee*. As proibições acima têm como objectivo restringir que um auditor forneça serviços que mais tarde irão ser avaliados por si próprio.

A independência de um auditor estará em causa quando uma ou várias das seguintes situações acontecer:

- Quando o auditor está a executar uma monitorização de actividades de controlo. Esta situação pode incluir a aprovação de transacções ou execução de actividades de rotina na organização;
- Determinar qual o sistema de controlo interno a ser implementado;
- Reportar o estado dos controlos internos para a administração em nome da

Gestão;

- Ter uma relação com um qualquer empregado da empresa, que possa gerar conflito de interesses;

2.4.2.3 Tipo de serviços que as empresas de auditoria podem aceitar

A Lei *Sarbanes Oxley* coloca uma maior restrição no tipo de serviços que as empresas de auditoria podem aceitar, nomeadamente nos dois que se tinham tornado nas actividades principais da grande maioria das firmas:

1. Desenho e implementação de Sistemas de Informação Financeira;
2. *Outsourcing* das funções de auditoria interna.

Estes serviços serão aceitáveis se as receitas da empresa de auditoria, relacionadas com este tipo de serviços, for menor que 5% das receitas anuais obtidas pela da empresa face aos serviços que são autorizados. Este pressuposto tem por base o facto de uma auditora externa necessitar de ser independente do seu cliente (Raiborn e Schorg, 2004).

2.4.2.4 Período de "arrefecimento" dos Auditores

A Lei de *Sarbanes Oxley* de 2002 obriga as empresas cotadas em bolsa a respeitar um período de um ano antes de poderem contratar um antigo auditor e/ou dono de uma empresa de auditoria que lhes preste serviço para uma posição chave (Wright e Booker, 2005).

Reforçando o exposto acima, de acordo com Raiborn e Schorg (2004), uma empresa de auditoria está proibida de executar qualquer trabalho de auditoria para um cliente se esse cliente tiver contratado, para uma posição executiva (e.g.: CEO, *controller*, CFO ou CAO), um membro da empresa de auditoria que trabalhou para o cliente no ano transacto. O objectivo é evitar que os ex-colaboradores das empresas de auditoria tragam para a sua nova posição um conhecimento substancial sobre a forma como as auditorias são planeadas e conduzidas. Este conhecimento pode ser utilizado para contornar o decurso normal da auditoria.

2.4.2.5 Rotação dos *Partner*s

Raiborn e Schorg (2004), defendem que o segundo maior item na independência dos auditores é o da imposição que estabelece que o *Partner* encarregue da auditoria tem de rodar de cinco em cinco anos.

As novas regras de SEC requerem que o *Lead Partner* (responsável por todo o processo de auditoria) e o *Concurring Partner* (responsável por rever todo o trabalho produzido durante a auditoria) devem alternar entre clientes em cada 5 anos e que devem sujeitar-se a um período de interregno de mais cinco. Os *Audit partner*s (responsável pela execução do trabalho de campo), que não sejam os *Lead* e *Concurring*, não devem estar mais de sete anos num cliente e devem estar sujeitos a um período de interrupção de 2 anos. Desta forma, um *partner* pode servir como *Lead* numa subsidiaria significativa ou como *Audit partner* num nível mais acima do emissor até dois anos antes de se tornar o *Lead* ou Concurring *partner* do compromisso e ainda ter a capacidade para prestar serviço como *Lead* ou *Concurring* durante 5 anos (Lander, 2004).

Para Welytok (2006), o SOX assume que os auditores perdem a objectividade quando desenvolvem relações de proximidade e se sentem confortáveis com o cliente. Por esse motivo, a secção 203 exige que os *Lead* e *Concurring partner*s sejam substituídos em cada período máximo de 5 anos.

2.4.2.6 Conclusão

As regras impostas aos auditores actualmente não têm como objectivo criar uma parede entre o auditor e a gestão. No entanto, elas criaram uma maior tensão entre o auditor e os gestores, nomeadamente no que diz respeito ao excessivo conforto que estes haviam desenvolvido ao longo dos anos. O objectivo é criar uma maior responsabilização, no sentido de manter um equilíbrio e proteger o investidor (Rieger, 2006).

2.4.3 O *Audit Committee*

De acordo com Harrast e Mason-Olsen (2007), desde a entrada em vigor da Lei *Sarbanes Oxley* que os *Audit Committeees* têm assumido mais responsabilidades e papéis cada vez mais importantes nas matérias relacionadas com o reporte

financeiro. Por defeito, espera-se que os *Audit Committeees* mantenham uma linha de defesa contra a gestão fraudulenta, através da monitorização das funções de reporte financeiro e dos controlos internos das organizações. De facto, um *Audit Committee* independente e forte tem vindo, progressivamente, a ser indispensável no modelo de governo das organizações.

As actuais SRO (*Self-regulated organizations*) proíbem, por defeito, que os membros do *Audit Committee* 1) recebam compensações pelos seus serviços (outros que não os de directores); 2) sejam empregadores ou consultores da organização e 3) tenham quaisquer familiares directos que sejam ou empregados ou consultores da organização. Os antigos empregados e os auditores podem ser considerados independentes após um período de 3 anos de "arrefecimento" (*cooling-off*).

Um *Audit Committee* independente tem um papel fundamental no assegurar da credibilidade do reporte financeiro, bem como no reduzir da probabilidade de existência de fraude por parte da gestão. A lei *Sarbanes Oxley* veio fortalecer essas responsabilidades e requisitos.

De acordo com Pandit et al (2005) as secções 202, 301 e 407 da Lei *Sarbanes Oxley* requerem que:

- Cada membro do *Audit Committee* seja independente;
- Exista pelo menos um especialista financeiro como Membro do *Audit Committee*;
- O *Audit Committee* seja o responsável directo pela nomeação, compensação e supervisão do auditor, que por sua vez reporta directamente a este órgão;
- Todos os serviços de auditoria, e principalmente outro tipo de serviços que não os de Auditoria, sejam pré aprovados pelo *Audit Committee*;
- Sempre que considere necessário para a execução das suas funções o *Audit Committee* contrate/recorra a serviços de consultoria independentes;

- O *Audit Committee* estabeleça procedimentos para receber, reter, resolver e tratar confidencialmente todas as reclamações relacionadas, ou não, com aspectos financeiros da empresa.

O *Audit Committee* é responsável pela avaliação da Gestão e dos auditores, e deve reter a objectividade relativamente a ambos. Esta entidade é responsável por monitorizar a forma como a gestão disponibiliza a informação necessária aos auditores, para que estes possam determinar se o reporte financeiro da empresa está preparado de acordo com as GAAP e com as GAAS (*Generally Accepted Auditing Standards*). Este órgão não se deve envolver na execução das auditorias, deve sim facilitar a execução das mesmas. O *Audit Committee* constitui-se como um interface essencial entre a organização a gestão e os auditores independentes, com o objectivo de assegurar, a todo o momento, que a opinião dos auditores são baseadas em informação completa e correcta acerca da operação da organização (Welytok, 2006).

O *Audit Committee* tem de autorizar todos os serviços de Auditoria, isto significa que tem aprovar qualquer serviço que a empresa de auditoria disponibilize à organização. Estes serviços incluem a confirmação por escrito que o reporte financeiro de uma organização responde aos requisitos emanados pelas agências reguladoras.

Em particular o *Audit Committee* tem de assegurar que a empresa de auditoria que executa o serviço de auditoria não executa outro proibido pela SEC, ao abrigo do SOX, nomeadamente os serviços referidos em cima como interditos aos auditores.

Qualquer serviço não contemplado nessa lista é permitido ser fornecido desde que seja aprovado *à priori* pelo *Audit Committee*. Relacionado com os serviços que não são especificamente proibidos, o SOX contém excepções mínimas. Estas excepções aplicam-se a serviços que não sejam considerados significativos[5].

[5] Conforme referido atrás um serviço é considerado não significante se o total do serviço não relacionado com a prestação de serviços de auditoria não exceda 5% do pagamento do auditor. Se

O *Audit Committee* é responsável por assegurar que as organizações divulgam à SEC qualquer serviço prestado pela empresa Auditora que não o de auditoria, incluindo os mínimos já descritos (Welytok, 2006).

O mesmo autor refere ainda que de acordo com a Lei *Sarbanes Oxley*, o *Audit Committee* é responsável pela supervisão e por assegurar que a rotação dos *Partner*s efectivamente acontece.

De acordo com Lipman (2006), existem 10 melhores práticas para os *Audit Committee*s:

1. Estabelecer uma função de auditoria interna que reporte directamente ao *Audit Committee*;
2. Criar uma cultura ética, obediente à lei dentro da organização, sem desencorajar a vertente de risco inerente à cultura empresarial;
3. O *Audit* Committtee deve comunicar com as pessoas chave dentro da organização. Em adição, para os auditores externos, CEO e CFO o *Audit Committee* deve considerar entrevistar, pelo menos uma vez por ano, empregados e prestadores de serviços em funções chave tais como: *Controller*, Assistente de *Controller*, Chefe de Vendas; Responsável pelos Impostos, etc.;
4. Monitorizar a venda de acções pela gestão. Sempre que ocorra uma venda interna o *Audit Committee* deve adoptar a politica de requerer um aviso prévio de vários meses antes da venda ocorrer, bem como de providenciar as auditorias necessárias;
5. Estar atento a outros “avisos”. Há um conjunto de ocorrências que devem servir de alerta para o *Audit Committee* despoletar auditorias extensas e intensas. (…) Nunca falhar a projecção de lucros deve levantar uma bandeira

---

este pressuposto se verificar não é necessária a pré aprovação, contudo o Audit Committe deve aprovar o serviço antes do mesmo ser concluído.

vermelha;

6. Controlar o conflito de interesses. Nas raras situações em que o *Audit Committee* elege e aprova o conflito de interesses, um mecanismo de monitorização constante e independente deve ser montado e estabelecido;

7. O *Audit Committee* deve colocar as seguintes 4 questões de auditor:

    a. Se o auditor fosse o responsável pela elaboração do reporte financeiro, o auditor teria preparado o reporte financeiro de uma forma diferente daquela que a gestão o fez?

    b. Se o auditor fosse um investidor teria ele recebido a informação essencial para perceber de forma correcta o desempenho financeira da empresa durante o período em causa?

    c. O auditor sabe de algum facto operacional que tenha causado movimentos significativos no lucro ou vendas da organização?

    d. Se o auditor fosse o CEO a organização estaria a utilizar os mesmos procedimentos de auditoria?

8. Assegurar a independência do auditor. Se o auditor não é independente, ambos, empresa e auditor, estão a violar a Lei de *Securities Exchange Comission* de 1934;

9. Evitar utilizar o auditor para o planeamento fiscal e a preparação dos serviços fiscais. Embora o planeamento fiscal não tenha impacto na independência dos auditores de acordo com a regras da SEC, os *Audit Committee*s devem considerar se utilizar os auditores para planear os serviços é do melhor interesse para a Empresa;

10. Ponderar cautelosamente de que forma os auditores preferem que as questões contabilísticas sejam tratadas. A Lei *Sarbanes Oxley* e as regras da SEC requerem que os auditores divulguem quais são as formas preferidas por estes relativamente a determinados movimentos contabilísticos.

2.4.4 Os "*Whistleblowers*[6]"

2.4.4.1 Definição de "*Whistleblowers*"

Um "*Whistleblowers*" é usualmente definido como um empregado que divulga informação que potencialmente pode afectar o seu empregador a uma entidade com autoridade, nomeadamente o responsável máximo pela empresa, os media ou o próprio governo (Kranacher, 2006).

Welytok (2006) refere que, ao abrigo do SOX, um "*whistleblower*" é um empregado que disponibiliza informação a uma agência reguladora ou semelhante, a um membro do congresso ou à pessoa que tem a autoridade para supervisionar a conduta do empregado que está a violar:

- Uma regra ou legislação emitida pela SEC;
- Crimes contra provisões estabelecidas para os mercados de capitais;
- Diferentes tipos de fraude.

2.4.4.2 Protecções previstas para os "*Whistleblowers*"

A secção 806 da Lei *Sarbanes Oxley* proíbe que uma empresa cotada em bolsa despeça, despromova, suspenda, ameace, incomode ou discrimine de qualquer outra forma um oficial de justiça, empregado, contratado, subcontratado, ou agente nos termos e condições do seu emprego devido a um qualquer acto legal despoletado por essa pessoa para disponibilizar informação, potenciar a disponibilização de informação ou auxiliar numa investigação que diga respeito a qualquer conduta que o empregado acredita que constitui uma violação das leis federais, qualquer regra ou regulação por parte da SEC, qualquer provisão de lei federal relacionada com fraude contra os accionistas, quando a informação ou assistência é disponibilizada ou a investigação é conduzida por qualquer uma das seguintes entidades ou personalidades:

---

[6] O autor utilizou a expressão inglesa porque a tradução à letra seria "Bufos" e o sinónimo "delator"; como este último não expressa o objectivo da palavra optou por manter a original.

- Uma entidade de regulação federal ou uma agência de que faça cumprir a lei;
- Um qualquer membro do congresso; ou
- Uma pessoa com autoridade de supervisão sobre os empregados (ou uma outra pessoa com a autoridade semelhante a trabalhar para o empregador e com a autoridade de investigar, descobrir ou extinguir má conduta) (Lander, 2006).

Kinaga (2006) explica que uma das provisões da Lei *Sarbanes Oxley* define que os empregados estão protegidos desde que tenham uma crença fundamentada que casos particulares de desrespeito legal ocorreram, independentemente das actividades terem ou não tido lugar. Esses empregados são protegidos se reportarem suspeitas de violação a um supervisor ou empregado com a autoridade de descobrir, investigar ou parar a alegada conduta inapropriada, a qualquer agência reguladora federal, um agente da lei ou qualquer membro do congresso.

Se durante o processo administrativo e/ou em tribunal se verificar que o "*whistleblower*" estava correcto, ele ou ela têm direito a todos os meios necessários para compensar as suas perdas, nomeadamente a sua readmissão com o mesmo nível, o pagamento de direitos passados acrescidos de juros e compensação por quaisquer prejuízos especiais, incluindo custos de litigação, testemunhas especializadas e advogados (P. Lander, 2006).

2.4.4.3 Penalizações previstas na Lei

As sanções pela violação da secção 806 incluem compensações pelos prejuízos causados, nomeadamente a readmissão do empregado, o pagamento dos salários não pagos durante o período acrescido de juros e as custas de tribunal. A secção 1107, por outro lado, estabelece multas para qualquer pessoa que tenha uma atitude de retaliação contra um "*whistleblower*" que tenha fornecido informação a uma instituição estatal independentemente da comissão, ou eventual comissão, de qualquer ofensa federal. Esta protecção não se aplica aos relatórios produzidos para os supervisores ou para o congresso. As protecções acauteladas na secção 1107 são mais amplas e cobrem todos os indivíduos, independentemente do sítio

onde estão empregados. As multas podem ir desde $250.000 com 10 anos de prisão podendo ser impostas a indivíduos por violarem a secção 1107, enquanto as organizações podem ser multadas até $500.000 (Kranacher, 2006).

2.4.5 A Secção 302

A secção 302 da Lei *Sarbanes Oxley* requer que os Gestores das empresas cotadas em bolsa desenhem, estabeleçam e mantenham um sistema de controlo interno que assegure que a Gestão de topo seja mantida informada sobre toda a informação relevante da empresa. A Gestão deve emitir um relatório acerca da efectividade dos controlos internos e divulgar para os seus auditores financeiros e conselho de administração qualquer deficiência material no desenho ou operação dos controlos internos que possa afectar a capacidade da organização em registar, processar resumir ou reportar os dados financeiramente relevantes (Zimmermann e Thompson, 2006).

Buyer (2005) refere que as provisões da lei *Sarbanes Oxley,* citadas com maior frequência, são as relacionadas com as secções 302 e 404. A secção 404 define a responsabilidade da organização sobre os relatórios financeiros e controlos internos utilizados para se assegurarem sobre a veracidade dos dados da organização. Os controlos internos mencionados na secção 302 foram definidos para divulgar a responsabilidade que os gestores assumem pela declaração de impostos da empresa e por outros documentos relacionados para a SEC, que são responsáveis pela criação, manutenção e efectividades dos controlos que as sustentam. Adicionalmente, esses gestores devem reconhecer que estão a par de qualquer deficiência significativa ou material, no desenho ou operação, dos controlos internos que possam afectar adversamente a capacidade do emissor registar, processar, sumariar e reportar dados financeiros relevantes.

Em suma, os gestores devem comprometer-se, através de um documento legal, que dominam completamente os movimentos financeiros da organização e sistemas de controlo, e que têm condições para garantir que não existem falhas ou fraquezas em qualquer um deles.

Conforme Welytok (2006) defende, a secção 302 não deixa os CFO's e os CEO a

especularem sobre aquilo que as certificações devem conter, nem lhes dá muito espaço de manobra. Os requisitos estão estruturados de forma a disponibilizarem uma *checklist* sobre o que cada uma das certificações deve conter. Cada parágrafo da secção 302 identifica um assunto particular no que diz respeito ao reporte anual ou trimestral sobre o qual a empresa deve ser certificada.

Segundo Marchetti (2006) a certificação da secção 302 consiste em seis pontos específicos:

1. "O Executivo responsável pela certificação reviu o relatório". Note-se que rever o relatório não é a mesma coisa que ler o relatório. A simples leitura não vai ao encontro do requerido pela lei – as empresas cotadas e os seus Executivos são responsáveis pelo conteúdo e precisão dos relatórios financeiros. Os Executivos de cada organização devem aplicar os níveis apropriados de escrutínio, por forma garantirem que perceberam as matérias, as fontes, pressupostos chave e estimativas incluídas nos relatórios financeiros;

2. "Baseado no conhecimento do Executivo, o relatório não contém qualquer erro material ou omite factos necessários para que esse erro seja divulgado, e teve em consideração as circunstâncias em que o reporte foi feito e que não foi corrompido". Por outras palavras, o exposto acima significa que, baseado no conhecimento da gestão, o relatório é **Preciso** e **Completo**. Preciso, no sentido de ser factual e não conter qualquer "divulgação materialmente errónea". Completo, na medida em que contém todos os dados relevantes e que a informação apresentada não engana o leitor;

3. "Baseado no conhecimento do Executivo, as Demonstrações Financeiras, e outra informação financeira incluída no relatório, apresentam de forma justa e em todos os aspectos materiais, a condição financeira e os resultados das operações da organização à data, e para, os períodos apresentados no relatório". Adicionalmente ao facto das demonstrações financeiras da informação necessitar de ser precisa e completa, esta deve também reflectir correctamente o resultado das operações para o período específico que está

a ser apresentado no relatório;

4. Os executivos responsáveis por assinar são obrigados a:

    - Estabelecer e manter controlos internos;
    - Desenhar os controlos internos que assegurem que a informação material do emissor e que a consolidação das suas subsidiárias é feita pelos executivos dessas entidades, em particular para o período em que os relatórios periódicos estão a ser preparados;
    - Avaliar a estrutura de controlos internos do emissor durante o período de 90 dias que antecede o relatório; e
    - Apresentar no relatório as suas conclusões acerca da efectividade dos controlos internos, baseados na avaliação realizada naquela data;

A gestão é que responde pelo desenho, implementação, efectividade, operação contínua e avaliação de todos os controlos internos que asseguram que a informação financeira divulgada é completa e precisa. Uma componente critica do ambiente de controlo é assegurar que o nível de informação apropriado corre efectivamente pela organização até chegar aos executivos responsáveis pela certificação. Este processo procura prevenir que a informação seja distorcida, composta ou bloqueada.

5. “Os Executivos responsáveis pela certificação deram a conhecer aos auditores do emissor e ao *Audit Committee* do corpo de directores (ou pessoas a exercerem funções equivalentes):

    - Todas as deficiências significativas no desenho e na operação dos controlos internos que possam afectar de forma adversa a capacidade do emissor em registar, processar, sumariar e reportar a informação, e que identificaram aos auditores do emissor qualquer deficiência material nos controlos internos; e
    - Qualquer fraude, material ou não, que envolva a gestão ou outro

empregado que tenha uma função significativa na estrutura de controlos internos do emissor."

Adicionalmente a detalharem a efectividade dos controlos internos sobre o reporte financeiro, a gestão deve, também, divulgar todas as deficiências significativas e incidentes relacionados com fraude de gestão para o *Audit Committee* (ou função equivalente conforme defino pela lei) e para os auditores externos do emissor. O relatório de fraude é limitado a situações que envolvam empregados com cargos de gestão que, por natureza da sua posição, tenham um papel activo na estrutura de controlo interno da organização. O reporte de fraude deve ser feito independentemente da materialidade da atitude fraudulenta. Actividades fraudulentas requerem uma comunicação atempada.

6. "Os Executivos responsáveis pela certificação indicaram no relatório a existência ou não de alterações significativas na estrutura de controlos internos ou noutros factores que pudessem afectar significativamente os controlos internos após a data da avaliação, incluindo qualquer acção correctiva relacionada com deficiências e fraquezas materiais." A gestão deve ainda certificar que os relatórios financeiros revelam, afirmativa ou negativamente, se houve uma qualquer alteração na estrutura de controlos internos, após a conclusão da avaliação dos controlos internos, que possa ter impacto significativo. Essas revelações devem incluir todos os factores que possam afectar os controlos internos.

2.4.5.1 Definir a divulgação de controlos e procedimentos de acordo com a Secção 302

Para Welytok (2006), a Secção 302 do SOX requer que o CEO e CFO de uma empresa cotada em bolsa se certifiquem que têm controlos internos desenhados e suficientemente robustos para assegurar que estes (CEO e CFO) tomam conhecimento de todas as informações materiais dentro da organização. Esta certificação reporta ao período que cada relatório a entregar à SEC foi preparado. A SEC preconiza que qualquer divulgação acerca dos controlo e procedimentos deve pormenoriza-los, por forma a garantir que os relatórios que lhe sejam submetidos

estão correctos. O âmbito do termo “divulgação de controlos e procedimentos” é mais lato que o termo “controlo interno sobre o reporte financeiro”. A divulgação de controlos e procedimentos inclui os controlos sobre toda a informação que tem impacto sobre os recursos da empresa, não apenas nos registos contabilísticos e informação financeira.

No final de cada ano fiscal a SEC requer que a gestão:

- Avalie a divulgação dos controlos e procedimentos na altura do fecho do ano num relatório específico;
- Estabeleça as conclusões sobre a efectividade dos controlos e procedimentos que as organizações têm implementado.

Para cumprir estes preceitos as empresas iniciam um teste preliminar dos controlos internos e procedimentos o mais cedo possível no ano em que estão a reportar e realizam um teste final no fecho do ano para se certificarem que o relatório que a gestão e os auditores submeteram é válido, conforme é requerido pela secção 404.

A estrutura de controlos e procedimentos mínimos varia de acordo com as indústrias em que cada empresa opera e com as estruturas organizacionais de cada empresa. Contudo, em todas as organizações, existem preceitos básicos que necessitam de estar presentes, de modo a que a gestão possa preparar os relatórios e para que os auditores possam indicar que o relatório da gestão é preciso. Assim, a estrutura de controlos e procedimentos que uma empresa cotada em bolsa deve ter implementado, como mínimo, é a seguinte:

- **Procedimentos escritos** – Os controlos internos e procedimentos de uma organização devem ser escritos com o detalhe suficiente para poderem funcionar como linhas orientadoras, mas excessivamente detalhados, pois podem tornar-se demasiado pesados e difíceis de seguir. A implementação de controlos e procedimentos demasiado detalhados podem tornar os processos rígidos e inflexíveis e criar problemas desnecessários para a certificação;

- **Supervisão da gestão sistemática** – a gestão deve ser formalmente envolvida na supervisão dos controlos internos e dos procedimentos a um nível prático. As organizações devem, igualmente, desenvolver um calendário para monitorizar os controlos e procedimentos.

- **Um processo para rever a efectividade** – os controlos internos e os procedimentos, para as organizações residentes nos EUA, devem ser avaliados trimestralmente com o objectivo de terem a certeza que continuam efectivos.

2.4.6 A Secção 404

A (Secção 404 da) Lei *Sarbanes Oxley* define que a Gestão é responsável por "estabelecer e manter uma estrutura adequada de controlo interno e procedimentos sobre o reporte financeiro" bem como realizar uma avaliação "sobre a efectividade da estrutura de controlo interno e procedimentos" da organização que está a reportar. A lei requer ainda que "uma empresa de auditoria que prepare ou emita um relatório de auditoria para o emissor deva atestar que, e reportar sobre, a avaliação feita pela Gestão do emissor" e que "essa certificação seja feita sobre esta secção e de acordo com os standards definidos ou adoptados pelo PCAOB. Qualquer outra certificação não deve ser sujeita a um compromisso diferente" (Marchetti, 2005).

O conceito de controlo interno não é novidade. Antes da existência do SOX muitas organizações tinham excelentes controlos e procedimentos implementados. No entanto, a s404 do SOX foi criada com 3 objectivos:

- Clarificar o nível de controlo interno adequado para uma empresa;

- Obrigar a gestão e os auditores a certificarem formalmente que os controlos internos estão implementados correctamente;

- Definir as responsabilidades da SEC e do PCAOB na persecução dos objectivos do SOX.

Para levar a cabo o seu mandato a SEC definiu um conjunto de regras para implementar a s404 e focou-se em duas áreas criticas:

- Responsabilidade da Gestão – Os relatórios anuais, que têm de ser entregues na SEC, devem estabelecer de forma explícita a responsabilidade da Gestão no estabelecimento e manutenção de uma estrutura de controlo interno adequada, bem como dos procedimentos sobre o reporte financeiro;

- Efectividade dos controlos internos – O relatório anual deve conter a avaliação da efectividade da estrutura de controlo interno da organização e dos procedimentos com impacto no relatório financeiro, nomeadamente a forma como estes estão implementados no final do respectivo ano fiscal.

A secção 404 do SOX requer ainda que o PCAOB crie regulamentos específicos para os auditores auditarem a secção 404. De acordo com a secção, os auditores externos são responsáveis por atestar e reportar sobre a avaliação realizada pela gestão. Estes devem fazê-lo de acordo com os standards adoptados para o efeito pelo PCAOB. O *Auditing Standard* No.2 (e mais recentemente o AS No5) tem como propósito guiar as empresas de auditoria na certificação com a s404. A maioria das organizações tem até ao final do ano fiscal que "acabe em ou depois" de 15 de Julho de 2007 para cumprir com os requisitos divulgados pela norma SOX.

A Secção 404 do SOX impõe que todas as empresas cotadas em bolsa estejam obrigadas a incluir nos seus relatórios anuais um relatório emitido pela gestão acerca dos controlos internos da organização sobre o reporte financeiro.

As regras da SEC descrevem o controlo sobre o reporte financeiro como um processo desenhado para dar uma segurança razoável em relação à fiabilidade do reporte financeiro e na preparação das demonstrações financeiras para uso externo.

As regras da SEC impõem que o controlo interno sobre o reporte financeiro satisfaça as seguintes 3 funções principais:

- **Registo de dados** – o processo tem de assegurar que os registos são mantidos de uma forma precisa, regular, e com um nível de detalhe suficiente, de forma a reflectirem as transacções e abates que envolvam património da empresa;

- **Certificação** – o processo deve dar a segurança necessária, para garantir que as transacções são efectivamente registadas, de forma a assegurar que os recebimentos e despesas são feitos apenas quando autorizados pela gestão e que são registados de forma a que as demonstrações financeiras possam ser preparadas de acordo com as GAAP;

- **Prevenção e detecção** – o processo deve dar a segurança necessária para que a alienação não autorizada de activos da empresa possa e seja detectada.

No relatório anual entregue na SEC, a Gestão tem de incluir o seu próprio relatório sobre os controlos internos sobre o reporte financeiro da empresa. Adicionalmente, a empresa de auditoria que audita as demonstrações financeiras da empresa, tem de emitir um relatório sobre a avaliação dos controlos internos realizado pela Gestão. Este relatório é uma parte do relatório entregue anualmente pela organização.

A Gestão é obrigada a basear a sua avaliação de efectividade dos controlos internos sobre o reporte financeiro num conjunto de standards fidedignos e reconhecidos por especialistas. A SEC refere-se especificamente ao *Committee of Sponsoring Organizations of the Tradeway Commission* (COSO) como uma framework aceitável para a gestão basear a avaliação que realiza. As directivas no *Auditing Standard No 2* do PCAOB são baseadas na *framework* estabelecida pelo COSO (Welytok, 2006).

2.4.6.1 Auditing Standard No2 (AS No2)

Paul (2005) refere que o AS No2 impõe muitas responsabilidades novas às empresas de auditoria que prestam serviços às organizações cotadas em bolsa e, por acréscimo, também, às organizações. Nas suas mais de 200 páginas, o Standard No2 explana as expectativas do PCAOB relativamente a uma auditoria de controlo interno.

Definição "lata" de Auditoria Interna

Embora o AS No 2 defina "auditoria" como um processo integrado entre a auditoria

financeira e a de controlo interno, auditorias separadas levadas a cabo aquando das auditorias de controlo interno facilitam o entendimento. O AS No2 identifica os seguintes passos principais numa auditoria de controlo interno:

- Planear a auditoria;
- Analisar o processo de avaliação da gestão;
- Obter um entendimento sobre a estrutura de controlo interno;
- Testar e avaliar a efectividade do desenho dos controlos;
- Testar e avaliar a efectividade da operacionalidade dos controlos;
- Avaliar quais os testes suficientes;
- Formar uma opinião sobre a efectividade dos controlos internos sobre o reporte financeiro;
- Emitir um relatório sobre os controlos internos;
- Comunicar os "*findings*" ao *Audit Committee* e à gestão;

Responsabilidades da Gestão

O AS No 2 requer que a gestão faça o seguinte:

- Assegurar a responsabilidade pela efectividade dos controlos internos sobre o reporte financeiro;
- Avalie a efectividade dos controlos internos sobre o reporte financeiro, utilizando para o efeito um critério tal como a *framework* de controlos do COSO ou, alternativamente, uma igualmente reconhecida pelo corpo de especialistas que seguem o processo;
- Suporte a avaliação de efectividade ao controlo interno através de evidências documentais suficientes;
- Apresentar, por escrito, o resultado da análise acerca da efectividade dos

controlos internos da organização, tal como estes se encontram no final do mais recente ano fiscal;

A gestão deve realizar procedimentos suficientes para suportar a sua avaliação de efectividade dos controlos. O AS No2 proíbe a utilização dos testes realizados pelo Auditor como parte dos testes de base para a avaliação de conformidade da gestão. Se a gestão falhar no preenchimento destas responsabilidades, o auditor deve informar que a sua opinião sobre os controlos é condicionada.

Responsabilidades do Auditor

De acordo com o AS No2 o auditor tem as seguintes responsabilidades:

- Perceber e avaliar o processo de avaliação da efectividade dos controlos internos sobre o reporte financeiro levado a cabo pela gestão;
- Planear e conduzir a auditoria aos controlos internos da organização;
- Dar uma opinião sobre a avaliação formal conduzida pela gestão sobre a efectividade dos controlos internos da organização. Esta opinião incorpora a opinião do auditor sobre a efectividade dos controlos internos sobre o reporte financeiro da organização.

Efectividade do Desenho dos controlos Vs. Operacionalidade

Garantir a efectividade do desenho dos controlos tem como objectivo assegurar que o controlo está desenhado apropriadamente. A operacionalidade, por seu lado, tem como objectivo verificar se os controlos desenhados previnem, detectam ou corrigem efectivamente erros ou irregularidades de uma forma sistemática.

Importância da data da avaliação

A diferença fundamental entre uma auditoria financeira e uma de controlo interno reside no facto de existir uma oportunidade para se poder corrigir. Ao passo que as organizações podem corrigir erros materiais durante uma auditoria financeira, aceitando as recomendações do auditor, se um auditor detectar uma falha material num controlo a correcção pode não ser possível atempadamente. Assim, como a

opinião do auditor é feita à data do fecho do balanço, se existir uma deficiência material o auditor pode emitir uma opinião adversa sobre o controlo interno, mesmo quando a organização não recebe qualquer tipo de salvaguarda da auditoria financeira.

O AS No2 indica que a opinião do Auditor sobre o controlo interno é feita num determinado momento no tempo e tirada como um todo: "para expressar uma opinião sobre a efectividade dos controlos internos sobre o reporte financeiro, num determinado momento no tempo, o auditor deve obter evidência que os controlos internos sobre o reporte financeiro estão a operar, de forma efectiva, há um período de tempo suficiente, que pode ser menos que o período inteiro coberto (normalmente um ano) pelas demonstrações financeiras da organização. Para expressar a opinião sobre a efectividade dos controlos internos sobre o reporte financeiro, o auditor deve obter evidência acerca da efectividade dos controlos sobre as asserções relevantes para todas as contas identificadas nas demonstrações financeiras. Isto faz com que o auditor teste a efectividade do desenho e da operacionalidade dos controlos, como não o faria se apenas estivessem a analisar e a emitir opinião sobre as demonstrações financeiras.

Extensão necessária dos testes

A AS No2 requer que o auditor obtenha evidência sobre a efectividade dos controlos internos, com impacto em todas as asserções que afectem as demonstrações financeiras, anualmente. Cada ano deve ser tratado de forma independente. A norma também refere que o auditor deve variar a natureza dos testes, a extensão, a altura do ano em que o faz, que deve introduzir uma componente aleatória e que deve responder a potenciais alterações. Exemplos de variações de testes podem incluir a alteração do número de testes a serem executados e a combinação dos procedimentos de teste. O auditor deve geralmente executar uma bateria de testes suficientes, para obter um elevado grau de confiança, situado no intervalo entre 95% e 99%, que os controlos podem prevenir, detectar, ou corrigir erros materiais em qualquer asserção.

Utilização do "trabalho" de outros

Um auditor pode utilizar o trabalho dos colaboradores competentes do cliente, desde que o trabalho do auditor seja a principal evidência a suportar a opinião final. O termo principal "evidência" não deve ser interpretado de uma forma puramente quantitativa, o auditor deve poder ser capaz de confiar de forma extensiva em certos testes executados pelos colaboradores dos clientes, mas colocar em causa outros. As seguintes considerações devem ser tomadas em atenção quando se confia no trabalho dos outros:

- Quanto maior for a materialidade, o grau de julgamento e as estimativas inerentes numa conta, menos o auditor deve confiar nos testes dos clientes
- Quanto mais significativo for o controlo e maior for o grau de julgamento envolvido na aferição da efectividade do mesmo, mais o auditor deve confiar no seu próprio trabalho;
- Onde exista uma probabilidade elevada da gestão ignorar problemas, o auditor não deve confiar excessivamente nos testes executados pelo cliente;

Avaliação de fraquezas

De acordo com o AS No2, uma deficiência de controlo existe quando o desenho ou a operação não permite uma prevenção ou detecção atempada de erro. O standard define como deficiência significativa, algo que afecta a capacidade da organização em confiar no processo e nos relatórios financeiros, na medida em que passa a existir uma probabilidade mais do que remota das demonstrações financeiras serem afectadas de forma não material. O AS No2 define que uma fraqueza material é uma deficiência significativa, ou uma combinação de deficiências significativas, que resultam numa probabilidade mais do que remota de existir um erro material nos resultados financeiros anuais da empresa, sem que estes possam ser detectados ou prevenidos. A identificação de uma fraqueza material requer que o auditor examine as deficiências identificadas para determinar se alguma deveria ser classificada como deficiência significativa e para avaliar se alguma deficiência significativa deveria ser uma fraqueza material.

Relatório de Auditoria

O AS No2 especifica que o conteúdo do relatório sobre o controlo interno deve conter. Os auditores devem estar a par de vários factores:

- Um auditor pode disponibilizar, de forma separada ou através de relatórios conjuntos, as opiniões sobre as demonstrações financeiras e de controlo interno;
- Ao passo que a opinião sobre as demonstrações financeiras tipicamente endereçam múltiplos períodos, a opinião sobre os controlos internos cobrem apenas o ano fiscal mais recente;
- Quando o auditor emite relatórios separados o relatório anual deve conter ambos;
- Os relatórios devem ter a mesma data, por norma a última do trabalho de campo;
- O relatório do auditor para a gestão acerca dos controlos internos sobre os relatórios financeiros deve incluir uma opinião sobre a estrutura de controlo interno da organização.

Modificações aos relatórios

As seguintes situações podem motivar a alteração de uma opinião sem anotações (*clean opinion*) por parte do auditor:

- A avaliação/reporte inadequado da gestão sobre os controlos internos;
- Existência de deficiências materiais na estrutura de controlos internos da organização;
- A Gestão ou um conjunto de circunstâncias restringiu o âmbito da análise;
- O relatório do auditor confia em parte no relatório de outro auditor;
- Ocorrência de um acontecimento importante após a data em que o parecer foi emitido;

- A análise da gestão contém informação adicional. Novas informações podem trazer acções correctivas após a avaliação da gestão ou indicar planos para novos controlos serem implementados. O auditor deve emitir o seu parecer sobre esta nova informação também.

2.4.6.2 *Auditing Standard* No5

Instados a comentar o AS Nº5 Gramling e Hermanson (2007), referem que as linhas orientadoras da SEC foram sempre muita limitadas, muitas Organizações olharam para o AS No2 do PCAOB, *Uma Auditoria de Controlo Interno sobre o reporte financeiro executada em conjunto com uma Auditoria Financeira*, como as linhas orientadoras a serem utilizadas pelas empresas cotadas em bolsa. Aos olhos de muitos observadores, o facto da SEC ter emitido poucas orientações teve como resultado muitas organizações serem influenciadas pelos auditores externos a gastar demasiado tempo e energia, focando-se em detalhes de controlo interno sobre o reporte financeiro, e não adoptarem uma abordagem de risco *top-down* para endereçar o problema.

Principais fundamentos

As linhas orientadoras agora emitidas pela SEC baseiam-se em dois princípios, que de uma forma sistemática, reforçam a importância de se adoptar uma abordagem baseada em risco para endereçar a Secção 404:

- O primeiro princípio refere que a gestão deve avaliar o desenho dos controlos que implementou para determinar se estes endereçam, de uma forma adequada, o risco de um erro material nas demonstrações financeiras não ser detectado atempadamente;

- O segundo princípio defendido é que a evidência que suporta a avaliação dos controlos por parte da gestão deve ter em consideração a abordagem de risco seguida.

O primeiro princípio é impulsionado pelo facto da abordagem de risco fomentar a avaliação de risco levada a cabo pela gestão. A SEC diz que apenas os controlos chave (*key controls)* necessitam de ser avaliados, não todos os controlos. As linhas

orientadoras também referem que os controlos ao nível da Entidade podem servir como controlos chave. A essência do segundo princípio reside no facto da avaliação da gestão relativamente à operação dos controlos dever igualmente ser despoletada pelo risco associado. A gestão deve realizar testes mais aprofundados nas zonas de maior risco – seguindo a mesma abordagem que os auditores externos.

Passos a seguir no processo

Para Gramling e Hermanson (2007), a SEC disponibiliza um processo lógico, que deve ser aplicado na avaliação de controlos interno sobre o reporte financeiro. No processo de avaliação a gestão deverá despoletar as seguintes actividades:

1. Identificar os riscos e controlos sobre o reporte financeiro:
    - Identificar os riscos sobre o reporte financeiro;
    - Identificar os controlos que mitigam os riscos de uma forma adequada;
    - Considerar controlos ao nível da entidade;
    - Considerar o papel dos controlos gerais das tecnologias de informação (TI); e
    - Preparar as evidências que suportam o processo de avaliação.
2. Avaliar a efectividade da operacionalidade dos controlos internos sobre o reporte financeiro:
    - Determinar a evidência necessária para suportar a avaliação;
    - Implementar procedimentos para avaliar a operação dos controlos internos sobre o reporte financeiro; e
    - Preparar as evidências que suportam o processo de avaliação.

Quando se identificarem os riscos e o desenho dos controlos a gestão deve ter em consideração:

- Quais são os riscos chave sobre o reporte financeiro?

- Quais são os controlos que a organização tem implementados para endereçar esses riscos?
- Quais são os controlos ao nível da entidade que a organização tem implementados para endereçar esses riscos?
- Quais são os controlos relacionados com as TI que estão implementados?
- Quais são as evidências que a Organização tem para suporta a efectividade do desenho dos controlos?

A documentação do desenho dos controlos pode assumir as mais variadas formas, tudo depende da natureza da organização.

Quando a gestão avaliar as evidências que suportam a operacionalidade dos controlos internos sobre o reporte financeiro deve considerar:

- Que evidências são necessárias para avaliar a efectividade dos controlos;
- Que testes necessitam ser realizados;
- Que evidências necessitam de ser documentas.

As estratégias de testes e formatos de documentação vão variar, pois dependem do julgamento da gestão e das tipologias de controlo envolvidas. As áreas de maior risco requerem um maior nível de evidência para suportar as conclusões da gestão e algumas áreas podem estar cobertas, simplesmente, através do contacto diário da gestão com os controlos.

Quando o processo de avaliação está concluído a gestão foca-se nos pontos em que o reporte teve problemas, é aí que as deficiências de controlo são avaliadas para determinar se existe alguma fraqueza material que necessite ser reportada.

Os benefícios desejados

A SEC acredita que as linhas orientadoras propostas endereçam muitas das críticas levantadas nos últimos anos à s404, nomeadamente:

- Explica como se deve variar, em termos de abordagem, de recolha de evidências para suportar uma avaliação baseada em risco;
- Explica a utilização de "interacção diária", auto avaliação e outras actividades de monitorização como evidências de avaliação;
- Explica o propósito da documentação e como a gestão tem flexibilidade para adoptar a documentação mais apropriada;
- Disponibiliza à gestão uma flexibilidade significativa na realização de julgamentos relacionados com as evidências que suportam as zonas de menor risco; e
- Permitem à gestão e ao auditor externo adoptarem diferentes abordagens de teste;

O mais importante é que a abordagem proposta pela SEC é mais flexível e específica para cada organização. Este sistema defende que os principais controlos sobre o reporte financeiro estejam apropriadamente desenhados, documentados e testados a SEC está confortável com a abordagem.

2.4.7 O *Public Company Accounting Oversight Board* (PCAOB)

2.4.7.1 Antecedentes

Antes da existência do SOX, a SEC, os estados individualmente, e os próprios auditores partilhavam entre eles a responsabilidade de regular as empresas de auditoria que auditavam as empresas cotadas em bolsa. A influência destes era definida da seguinte forma:

- A SEC mantinha os standards para as demonstrações financeiras submetidas através dos requisitos impostos pelas leis de 1933 e 1934. Era proibido que uma *Certified Public Accounts* (CPA's) exercesse funções se não estivesse bem posicionado;
- Os estados tinham a responsabilidade de licenciar e registar os CPA's;

- A profissão de auditoria era estabelecida pela *American Institute of Accounts*, que mais tarde se tornou o *American Institute of Certified Public Accounts* (AICPA). Esta entidade privada desenvolvia standards para os auditores, para tutelar a profissão, para os conteúdos das demonstrações financeiras e ainda para a forma como as auditorias devem ser conduzidas. Os standards definidos pela AICPA foram seguidos pela maior parte dos estados de forma admirável e sem qualquer incidente até ao surgimento dos recentes escândalos.

A Lei *Sarbanes Oxley* acaba com uma era de auto-regulação, apreciada pelas empresas de auditoria, que auditam as empresas cotadas em bolsa. Esta lei cria o PCAOB com o objectivo de registar, supervisionar, e disciplinar estas empresas (Welytok, 2006).

2.4.7.2 Criação do *Public Company Accounting Oversight Board* (PCAOB)

O título I da lei *Sarbanes Oxley* cobre o estabelecimento e organização da *Public Company Accouting Oversight Board* (PCAOB). A secção 101 estabelece um corpo independente, não governamental para supervisionar as auditorias às empresas cotadas em bolsa, para proteger os interesses dos investidores e para aumentar a confiança dos investidores na independência dos relatórios de auditoria. Os poderes do PCAOB são os seguintes:

- Registar e disciplinar as empresas de auditoria que auditem empresas cotadas em Bolsa;
- Estabelecer standards contabilísticos e de auditoria;
- Investigar irregularidades financeiras.

2.4.7.3 Organização da *Public Company Accounting Oversight Board* (PCAOB)

O conselho deve ser constituído por cinco pessoas (duas que sejam CPA's e três que não sejam CPA's, mas que compreendam demonstrações financeiras, reporte financeiro, e as responsabilidades da auditoria). A nomeação destas pessoas é feita

pela *Securities Exchange Commission* em conjunto com os *Chairmans* da *Federal Reserve* e a *Treasury Secretary*. Os membros da comissão não podem manter as suas posições, nem receber pagamentos de empresas de auditoria, com excepção das reformas (Raiborn et al 2004).

2.4.7.4 Missão Visão e Objectivos

A missão do PCAOB, conforme determinado pela Lei *Sarbanes Oxley*, é supervisionar os auditores das empresas cotadas em bolsa, de forma proteger os interesses dos investidores e do público em geral, na preparação de informação, justa, e independente nos relatórios de auditoria.

Como visão, o PCAOB procura ser uma organização de regulação modelo. Usando a inovação e ferramentas apropriadas em termos de orçamento, o PCAOB tem como objectivo melhorar a qualidade das auditorias, reduzir os riscos de ocorrerem falhas nas auditorias a empresas cotadas nos mercados de capitais dos EUA e promover a confiança do publico em geral ao nível do reporte financeiro e na profissão de auditoria (http://www.sec.gov/about/whatwedo.shtml).

De acordo com a secção 102 da Lei *Sarbanes Oxley,* todas as empresas de Auditoria devem registar-se na comissão. A secção 106 requer que qualquer empresa de auditoria não residente nos EUA que prepare ou forneça um relatório de auditoria para uma qualquer empresa, deve estar sujeita aos requisitos da Lei (Lander, 2004)

O PCAOB é uma agência independente, não governamental e sem fins lucrativos que supervisiona a função de auditoria das empresas cotadas em bolsa, nos EUA, sujeitas à legislação relacionada com o mercado de capitais, a comissão está mandatada para conduzir inspecções às empresas de auditoria e ao seu pessoal de forma avaliar a conformidade com o estabelecido no acto. A frequência destas inspecções depende do número de empresas que empresa de auditoria audita (Raiborn et al 2004).

2.5 A Securities and Exchange Commission (SEC)

2.5.1 A Missão da *Securities and Exchange Commission*

A Missão da US *Securities and Exchange Commission* (SEC) é proteger os investidores, manter a justiça, a ordem, os mercados eficientes e facilitar a criação de capital.

2.5.2 A importância da *Securities and Exchange Commission*

O mundo dos investimentos é fascinante e complexo, e pode ser muito produtivo. Contudo, ao contrário do mundo bancário onde os depósitos são garantidos pelos Governos federais (realidade nos EUA), as acções, obrigações e outros títulos podem perder valor. Não têm qualquer garantia. É por esse motivo que investir não é um "desporto para espectadores". A melhor forma que os investidores têm de proteger dinheiro investido nos mercados financeiros é pesquisar e perguntar de modo antecipar problemas.

As leis e regras que governam os mercados de capitais nos EUA derivam de um conceito simples e prático: todos os investidores, sejam eles grandes ou privados individuais, devem ter acesso a determinadas informações antes de investirem, bem como durante o tempo que detiverem os activos. Para alcançar este objectivo a SEC requer que as empresas cotadas em bolsa divulguem publicamente toda a informação financeira relevante e outra qualquer pertinente. Esta situação fomenta uma base de conhecimento para que todos os investidores usem e tomem as suas decisões por si próprios, sejam elas de compra, venda ou manutenção de um título.

2.5.3 A Criação da *Securities and Exchange Commission*

A fundação da SEC foi concretizada numa altura em que era necessário fazer um reforma. Antes da grande depressão de 1929, a regulação dos mercados financeiros por parte do estado era muito ténue. Este facto foi ainda mais evidente após a 1º Grande Guerra Mundial. As propostas que o governo federal requeresse a divulgação de informação financeira de forma a prevenir a venda fraudulenta nunca foram levadas a sério.

Tentados pelas promessas de rápida ascensão a "novos-ricos" e de crédito fácil,

poucos investidores tiverem em consideração os perigos inerentes de um mercado descontrolado. Durante os anos 20, aproximadamente 20 milhões de grandes e pequenos accionistas aproveitaram a era de prosperidade vivida no pós guerra e decidiram fazer fortuna nos mercados financeiros. Durante este período estima-se que dos cerca de 50 biliões de dólares oferecidos em novos títulos pelo menos metade tenha perdido valor.

Quando o mercado de capitais implodiu em Outubro de 1929, as fortunas de inúmeros investidores perderam-se. Os bancos, também, perderam uma grande quantia de dinheiro neste período, pois tinham investido fortemente no mercado financeiro. A população, com receio que os bancos não fossem capazes de restituir os depósitos que tinham recebido, correu a levantar os mesmos provocando uma quebra no sistema bancário.

Com a queda bolsista e a consequente depressão que se seguiu, a confiança dos investidores nos mercados caiu radicalmente. Para que a economia reanimasse era necessário restituir novamente a confiança dos investidores nos mercados de capitais.

As leis designadas para restaurar a confiança dos investidores nos mercados de capitais foram a *Securities Act* de 1933 e *Securities Exchange* Act de 1934. Estas leis tinham como objectivo promover uma maior e mais estruturada supervisão do estado. Os dois objectivos fundamentais destas leis podem reduzir-se a duas notas de senso comum:

- As empresas que ofereçam publicamente títulos de investimento têm de divulgar ao público a verdade sobre o seu negócio, os títulos que estão a disponibilizar e os riscos envolvidos no investimento;
- As pessoas que vendam ou troquem títulos (e.g.: corretores) têm de tratar os seus investidores de uma forma justa e honesta, colocando os interesses dos investidores acima de tudo.

Como a monitorização do mercado financeiro requer um enorme esforço de coordenação, o congresso norte americano estabeleceu a SEC, em 1934, com o

intuito de forçar o cumprimento das leis estabelecidas, promover a estabilidade nos mercados e, mais importante que tudo, proteger os investidores.

2.5.4 Organização da *Securities and Exchange Commission*

A SEC é constituída por cinco comissários nomeados pelo presidente do EUA, após ter recolhido o aconselhamento e consentimento do Senado. Cada mandato dura cinco anos, porém todos os anos, a 5 de Junho, há um que cessa funções.

Entre outras, algumas das violações mais comuns que podem levar a investigações por parte da SEC são:

- Comprar ou vender um título motivado pelo acesso a informação privilegiada não pública;
- Informações falsas ou omissões importantes acerca de títulos;
- Manipulação dos preços dos títulos nos mercados;
- Roubar fundos ou títulos aos clientes;
- Os corretores violarem o princípio através do qual são obrigados a tratar os seus clientes de uma forma justa;
- Venda de títulos sem estarem devidamente registados.

2.5.5 *Sarbanes Oxley* e a *Securities and Exchange Commission*

A SEC está encarregue de estabelecer as regras para implementar todas as provisões legais da Lei *Sarbanes Oxley*. De facto o SOX requer especificamente que a SEC estabeleça regras em 19 áreas diferentes. O congresso exigiu que 12 dessas áreas fossem disponibilizadas no espaço de 12 meses após a passagem da Lei em 2002. Adicionalmente, o SOX requer que a SEC reveja os relatórios anuais e trimestrais das empresas cotadas em bolsa pelo menos uma vez em cada três anos. A SEC anunciou, inclusive, que as maiores empresas cotadas em bolsa poderiam preparar-se para pelo menos uma vez por ano serem auditadas (Welytok, 2006).

Anand (2006) menciona que a SEC adoptou muitas das provisões estabelecidas

pela Lei *Sarbanes Oxley* e que esta entidade supervisiona o PCAOB. A Lei *Sarbanes Oxley* requer que a SEC promulgue todas as regras e regulações relacionadas com qualquer material retido, relacionado com auditorias; nomeadamente comunicações, correspondência e outros documentos criados, enviados ou recebidos que tenham ligação com uma auditoria ou revisão. A seguinte lista define os deveres adicionais da SEC:

- Supervisionar o PCAOB;
- Nomear os membros do PCAOB;
- Requerer uma ordem de tribunal para impedir uma pessoa de se tornar ou manter como director ou executivo de um emissor, se o comportamento desse indivíduo não for o adequado para a posição;
- Rever os relatórios enviados pelas empresas pelo menos uma vez a cada 3 anos;
- A SEC disponibilizou um conjunto de regulamentos que os advogados devem seguir:
    - Qualquer advogado que trabalhe para uma empresa cotada em bolsa deve reportar ao CEO ou ao Executivo principal da Organização, se tiver evidência que ocorreu uma violação de regulamentação;
    - O Advogado deve ainda assegurar-se que o Executivo principal ou o CEO tomas acções relativamente a essa evidência. Se nenhum destes tomar providência o advogado deve informar o conselho de administração e o *Audit Committee*.

3 Caso de Estudo

3.1 Organização do Projecto

3.1.1 Introdução

Dada a dimensão do Grupo, o número de entidades envolvidas na certificação da s404 era muito elevado e a estrutura organizacional complexa. Ao mais alto nível estavam envolvidos os CEO/CFO do Grupo, os CEO/CFO das entidades regionais e ainda os CEO/CFO das empresas locais. Esta multiplicidade e grandeza fazia com que os mais altos executivos precisassem de confiar nos *sign-offs* realizados pela gestão intermédia, bem como nas informações recolhidas pelas equipas de projecto locais.

Com o objectivo de simplificar a gestão do projecto e simultaneamente fazer com que a implementação fosse robusta, a Gestão de Topo promoveu uma implementação dividida em duas componentes, uma de gestão central, a nível do Grupo, com o propósito de coordenar o progresso e disponibilizar linhas orientadoras, outra focada na implementação das orientações do grupo localmente.

Como o projecto no grupo era patrocinado pelos mais altos Gestores do Grupo, a Gestão de topo das empresas locais apoiou a sua implementação. Este factor foi crítico para o sucesso, pois o suporte da Gestão funcionou, em muito casos, como um acelerador para as situações de impasse.

3.1.2 Fases do Projecto

O projecto de implementação da s404 conheceu várias fases até chegar a *Business as Usual* (BAU). A equipa de gestão de projecto do Grupo, em conjunto com a Gestão de Topo, definiu o plano e as *milestones* que deveriam ser cumpridas por todas as empresas do Grupo. O projecto arrancou em Setembro de 2004, com objectivo de atingir 31 de Março de 2006 com toda a *framework* de controlos implementada e com um ano de *buffer* para endereçar pequenos ajustes, nesta fase já em BAU.

O plano de projecto era complexo, porém foram identificadas logo à partida um

conjunto de *milestones* criticas que tinha de ser cumpridas por todos. Em baixo apresentam-se as mais importantes:

Documentação, Remediação e Testes Piloto – 28 de Fevereiro de 2006

> Contemplava as fases de levantamento da realidade existente nas empresas, nomeadamente a definição do âmbito, a identificação do GAP face ao exigido pela s404 e a implementação da respectiva remediação. É nesta fase que os Processos de Negócio são desenhados e ajustados para dar resposta aos requisitos da s404. Esta etapa termina com a primeira fase de testes operacionais à *framework* de riscos e controlos. O objectivo dos testes nesta fase era não só testar os controlos, mas, também, a metodologia de testes. De referir, que não obstante o facto do *deadline* principal ser o apresentado esta fase teve *milestones* intermédias, por forma a se poder avaliar o progresso.

Dry Run focado no fecho do ano e na consolidação das contas – Março/Maio 2006

> Simulação do fecho de ano, contemplou os processos de reporte mais significativos da organização e abrangeu todo o Grupo. Como o fecho de ano apenas ocorre anualmente, esta simulação era de extrema importância e deveria abarcar todos os controlos da *framework* que constassem nos processos.

Iniciar a fase de *Business as Usual* – 1 de Abril de 2006

> Após a fase inicial de levantamento e correcção das situações de excepção identificadas, esta fase tinha como objectivo garantir a sustentabilidade da certificação.

Concluir o desenho dos controlos – 30 de Junho de 2006

> Prazo limite para conclusão do desenhos de controlos considerados como mais difíceis de corrigir. Importa salientar que as empresas que precisaram recorrer a esta fase tiveram de submeter uma exposição ao Grupo, previamente aprovada pela Gestão local;

Testar a operacionalidade dos controlos chave uma vez – 30 de Setembro de 2006

Nesta data todos os controlos chave da organização precisavam de ter sido testados pelo menos uma vez. Esta fase tem uma importância significativa, porque, após a avaliação do desenho dos controlos ter sido concluída, é preciso verificar se estes são passíveis de operar. Caso se conclua que os controlos são não eficazes operacionalmente, tem de se promover a respectiva remediação. Por este motivo, quanto mais cedo isso for aferido menos risco envolve para a certificação.

Simular o processo da Certificação – 30 de Setembro de 2006

Em linha com a simulação de fecho ocorrida na data do fecho do ano, esta deveria ser uma réplica do processo que iria ocorrer na data de certificação. O objectivo era simular o processo de certificação para que na data do mesmo tudo corresse conforme planeado.

Excepções

Embora a Gestão local tivesse a responsabilidade de garantir que todos os esforços eram feitos para que as *milestones* fossem cumpridas, em casos excepcionais – nomeadamente os relacionados com a eficiência do negócio – os atrasos eram autorizados. Por exemplo, se uma alteração significativa ocorresse em Setembro de 2006 a Gestão podia querer esperar pela implementação da alteração e apenas depois documentar e realizar os testes. Nestas circunstâncias a Gestão local necessitava de contactar o Grupo para acordar um novo *deadline* e submeter essa data à aprovação da Gestão de Topo.

3.1.3 Departamento no Grupo responsável pela Certificação

3.1.3.1 Estrutura da equipa e principais responsabilidades

Dada a importância do Projecto existia um Patrocinador Executivo – o CEO do Grupo – que encorajava dentro da organização uma cultura de honestidade e abertura. O objectivo era obter o máximo conhecimento e identificar todas as

deficiências, que devessem ser reportadas ao *Audit Committee*. Dada a elevada posição do Patrocinador Executivo, havia a necessidade de identificar uma pessoa, com responsabilidade e *empowerment,* que acompanhasse a implementação do projecto de forma mais apertada. O Director financeiro foi indicado como Patrocinador do Projecto reportando directamente ao CEO do Grupo e à *Steering Committee*. A este gestor cabia a responsabilidade de assegurar a gestão operacional da equipa de projecto, vide figura 1.

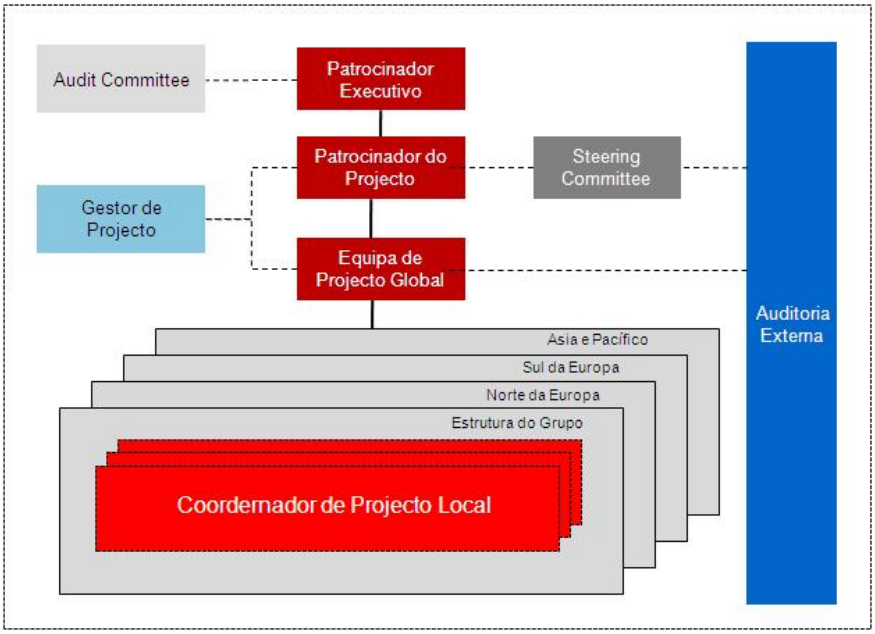

Figura 1 – Organigrama Global da Equipa de Projecto

(Fonte: Empresa objecto de caso de estudo)

A equipa de projecto foi então montada da seguinte forma: um Gestor de Projecto – que reportava directamente ao Director Financeiro – e uma equipa que se dividia em duas vertentes, uma focada nos Processos de Negócio e outra nos *General IT Controls* (GITC), cada uma com um líder operacional. As principais responsabilidades desta equipa eram:

- Definir uma metodologia de implementação da s404;
- Implementar uma ferramenta que suportasse a certificação, nomeadamente que armazenasse a documentação relacionada com a avaliação dos controlos que suportam o reporte financeiro;

- Desenvolver e disponibilizar métodos de formação às empresas do grupo;
- Determinar os racionais que suportam a definição do âmbito da certificação;
- Definir a estratégia de testes dos controlos;
- Executar revisões qualitativas periódicas sobre o trabalho levado a cabo pelas empresas do grupo;
- Monitorizar e reportar para a gestão de topo o cumprimento das *milestones* do projecto;
- Avaliar o impacto das deficiências detectadas na certificação global;
- Reportar à *Steering Committee* da s404; e
- Reportar para o *Audit Committee* do Grupo qualquer deficiência significativa ou material encontrada.

Embora a estrutura de recursos humanos fosse composta maioritariamente por recursos internos da empresa, houve a necessidade de recorrer a algum suporte de consultoria. A s404 era uma peça de legislação muita recente, não existiam metodologias e/ou casos de estudo que pudessem ser seguidos. A utilização de recursos externos, especializados em controlo interno e gestão de risco, que congregassem conhecimentos financeiros com sistemas de informação, foi importante para acelerar a fase inicial do projecto. Por esse motivo, foi definido um parceiro estratégico que disponibilizava recursos especializados nestas matérias e que servia igualmente de consultor nas reuniões de *Steering* e *Audit Committee*s, colocando à disposição todo conhecimento acumulado ao longo de vários anos de experiência.

3.1.3.2 Relacionamento com as empresas do Grupo

As responsabilidades que a equipa de Gestão de Projecto global assumia faziam com que o relacionamento com as restantes empresas do Grupo tivesse de ser muito estreito. Era extremamente importante manter os canais de comunicação abertos e fomentar a partilha de conhecimento entre os vários interlocutores. Os

assuntos a tratar eram sempre variados, logo os formatos, também, eram diferentes. Dependendo do assunto o formato da comunicação/interacções variava. Em baixo o autor apresenta aquelas formações/interacções que na sua perspectiva tiveram maior importância no desenrolar do projecto.

Sessões de Formação

Principalmente na fase inicial, porém igualmente importante para acolher novos recursos, as sessões de treino tinham como intuito formar os elementos das diferentes entidades do Grupo nas ferramentas, metodologia de análise adoptada e explicar a *framework* de Riscos e Controlos da organização

Worskshops

Sessões regulares de partilha de informação e *Best Practices*. O objectivo de fomentar a cooperação entre as várias empresas do Grupo. Nestes eventos cada entidade era convidada a partilhar com as restantes um caso de sucesso e a preparar uma sessão de *brainstorming* sobre o tema. No final, eram recolhidos os principais tópicos de interesse e partilhados entre todos.

Conference Calls

Quinzenalmente eram organizadas *Conference Calls* em que participavam todas as entidades. O propósito destas era discutir e partilhar os assuntos de curto prazo.

Manuais

Manuais detalhados com linhas orientadoras sobre os mais variados temas relevantes para a certificação. Estes contemplavam, por exemplo, a forma como o âmbito era definido, metodologias de auditoria, os procedimentos de testes operacionais e análise de deficiências.

Memorandos

Sempre que acontecimentos importantes ocorriam eram enviados memorandos para os Contactos Chave e para a Gestão de Topo dessas

empresas. Estas comunicações ocorriam essencialmente para comunicar *deadlines* impostos pela *Steering Committee*, alterações aos manuais e/ou outros assuntos pertinentes a serem considerados localmente.

3.1.3.3 O Envolvimento da AI

Em virtude da importância que o *Audit Committee* tem sobre a s404, bem como da experiência acumulada que os Auditores internos possuem sobre a componente de Gestão de risco, a Auditoria Interna da Organização assumiu um papel muito importante na certificação. As responsabilidades da Auditoria Interna no contexto da s404 consubstanciavam-se no seguinte:

- Monitorizar a implementação no sentido de assegurar que os riscos estão mitigados, nomeadamente através da supervisão dos testes operacionais;
- Disponibilizar suporte à gestão local para assuntos relacionados com âmbito de risco e documentação;
- Validar os planos de remediação fornecidos pelas áreas;
- Formar os elementos responsáveis pela execução dos testes;
- Testar as zonas de mais alto risco;
- Confirmar a execução a adequada dos testes.

3.1.3.4 Acompanhamento do Projecto

O progresso do projecto era monitorizado com uma periodicidade mensal, através da submissão de um relatório de KPI's preenchido por todas as empresas do Grupo. Este relatório era composto por duas vertentes, uma que media o progresso das várias *streams* de trabalho (identificadas em cima) face aos *deadlines,* e outra que avaliava a qualidade dos *outputs* produzidos, isto é, o número de controlos efectivos face ao total requerido. No final de cada mês o Grupo agregava os relatórios submetidos pelas empresas e consolidava a informação num único relatório, que era submetido para todos os CEO's, CFO's e contactos chave das empresas. Com isto o grupo pretendia dar visibilidade sobre o progresso das várias empresas e

promover a identificação/resolução de eventuais pontos de atraso com que as empresas se pudessem estar a deparar.

3.1.4 Departamento responsável pela Certificação Local

3.1.4.1 Estrutura da equipa e principais responsabilidades

Embora as linhas orientadoras provenientes do Grupo fossem extremamente úteis, a verdade é que a especificidade de cada país fazia com que os moldes de gestão de projecto adoptados pelas diferentes empresas do Grupo diferisse. Em Portugal a opção foi montar uma equipa de projecto dedicada 100% à certificação.

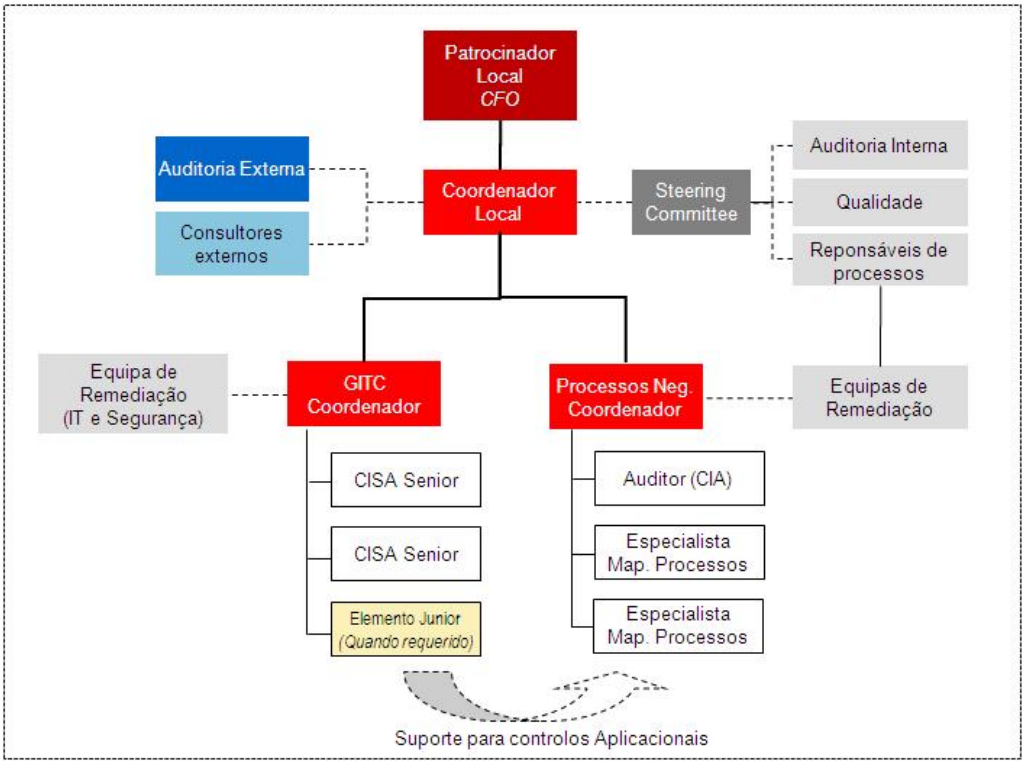

Figura 2 – Organigrama local da Equipa de Projecto

(Fonte: Empresa objecto do caso de estudo)

A equipa de Projecto Local era composta por um Coordenador e por duas equipas de trabalho, a de GITC e a de processos de negócio. Cada uma destas equipas tinha um *Team Leader* que reportava ao Coordenador de projecto que por sua vez respondia hierarquicamente perante o CFO local, o Patrocinador do local do projecto.

Em termos de responsabilidades, para o Coordenador do Projecto foram definidas as seguintes:

- Coordenar o processo de certificação da s404 para a empresa;
- Preparar o plano para a área e alocar recursos;
- Promover a concretização do plano;
- Assegurar a conclusão da documentação relevante, os testes dos controlos, acções de remediação e respectiva monitorização de conclusão;
- Reportar o progresso para o grupo;
- Solucionar os problemas operacionais e escalar os mesmos recursos quando necessário;
- Manter uma linha de comunicação regular com a equipa de projecto do Grupo, a Auditoria Interna, e com o CFO local;
- Assegurar o nível adequado de treino para os colaboradores envolvidos na certificação da s404;
- Rever a documentação, no sentido de garantir que os interfaces entre departamentos e/ou outras entidades estão assegurados de forma adequada;
- Garantir a implementação da abordagem relacionada com os GITC, por forma a garantir que os Processos de Negócio estão devidamente suportados;
- Assegurar que os Responsáveis pelos Processos de Negócio estão cientes da sua responsabilidade e esfera de actuação;
- Assegurar a disponibilidade dos recursos necessários;

Os *Team Leaders,* além de suportarem o Coordenador na prossecução das responsabilidades enunciadas em cima, tinham ainda o dever de:

- Garantir que a gestão estava comprometida com os objectivos, através de acções de sensibilização;
- Documentar, testar e avaliar os processos e controlos internos;
- Executar revisões de qualidade à documentação; e
- Detalhar as actividades de terreno, o progresso, resolver problemas operacionais; e reportar o andamento do projecto ao Coordenador local.

A Equipa de projecto era maioritariamente constituída por recursos internos da empresa, porém era necessário dotar a mesma de alguns *skills* específicos. A utilização de recursos externos, como parte integrante da mesma, foi um factor extremamente importante. Estes recursos trouxeram para a equipa um tipo de conhecimento diferente, focado no essencial e suportado nas melhoras práticas do mercado. Na componente de GITC a utilização deste tipo de conhecimento foi fundamental.

Atingir a conformidade com a s404 é um objectivo complexo de atingir. Envolver toda a organização e garantir que esta estava sensibilizada para o efeito foi um factor crítico de sucesso. Por esse motivo, existiam outras entidades (e.x.: *Steering Committee*) que, embora não tivessem um linha hierárquica de reporte formal associada, funcionavam como membros consultivos, de decisão e ou de acompanhamento e suporte.

3.1.4.2 Relacionamento com a Organização

Embora a equipa de projecto assumisse uma grande quota de responsabilidade na implementação dos requisitos da s404, era necessário garantir o envolvimento de toda a organização. Para o efeito, a equipa de projecto preparou uma estratégia, que contemplava três vectores de actuação: uma comunicação efectiva com a organização, sessões de formação e esclarecimentos e *workshop* para fomentar a partilha de conhecimento e a interacção entre os vários elementos da organização envolvidos.

Comunicação

Os requisitos da norma exigiam da organização um esforço significativo, por isso comunicar da forma correcta era crucial para captar a atenção e garantir o envolvimento. Por este motivo, a equipa dedicava especial atenção às comunicações; todas eram focadas no essencial e adaptadas ao receptor, sendo o principal objectivo acautelar a passagem de ruído e evitar que a empresa fosse inundada de informação acessória que pudesse causar desconforto.

O Coordenador do Projecto definiu a abordagem como *Top Down* e *Bottom-up*. A primeira era alcançada através do Coordenador nos fóruns em que tinha assento, a segunda através dos líderes equipas de projecto que procuravam e garantir o envolvimento dos colaboradores a nível operacional.

Sessões de formação

As sessões de formação tinham como principal objectivo formar e dotar os membros da organização do conhecimento necessário para este desempenharem suas responsabilidades no âmbito da s404. Estas sessões de formação tiveram uma incidência muito forte no início do projecto e focavam-se essencialmente nos seguintes pontos:

- Requisitos da lei;
- Ferramentas de suporte;
- Princípios metodológicos inerentes à *framework* de riscos e controlo;
- Conceitos básicos de mapeamento de processos;

Após a fase de arranque – altura em que foi preciso elevar o nível de conhecimento da organização até um determinado patamar – estas sessões de treino passaram a ter uma periodicidade diferente. Decorridos os primeiros seis meses estas acções passaram a ocorrer trimestralmente, para dar resposta aos elementos novos das equipas, que lidam mais de perto com estes temas.

Workshops

As *workshops* eram sessões de trabalho um pouco diferentes das sessões de formação referidas em cima. Não tendo uma periodicidade definida estas sessões aconteceram, essencialmente, durante o período em que foi necessário desenvolver/implementar as correcções identificadas na auditoria inicial.

Nestas sessões participavam os elementos das equipas de projecto e as áreas da organização, sendo o objectivo discutir um determinado tema (normalmente relacionado com a matriz de riscos e controlos) utilizando diferentes tipos de conhecimento. O resultado deste tipo de acções era reconhecidamente positivo por vários motivos:

- Envolvia a e aproximava a organização dos temas críticos para a certificação;
- Os controlos tinham uma probabilidade maior de serem considerados operacionalmente efectivos, pois o conhecimento de terreno utilizado era o da organização;
- O envolvimento das áreas na solução promovia uma sensação de pertença e de partilha, motivando um maior *buy-in* destas face ao projecto;
- A equipa de projecto era vista como um parceiro que acrescentava valor para a organização.

3.1.4.3 Acompanhamento do projecto

De acordo com vários estudos realizados os projectos de implementação da s404 eram extremamente difíceis e complexos de levar a cabo com sucesso. Juras et al (2007) referem que a implementação da s404 do SOX é um pesadelo para as empresas que têm de responder aos seus requisitos. Além dos custos com as auditorias externas crescerem de forma exponencial é igualmente requerido um dispêndio considerável de tempo e de recursos para o implementar. O autor refere

ainda que num estudo levado a cabo pela *Ernest & Young* em 2005, foi constatado que, não obstante o esforço das organizações, 14% destas ainda continuavam a reportar controlos não efectivos que se repercutiam com deficiências materiais.

Conhecendo estes estudos e a realidade nos EUA, onde as empresas eram forçadas a estar certificadas desde 2004, o Coordenador do Projecto local assumiu desde início um controlo muito apertado sobre os prazos e sobre a qualidade dos *outputs*. A gestão do projecto foi sempre feita recorrendo às melhores práticas existentes no mercado, nomeadamente através das linhas orientadoras do *PMI Book*. O progresso era medido através de métricas quantitativas e qualitativas - que ditavam a evolução positiva ou negativa - e periodicamente existia uma reflexão sobre o riscos e *issues* que podiam colocar em causa os *deliverables* estabelecidos.

O facto da equipa se encontrar dividida em dois pólos de actuação diferentes, fazia com que, necessariamente, existissem dois planos de trabalho distintos, um focado na componente de Processos de negócio e outro na vertente de GITC. Para realizar estes planos as *milestones* impostas pelo Grupo foram dissecadas em detalhe. Assim, cada uma das *work streams* definiu planos de trabalho distintos com *deliverables* intermédios, de modo a facilitar o acompanhamento do progresso e potenciar a tomada rápida de medidas correctivas/preventivas. Adoptando a máxima de “vamos procurar problemas antes que estes nos procurem a nós”, periodicamente os líderes das duas *work streams* reflectiam sobre os riscos e *issues* que podiam ter impacto nos prazos ou nos *outputs* e definiam um conjunto de acções com responsáveis e prazos limite para concretização. O Coordenador do projecto garantia a coesão dos planos através da sua monitorização reportando para o CFO a visão consolidada destes.

Não obstante o facto de o exposto em cima resultar de um trabalho diário, no decorrer do projecto foram constituídos alguns fóruns de discussão/decisão periódicos onde o progresso do projecto era debatido e monitorizado. Os três fóruns mais relevantes durante a fase de implementação foram a *Steering Committee*, as *Staff Meetings* da equipa de projecto e as reuniões periódicas com as equipas de remediação.

Steering Committee

O *Steering Committee* era um fórum quinzenal no qual participava o CFO, o Coordenador do Projecto, os Responsáveis pelos Processos da Organização – *Process Owners* –, o Director da Auditoria e o Responsável pela Qualidade (responsável por mapear os processos de negócio). Nestas sessões o Coordenador do projecto apresentava o progresso, salientando o que de mais relevante tinha ocorrido durante o período, reportando, igualmente, de que forma os principais *issues* e riscos tinham evoluído.

Como esta entidade assumia o papel de órgão consultivo e decisor, houve sempre o cuidado de filtrar ao máximo os temas apresentados, apenas os mais relevante e problemáticos levados para as sessões a fim de serem discutidos. O facto da *Steering* ter uma exposição elevada perante a gestão de topo fazia com que imediatamente antes da reunião os principais envolvidos tivessem o cuidado de acautelar que todos os pontos de agenda, nomeadamente, riscos, *issues* e progresso estavam de acordo com o expectável. Caso algum tema ainda não tivesse sido endereçado, o facto da *Steering* acontecer promovia uma resolução mais rápida. Normalmente, os problemas já eram apresentados com uma proposta de resolução, com um responsável atribuído e prazos definidos. Nestas situações a *steering* promovia apenas os ajustes necessários à sua concretização.

Reuniões de *Staff* Semanais

Embora a partilha de informação fosse uma prática instituída entre a equipa de projecto, foi definido desde o início que semanalmente havia uma reunião para monitorizar o progresso. Estas reuniões eram moderadas pelo Coordenador do projecto, mas os principais interlocutores eram os Líderes de cada uma das *work streams*. Estes apresentavam durante a sessão o progresso da semana salientado o que de mais relevante tinha acontecido.

Nestas reuniões os prazos do projecto eram monitorizados em detalhe e as dificuldades que podiam colocar em causa a certificação identificadas. Assim,

além do natural controlo de projecto, eram também discutidas questões relacionadas com o desenvolvimento qualitativo dos *outputs*, nomeadamente se a efectividade da *framework* de controlos necessária para mitigar os riscos estava a ser implementada com sucesso. Por norma, os problemas identificados assumiam posteriormente o formato de risco ou de *issues*, sendo que os com maior impacto eram reportados e os mais graves apresentados na *Steering Committee*.

Reuniões com as equipas de remediação

Após a equipa de projecto ter concluído a primeira auditoria e identificado o GAP da organização face à lei, as diferentes áreas da organização sentiram a necessidade de criarem Equipas de Remediação. Estas equipas eram formadas por elementos da empresa e/ou externos, cujo dever era garantir a implementação das devidas correcções aos Processos e/ou controlos. Estas equipas respondiam directamente aos Responsáveis pelos Processos, sendo que o seu relacionamento com a equipa de projecto era constante. Entre outros aspectos as equipas de remediação procuravam a equipa de projecto com o objectivo de obter suporte, linhas orientadoras e focos no essencial para a certificação.

Semanalmente, os elementos responsáveis pela acções de remediação apresentavam aos lideres das equipas de projecto o estado das acções que estavam a ser desenvolvidas no terreno para colmatar o GAP e as principais dificuldades e/ou progressos. A equipa de projecto utilizava estes encontros com vários objectivos:

- Monitorar o progresso das actividades de remediação e respectivos prazos;
- Desafiar as soluções apresentadas pelas áreas, nomeadamente se as soluções técnicas propostas para as actividades de controlo eram as mais adequadas e mais eficazes para mitigar os riscos inerentes;
- Garantir o envolvimento e o *Buy-in* das áreas da organização.

3.2 Visão Global da Metodologia do Grupo

3.2.1 Introdução

A metodologia seguida pelo grupo foi desenhada para responder aos requisitos específicos da s404 de uma forma eficiente, permitindo à gestão e aos auditores externos afirmarem e atestarem o considerado necessário.

As etapas principais da metodologia do Grupo consubstanciam-se da seguinte forma:

- Definição do âmbito das entidades ao nível das Contas e Processos;
- Avaliação dos controlos internos ao nível da entidade;
- Avaliação dos controlos internos ao nível dos processos, nomeadamente através da:
    - Identificação e documentação dos processos dentro do âmbito e fluxos de transacções relacionados;
    - Identificação dos riscos e controlos associados;
    - Execução de *walkthroughs* aos Processos e aos Controlos;
    - Testes sobre os controlos chave de cada processo dentro de âmbito;
    - Remediação das fraquezas identificadas nos controlos a tempo dos mesmos poderem ser testados ou re-testados;
    - Avaliação da efectividade dos controlos sobre o reporte financeiro;
- Certificação do controlo interno pela Gestão;
- Atestação do nível de controlo interno por parte dos Auditores externos;

Esta metodologia foi produzida com base nas melhores práticas existentes no mercado ao nível da Gestão de risco e pode ser ilustrada através da figura 3.

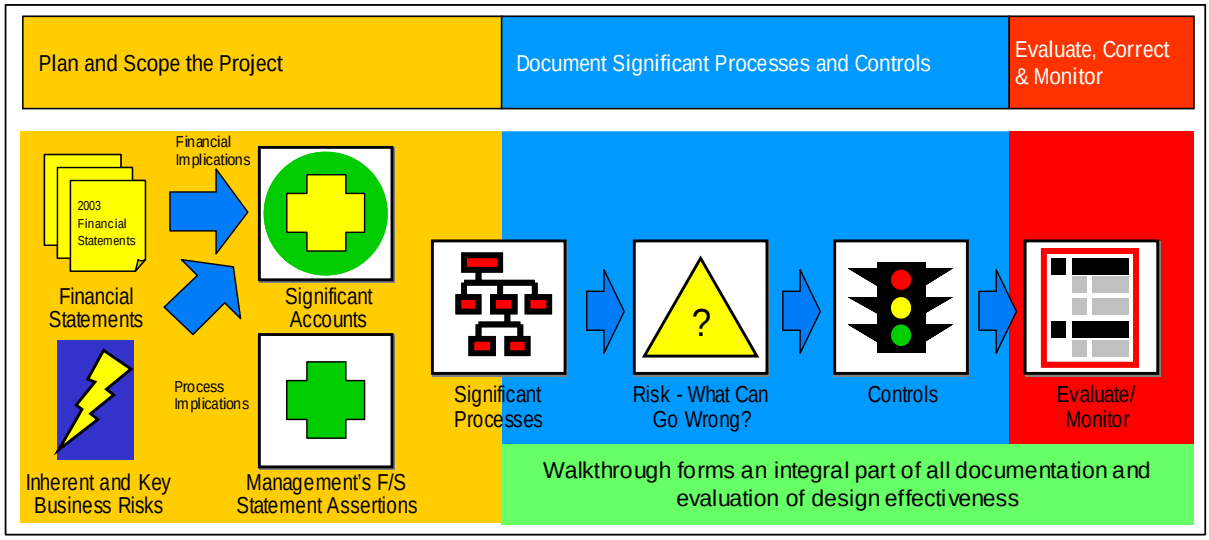

Figura 3 – Metodologia de definição de âmbito

(Fonte: Empresa objecto do caso de estudo)

3.2.2 Definição do Âmbito

3.2.2.1 Enquadramento

É através do processo de definição de âmbito que se identificam quais as empresas e contas do grupo relevantes para o propósito da s404. Este processo requer uma análise da Relevância Financeira de cada um dos vectores identificados na figura 3, bem como do risco de acontecer um erro material. A Relevância Financeira normalmente é definida como uma probabilidade mais que remota de uma conta conter um erro que de forma individual, ou agregado com outros, possa resultar num erro material nas demonstrações financeiras. Neste processo ambos os aspectos qualitativos e quantitativos da materialidade são considerados.

A definição do âmbito do trabalho da s404 inicia-se com a definição dos processos de Negócio Relevantes. De acordo com a metodologia do grupo existiam um conjunto de passos que deveriam ser tidos em consideração.

3.2.2.2 Definição da Materialidade

O conceito de materialidade é definido como a magnitude de uma omissão ou erro de forma individual ou agregada, à luz de determinadas circunstâncias, faça com que a probabilidade do julgamento de uma pessoa razoável que confia nas

Demonstrações financeiras tivesse mudado ou sido influenciado por essa omissão ou erro. Tendo em consideração a definição apresentada e para responder aos requisitos do AS No 2 o Grupo definiu que o seu nível de cobertura das contas associadas ao Reporte Financeiro seria de 70%. Para atingir esse nível de cobertura foi definido um limite para cada uma das empresas, a partir do qual as contas identificadas pelo grupo deveriam ser consideradas dentro de âmbito. No caso de Portugal o limite foi de aproximadamente 37.5 Milhões de Euros.

3.2.2.3 Identificação das Contas Significativas

As contas significativas para o Grupo eram identificadas com base na materialidade, nos factores de risco e na revisão dos relatórios anuais. Após essa identificação as contas eram comunicadas às empresas locais, que de acordo com a materialidade definida para cada uma individualmente, avaliavam se essas contas eram ou não igualmente relevantes localmente.

3.2.2.4 Identificação de Localizações Significativas

Através da alocação de um critério de materialidade pelo Grupo, a definição do âmbito era determinada por cada Empresa local. Este processo era utilizado para identificar o âmbito e a cobertura de cada uma das empresas do grupo e para assegurar a existência de uma cobertura adequada sobre todas as contas e processos relevantes para as demonstrações financeiras do Grupo.

3.2.2.5 Mapeamento das Contas com os Processos

Nesta fase as contas identificadas como significativas eram mapeadas com os Processos de negócio no sentido de se identificar o âmbito de Processos de Negócio da empresa. Este passo era muito importante porque para os processos dentro do âmbito, em linha com as fases descritas atrás (no capítulo anterior), era necessário documentá-los e identificar o gap.

De referir ainda que o âmbito dos processos de negócio, bem como a produção de toda a documentação inerente, reveste-se de uma importância muito significativa para os Sistemas de informação. Como vamos ver mais à frente é com base na informação dos Processos de Negócio que o âmbito dos sistemas de IT é definido.

3.2.2.6 Avaliação do nível de cobertura do Demonstrações Financeira do Grupo

Após todas as empresas do Grupo enviarem a definição local do âmbito para o Grupo, a equipa de projecto revia centralmente toda a documentação no sentido de assegurar que existia uma cobertura adequada na perspectiva do Grupo. Apenas depois desta fase se ter concluído o âmbito dos Processos de Negócio poderia ser considerado final.

3.2.3 Sistema de informação

A definição do âmbito dos Sistemas de informação tinha por base os Processos de Negócio considerados relevantes para efeitos da s404. As principais fases da definição do âmbito são as que se descrevem em seguida, sendo que a figura em baixo é ilustrativa dos vários passos do processo.

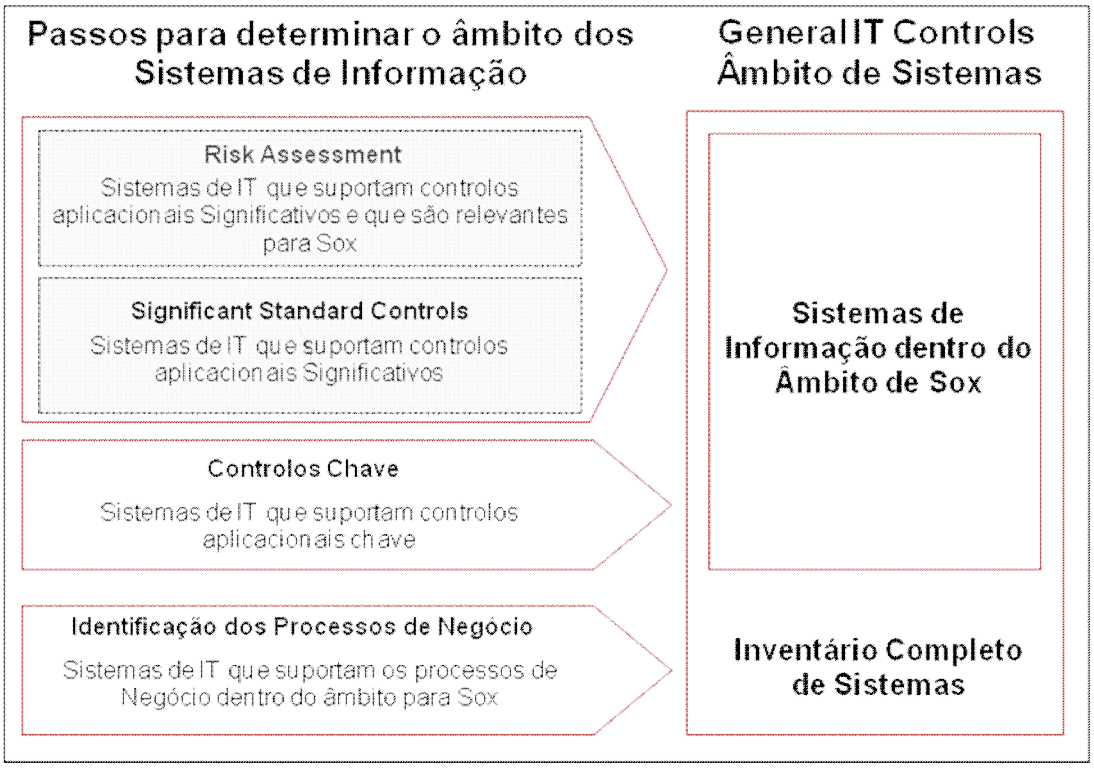

Figura 4 – Metodologia para definição de âmbito de sistemas de informação

(Fonte: Empresa objecto do caso de estudo)

3.2.3.1 Identificação do Inventário de Sistemas

O primeiro passo da definição do âmbito dos Sistemas de Informação era identificar

e documentar no inventário de Sistemas todas as aplicações e infra-estruturas que suportassem controlos aplicacionais mapeados nos processos de negócio relevantes para efeitos da s404. Por norma, esta identificação era realizada através dos fluxogramas e/ou narrativas dos processos de negócio. No entanto, dada a fase embrionária do projecto nem todos os processos relevantes para SOX se encontravam desenhados. Nestes casos havia a necessidade da equipa focada nos Sistemas de Informação se socorrer da de Processos de Negócio para garantir que estava a cobrir todo o espectro de sistemas.

3.2.3.2 Definição do âmbito

Com a conclusão do inventário haviam sido identificados todos os sistemas que suportavam controlos aplicacionais dentro de âmbito dos Processos de negócio. Porém, o racional construído pelo grupo ia um pouco mais longe. Seguindo as linhas orientadoras do PCAOB e as boas práticas de Gestão de Risco, o Grupo decidiu que apenas deveriam ser considerados dentro do âmbito todos sistemas que suportassem controlos chave da organização – controlos que mitigam uma parte substancial do risco. Adicionalmente, deveria ainda ser realizada pelas equipas locais, uma avaliação de risco que considerasse em que medida poderiam existir outros sistemas que, não suportando controlos chave, deveriam igualmente ser considerados. Estes critérios focavam-se essencialmente:

- Se os sistemas suportavam controlos significativos – classificação imediatamente a seguir aos chave;
- No nível de maturidade dos sistemas;
- Na probabilidade desses sistemas passarem a suportar controlos chave e/ou serem necessários para mitigar eventuais deficiências;
- No papel do sistema nos processos de reporte financeiro.

A conclusão desta fase resultou na identificação de 42 sistemas para efeitos de inventário, mas na inclusão de apenas 12 como relevantes para a s404. Os sistemas considerados dentro do âmbito suportavam fundamentalmente os

processos de Reporte Financeiro, de Receita, *Billing* e a Infra-estrutura Core que suportava o negócio da empresa.

3.3 General IT Controls

3.3.1 Introdução

Conforme é referido na revisão bibliográfica, de acordo com as exigências da s404 da Lei *Sarbanes Oxley,* a Gestão deve avaliar a efectividade do ambiente de controlo. Esta deve incluir, entre outros vectores, a documentação dos fluxos de transacções, nomeadamente como estas são iniciadas, autorizadas, registadas, processadas e finalmente reportadas. Na empresa em estudo, estes fluxos de transacções estão incluídos em sistemas aplicacionais que permitem automatizar processos e que processam e suportam elevados/complexos volumes de dados. Para que haja segurança que os controlos aplicacionais utilizados nos Processos de Negócio produzem os efeitos desejados, i.e., operam conforme foram desenhados e que as transacções constantes nos sistemas produzam os efeitos desejados, existem os *General* IT *Controls* (GITC).

Os GITC podem ser definidos como processos e controlos de IT que incidem sobre as aplicações e a infra-estrutura e que têm como objectivo principal garantir a integridades dos sistemas e dos dados. Para que se possa afirmar que os sistemas dentro do âmbito estão a responder aos requisitos da s404, os GITC's que os suportam necessitam de ser avaliados ao nível da Aplicação, Base de dados e Infra-estrutura.

A Equipa de projecto do Grupo em paralelo com as Equipas Locais desenvolveram uma Matriz de Riscos e Controlo baseada nos *Control Objectives for IT – CObIT* – para responder aos requisitos da s404. Esta *framework* focou-se nas seguintes área de controlo:

- *Acquire or Develop Applications and Manage Changes;*
- *Ensure Systems Security;*
- *Manage Operations* (incluí a componente de *Job Scheduling*, *Systems*

Logging e *Incident Management*);

- *Manage Data;*
- *Manage Facilities;*
- *Manage Outsourced Services*;

As próximas secções deste capítulo são dedicadas à apresentação detalhada das várias áreas de controlo enunciadas em cima e à metodologia de avaliação utilizada para aferir a efectividade do ambiente de controlo.

3.3.2 *Framework* de Riscos e Controlos

3.3.2.1 *Acquire or Develop Applications and Manage Changes*

Referências do *CObIT*:

> AI1 – Identificação de Soluções Automatizadas: A necessidade de novas aplicações ou funcionalidades requer uma análise antes da aquisição ou criação, de modo a assegurar que os requisitos do negócio estão satisfeitos através de uma abordagem efectiva e eficiente. Este processo cobre a definição das necessidades, consideração de soluções alternativas, revisão da exequibilidade tecnológica e económica, execução de uma análise de risco, de uma análise de custo/benefício e a conclusão de uma decisão final entre "comprar" ou "fazer". Todos estes passos capacitam as organizações para minimizar o custo de aquisição e implementação de soluções enquanto asseguram que o negócio tem capacidade para atingir os seus objectivos.
>
> AI2 – Aquisição e manutenção de software de aplicações.
>
> As aplicações são disponibilizadas em linha com os requisitos de negócio. Este processo cobre o desenho das aplicações, a inclusão dos controlos aplicacionais, requisitos de segurança apropriados e o desenvolvimento e configuração em linha com os standards. Com isto as organizações conseguem suportar de forma apropriada as operações do negócio com controlos aplicacionais correctos.

AI 3- Aquisição e Manutenção da Infra-estrutura Tecnológica

As Organizações têm processos para a aquisição, implementação e *upgrade* da infra-estrutura tecnológica. Isto requer uma abordagem planeada de aquisição, manutenção e protecção da infra-estrutura, em linha com as estratégias tecnológicas acordadas e de acordo com a preparação dos ambientes de desenvolvimento e teste. Isto assegura que existe um suporte tecnológico programado para as aplicações do negócio.

AI 4 – Estabelecer a capacidade para operar e utilizar

Existe conhecimento disponível sobre os sistemas. Este processo requer a produção de documentação e manuais para os utilizadores de IT e a disponibilização de formação para assegurar uma utilização apropriada das aplicações e infra-estrutura.

AI 6 – Gestão de alterações

Todas as alterações, incluindo as de manutenção de emergência e instalação de *patches*, relacionadas com a infra-estrutura e aplicação dentro dos ambientes de produção são geridas e controladas formalmente. Alterações (incluindo as realizadas a procedimentos, processos, sistemas e parâmetros de serviço) são registados, avaliados e autorizados antes da implementação e revistos face ao inicialmente planeado após a implementação. Deste modo, assegura-se a mitigação dos riscos que possam colocar em causa a estabilidade e integridade do ambiente de produção.

AI7 – Instalar e acreditar as soluções e alterações

Os novos sistemas precisam de ser colocados operacionalmente após concluído o desenvolvimento. Isto requer a realização de testes apropriados, num ambiente dedicado, com dados adequados, definição de instruções de migração e de instalação, planeamento da *release* e instalação para produção e revisões após ter sido implementado em produção. Estas actividades asseguram que os sistemas operacionais estão em linha com as expectativas

acordadas e com os resultados esperados.

Descrição do Risco:

R01 - Alterações não autorizadas ou testadas de forma deficiente nos sistemas podem ter impacto na integridade dos controlos que suportam o reporte financeiro.

Objectivo de controlo

Todas as alterações (aquisições, desenvolvimentos, melhorias realizadas ao sistemas, *upgrades* ou correcções) realizadas a aplicações e infra-estrutura, são autorizadas e devidamente testadas antes de serem transportadas para produção.

Actividades de Controlo Genéricas

C00 – As politicas e procedimentos utilizados para gestão das maiores alterações aos sistemas seguem uma metodologia de desenvolvimento de sistemas que está publicada e comunicada aos utilizadores. A Metodologia cobre aquisições, desenvolvimentos de novos sistemas ou melhorias realizadas nos sistemas. A metodologia de desenvolvimento é revista, actualizada quando necessário e aprovada pela Gestão periodicamente.

C01 – Existem políticas e procedimentos de *Change Management* documentados, actualizados e comunicados aos utilizadores. Estes cobrem aquisições, desenvolvimento de novos sistemas ou melhorias aos sistemas existentes e incluem alterações de emergência.

C02 – Todos os pedidos de alteração são registados e monitorizados num sistema de *tracking* (este pode ser um sistema automático ou registos manuais).

C03 – Todos os pedidos de alteração são devidamente aprovados pelo nível de gestão apropriado (nomeadamente pelo negócio) antes do desenvolvimento.

C04 – O potencial impacto de aquisições/novos desenvolvimentos de sistemas ou melhorias nos actuais sistemas na integridade dos controlos aplicacionais é determinado através de uma análise de risco.

C05 – Existe uma estratégia de testes que foi desenvolvida e aprovada para endereçar as grandes alterações realizadas nos sistemas, aquisições/desenvolvimentos de novos sistemas. Estas têm em consideração os resultados da análise de risco e incluem, entre outros, testes de integração e de aceitação por parte dos utilizadores.

C06 – Sempre que necessário, antes dos sistemas entrarem em produção, todas as alterações realizadas são testadas até ao nível apropriado (em linha com o que foi determinado antes do desenvolvimento) de forma a cobrirem o risco associado ao âmbito da alteração.

C07 – Após ter ocorrido uma revisão e/ou as alterações terem sido testadas, são formalmente autorizadas para serem implementadas no ambiente de produção, pela hierarquia adequada para o efeito (nomeadamente o negócio).

C08 – Ao longo do ciclo de desenvolvimento, existe um nível apropriado de segregação de funções entre desenvolvimento, testes e actividades de implementação.

C09 – Os acessos de pessoas de desenvolvimento a produção é restrito e controlado.

C10 – Alteração de configuração nas aplicações (e.x.: *reference data*) são *autorizadas* pela hierarquia adequada do negócio.

3.3.2.2 Ensure Systems Security

Referências do *CObIT*

DS5 – Assegurar a segurança dos sistemas

A necessidade de manter a integridade da informação e proteger os activos de IT requer a implementação de um processo de gestão de segurança. Este

processo inclui o estabelecimento e manutenção de perfis de segurança de IT, responsabilidades, políticas, standards e procedimentos. A gestão da Segurança também inclui a realização de acções de monitorização, de testes periódicos e da implementação de acções correctivas para as fraquezas ou incidentes de segurança detectados. Um processo de gestão de segurança efectivo protege todos os activos de IT e minimiza o impacto de vulnerabilidades e incidentes no negócio

Descrição do Risco

R02 - Acesso não autorizado aos sistemas e aos dados pode permitir a realização de transacções fraudulentas, maliciosas, ou não intencionadas bem como alteração do desempenho dos sistemas.

Objectivo de controlo

Existem controlos implementados para garantir a segurança dos sistemas e para prevenir a utilização não autorizada, a divulgação de informação, a alteração de dados ou ainda a perda destes.

Actividades de Controlo Genéricas

C11 – Existem políticas e processes relacionados com a gestão de acessos lógicos aos sistemas, sendo que estas estão disponíveis para os utilizadores.

C12 – O acesso a contas de administração e privilegiadas está restrito a um grupo mínimo de utilizadores. Estas contas apenas têm os privilégios suficientes para que os empregados desempenhem as suas funções.

C13 – Existe um processo de concessão, alteração e revogação de acessos às aplicações, bases de dados, sistemas operativos e à rede corporativa. Este processo contempla no mínimo os seguintes passos:

- Aprovação de um nível adequado de hierarquia, nomeadamente para garantir que as permissões são as adequadas;
- Todos os pedidos de acesso estão devidamente documentados e

indicam de forma clara o nível de acessos requeridos.

C14 – Quando um utilizador muda de funções os seus acessos são revistos (e corrigidos se necessário) por um nível adequado de gestão, por forma a garantir que os mesmos continuam adequados.

C15 – Existe um mecanismo que despoleta o cancelamento dos acessos quando os colaboradores saem da empresa.

C16 – São realizadas revisões periódicas aos acessos dos colaboradores da empresa, para garantir que os privilégios destes continuam adequados. Esta revisão contempla os seguintes vectores:

- Contas de administração e privilegiadas;
- Segregação de Funções;
- Acessos remotos à empresa;
- Entidades externas.

C17 – O acesso de colaboradores de desenvolvimento/manutenção a transacções de negócio na aplicação e aos dados é restrito e monitorizado.

C18 – Existem e estão aprovadas e implementadas Politicas e Configurações mínimas de segurança para as aplicações, base de dados e os sistemas operativos dos sistemas da organização. Estes standards devem incluir como requisitos mínimos:

- Standards para as *passwords*, tais como comprimento, complexidade, alteração forçada após um período definido de tempo e histórico de *passwords*;
- Bloqueio da conta após um numero definido de tentativas falhadas;
- Restrição dos utilizadores de administração e de utilizadores com acessos privilegiados;

- Encriptação das *passwords*;
- Parâmetros mínimos de segurança para os sistemas operativos;
- *Passwords* de *default* alteradas.

Quando as configurações mínimas de segurança não são passíveis de ser implementadas num sistema devido a restrições tecnológicas e/ou organizacionais, existem medidas compensatórias implementadas para mitigar o risco residual.

C19 – Existe um processo implementado para rever periodicamente as configurações mínimas de segurança.

C20 – Os acessos dos fornecedores aos sistemas é controlado e monitorizado.

C21 – A Topologia de rede implementada permite segregar os troços de rede onde se encontram os utilizadores finais do referente aos sistemas e estes dois da Internet. Este nível de segurança pode ser obtido, por exemplo, através da implementação de *routers* e *firewalls* que filtrem o tráfego de comunicações e apenas deixem passar o autorizado.

C22 – Existe software implementado para prevenir e detectar ataques de" *malware*" (vírus, *trojan-horse*, *worms*, etc) e estão implementados procedimentos que garantam que as definições deste software estão actualizadas.

3.3.2.3 *Manage Operations* (inclui a componente de *Job Scheduling*, *Systems Logging* e *Incident Management*);

Referências do CObIT

DS13 – Gestão das Operações

Um processamento completo e preciso dos dados requer uma gestão efectiva dos dados processados e uma manutenção diligente do hardware. Este processo inclui a definição de politicas e procedimentos de operações para estabelecer uma gestão efectiva dos *schedullers* que processam, protegem

resultados sensíveis, monitorizam o desempenho da infra-estrutura e asseguram a manutenção preventiva do hardware. Uma gestão efectiva das operações ajuda a manter a integridade dos dados e reduz o atraso do negócio e os custos das operações de IT.

Descrição do Risco

R03 - Se a gestão das operações falhar e/ou tiver problemas o processamento dos dados financeiros pode não ficar completo e/ou preciso.

Objectivo de controlo

Existem procedimentos operacionais implementados que garantam que o *Schedulle* de *Jobs* está controlado, é monitorizado e que caso ocorra algum incidente o mesmo é identificado, escalado e monitorizado até ser resolvido.

Actividades de Controlo Genéricas

C23 – Existem Políticas e Processos de gestão de operações documentados, actualizados e revistos periodicamente pela Gestão, que explicam como o Schedule dos *Jobs* é definido e como as alterações ou remoções do *scheduller* são autorizadas. Estas Políticas e Processos foram implementados e são seguidos para os *Jobs* existentes e para que as alterações a estes sejam devidamente autorizadas e documentadas, evidenciando a resolução quando há remoções do *Scheduller*.

C24 – Existem Políticas e Processos de gestão de operações documentados, actualizados e revistos periodicamente pela Gestão, que explicam como a monitorização de processos importantes de *Batch* é realizada e como as falhas são identificadas e solucionadas. Estas Políticas e Processos foram implementados e são seguidos para que exista uma monitorização com acções para resolver as falhas ocorridas durante o processamento.

C25 – Existem Políticas e Processos relacionados com a gestão das operações documentados, actualizados e revistos periodicamente pela Gestão, que definem como os Problemas e Incidentes devem ser identificados,

definidos em termos de prioridade e escalados até ficarem resolvidos em definitivo. Estas Políticas e Processos foram implementados e são seguidos para que exista uma monitorização com acções para resolver as falhas ocorridas durante o processamento.

C26 – Existem procedimentos implementados para obter e aplicar periodicamente *paches* e *upgrades* relacionados com a segurança dos sistemas.

C27 – Estão identificados e definidos nos sistemas os eventos e logs de segurança apropriados. Estes são revistos periodicamente tendo em vista a identificação de excepções, que devem ser investigadas e escaladas sempre que necessário.

3.3.2.4 *Manage Data*

Referências do *CObIT*

DS11 – Gestão dos dados.

Uma gestão efectiva dos dados requer que se identifiquem os requisitos dos dados. Os processo de gestão dos dados também inclui a estabelecimento de procedimentos efectivos para gerir o arquivo dos *media*, *backups* e recuperação de dados e ainda uma adequada utilização dos *media*. Um processo de gestão de dados efectivo ajuda a assegurar a qualidade e disponibilidade atempada dos dados para o negócio.

Descrição do Risco

R04 - No caso de ocorrer um desastre ou uma catástrofe a informação critica de negócio pode não ser recuperada e reportada.

Objectivo de controlo

Os dados podem ser restaurados de forma completa, precisa e válida, por forma a permitirem um reporte atempado do histórico das transacções financeiras e de outros dados financeiramente relevantes.

Actividades de Controlo Genéricas

C28 – Existe uma Politica e Processos de *Backup* documentados e em operação, com o objectivo de assegurar que toda a informação financeira relevante é armazenada regularmente.

C29 – Os *Backups* são testados periodicamente de forma a garantir que os dados residentes neles estão íntegros.

C30 – Os *Backups* estão devidamente protegidos do risco de perda ou danificação motivada por fogo ou actos maliciosos.

C31 – A execução dos *Backups* é monitorizada de modo a assegurar que eventuais erros são detectados e corrigidos atempadamente.

3.3.2.5 Manage Facilities

Referências do CObIT

DS12 – Gestão do ambiente físico

A protecção dos equipamentos de IT e pessoas envolvidas requer que as instalações sejam bem desenhadas e bem geridas. Este processo de gestão de ambiente físico inclui a definição de requisitos físicos dos *sites*, selecção das instalações correctas e o desenho de um processo para monitorizar os factores ambientais e a gestão dos acessos físicos. A gestão efectiva do ambiente físico reduz as interrupções no negócio devido a estragos nos equipamentos de IT e/ou motivado por pessoas.

Descrição do Risco

R05 - O acesso físico ao hardware pode proporcionar a oportunidade de acesso não autorizado aos sistemas e aos dados.

Objectivo de controlo

O acesso físico aos sistemas é restrito e autorizado a um número mínimo de pessoas, no sentido de minimizar o risco de perca ou danificação das

aplicações ou dados.

Actividades de Controlo Genéricas

C32 – Existe uma Política de Acessos Físicos aos sistemas documentada e actualizada.

C33 – Existem os controlos físicos apropriados (e.x.: barreiras físicas, acessos restritos aos *Data Centers* localizados em edifícios seguros, utilização de cartões de identificação para os visitantes) implementados para restringir os acessos aos sistemas por parte de pessoas não autorizadas.

C34 – Os pedidos de acesso físico aos sistemas estão documentados, indicam claramente o nível de acessos requerido e estão aprovados pelo nível adequado de gestão. Essa aprovação está documentada e armazenada.

C35 – Os acessos físicos são revistos periodicamente, no sentido de garantir que os mesmos continuam adequados.

C36 – Existem controlos ambientais adequados para acautelar a protecção dos sistemas, nomeadamente, detectores de incêndio e humidade e UPS (*uninterruptible power supplies*).

3.3.2.6 *Manage Outsourced Services*

Referências do *CObIT*

DS2 – Definição e gestão dos níveis de serviço

A necessidade de assegurar que os serviços disponibilizados por entidades externas (e.x.: fornecedores, vendedores e parceiros) atingam as metas estabelecidas requer um processo efectivo de gestão. Este processo é conseguido através da definição clara de funções, responsabilidades e expectativas das entidades externa,s bem como através da revisão e monitorização desses acordos tendo em vista a efectividade e a conformidade. A gestão efectiva dos serviços prestados por entidades externas minimiza o risco de negócio associado a fornecedores que não disponibilizam o serviço

acordado.

Descrição do Risco

R06 - Se as entidades externas, que gerem os sistemas, não forem devidamente controladas podem ocorrer acessos não autorizados / alterações não autorizadas que podem resultar na realização de transacções financeiras incompletas ou imprecisas.

Objectivo de controlo

Os níveis de serviço definidos estão em linha com os requisitos do negócio e são periodicamente monitorizados e geridos, de modo a assegurar que o desempenho atinge os objectivos.

Actividades de Controlo Genéricas

C37 – Estão definidos SLA (*service level agreements*) com as entidades externas que operam controlos para a empresa e/ou podem ter influência na integridade dos controlos. Estes SLA's incluem metas definidas para o desempenho e requerem que o fornecedor esteja de acordo com o que a empresa define para os seus diferentes ambientes de controlo.

C38 – Os SLA são geridos e revistos periodicamente contra as metas estabelecidas e face às políticas definidas pela empresa.

3.3.3 As fases de avaliação

3.3.3.1 Documentação dos GITC

Na fase inicial foi necessário efectuar um levantamento da realidade para identificar os estados da organização. Esta fase consistia na realização de entrevistas ou observação da realidade e tinha como objectivo documentar as actividades de controlos (existentes ou não) de forma a responderem aos controlos genéricos, identificados em cima.

No final desta fase, as equipas de projecto das empresas locais tinham um entendimento muito grande sobre a realidade da empresa. Os aspectos críticos de

cada controlo estavam perfeitamente identificados e era possível iniciar a fase de aferição da efectividade do desenho dos controlos existentes.

3.3.3.2 Avaliação da efectividade do desenho dos controlos.

Uma vez concluída a fase acima descrita, a equipa de projecto já tinha o conhecimento suficiente para iniciar a avaliação do desenho dos controlos através da realização de *walkthroughs*. Os *walkthroughs* são considerados os" testes de um" e são realizados utilizando um evento de controlo escolhido aleatoriamente para aferir se todos os pontos do controlo existem efectivamente e se as evidências suportam todos esses vectores do controlo. A documentação do *walkthrough* deve incluir todas a evidências que suportam os vários pontos referenciados no controlo. Estes podem assumir vários formatos, nomeadamente formulários, *templates*, *print screens* e actas de reuniões.

Durante esta fase era igualmente necessário avaliar em que medida existiam diferentes processos para a aplicação e infra-estrutura. Tipicamente as questões que se colocavam eram:

- É a mesma equipa que desempenha as funções para a aplicação e infra-estrutura?
- São utilizadas as mesmas ferramentas de suporte e os mesmos *templates*?
- As actividades de controlo relevantes para a s404 são as mesmas?

Quando existiam dúvidas relativamente à existência de uma única actividade de controlo para os dois *layers* era preciso levar a cabo *walkthroughs* diferentes para confirmar a existência – ou não – de actividades de controlo distintas.

Após a concretização dos *walkthroughs,* a equipa de projecto estava em condições de concluir sobre se as actividades de controlo encontradas no terreno cobriam de facto os pontos de controlo relevantes e se mitigavam os riscos pertinentes para a s404. Os controlos apenas eram considerados efectivos quando todos os pontos do controlo eram cumulativamente atingidos. Os critérios chave para considerar um controlo efectivo eram:

- O controlo mitiga efectivamente os riscos e endereça os objectivos de controlo identificado?
- Por forma a garantir o normal funcionamento operacional é provável que o controlo seja constantemente colocado em causa e não seja efectuado?
- Os membros das equipas executantes dos controlos conhecem as suas funções e sabem que actividades têm de executar?
- É guardada evidência da execução do controlo?
- Os procedimentos de execução dos controlos estão documentados, actualizados e disponíveis aos membros das equipas?

Tendo em consideração as questões focadas acima quando os controlos eram considerados não efectivos havia necessidade de documentar o GAP e de solicitar às equipas envolvidas um plano de remediação para o colmatar.

Quando a equipa de projecto terminou a avaliação do desenho de controlos verificou que a organização apresentava o cenário de maturidade representado na figura 5.

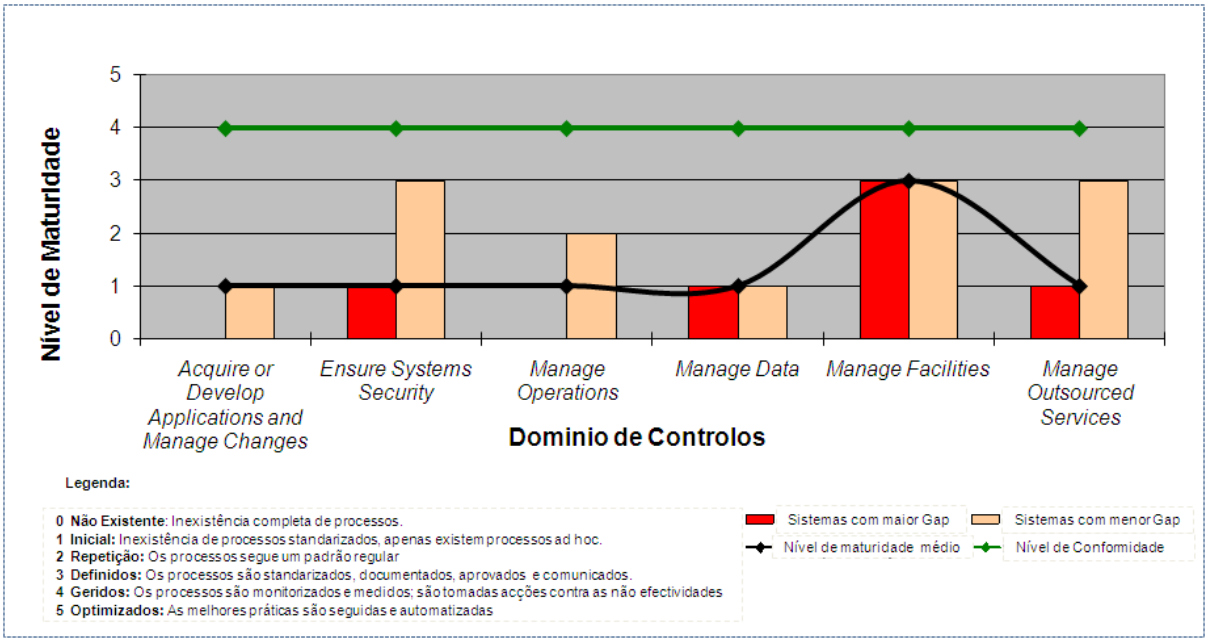

Figura 5 – Nível de maturidade de controlo inicial da organização

(Fonte: Empresa objecto do caso de Estudo

Conforme a descrição na figura, o nível 1 refere que os processos desenvolvidos que eram seguidos pelas pessoas que executam o mesmo tipo de tarefa, mas não existia um processo formal de formação e de comunicação dos standards, a responsabilidade era de cada pessoa individualmente. Existia uma dependência muito grande do conhecimento de cada colaborador para desempenhar as tarefas, por esse motivo a ocorrência de erros tinha uma probabilidade elevada.

3.3.3.3 Monitorização das acções de remediação.

Não obstante o facto deste tema já ter sido referido anteriormente, noutra secção da presente dissertação, importa frisar que era da responsabilidade da Gestão – neste caso delegada na equipa de projecto local – monitorizar o progresso para endereçar as deficiências de controlo identificadas. A equipa local era responsável por monitorizar o progresso e reportar quaisquer atrasos para o Grupo.

3.3.3.4 Testar os controlos operacionalmente

A fase de testes operacionais dos controlos ocorreu após a conclusão da

remediação e teve como objectivo avaliar em que medida os controlos estavam a operar como desenhados. Nesta fase, foi necessário testar operacionalmente todos os GITC que cobrissem os sistemas dentro de âmbito para a s404.

A execução dos testes operacionais focava-se nas áreas que constituíam maior risco para as aplicações, para os processos e para a integridade dos controlos. Apenas os controlos chave foram testados, os *standards* eram avaliados relativamente ao desenho. Caso durante os testes dos controlos se verificasse que algum controlo era operacionalmente não eficaz, era necessário despoletar remediação operacional.

Os GITC que davam suporte aos controlos sobre os processos de reporte financeiro eram considerados os mais críticos e por conseguinte a área de maior risco. Os controlos que suportavam sistemas cujos controlos estavam identificados no inicio da cadeia de transacções eram considerados menos críticos. Reconhecendo este facto, a abordagem de teste foi desenhada para assegurar que pelo menos as áreas de maior risco das aplicações dentro do âmbito eram testadas.

Em linha com a metodologia de *walkthroughs* todas as variantes dos controlos necessitavam de ser testadas. Assim, quando se despoletavam os testes dos controlos era necessário considerar todas as variantes de controlo que se tinham considerado durante a fase de *walkthroughs*.

No final da fase de testes realizada foi feita uma aferição do nível de maturidade da organização tendo em consideração os níveis de maturidade do *CObIT*. Podemos verificar que através da figura abaixo, que após aproximadamente dois anos de projecto, a organização tinha evoluído de uma situação de nível 1 (descrita atrás) para uma de nível 4.

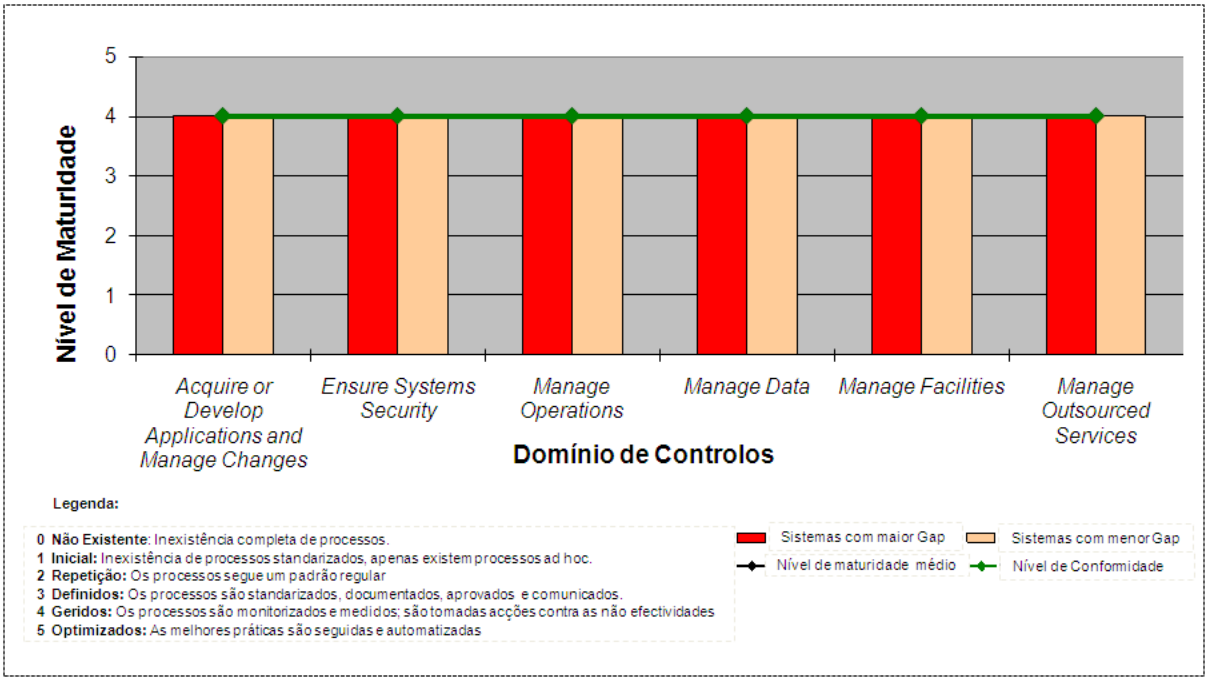

Figura 6 – Nível de maturidade de controlo final da organização

(Fonte: Empresa objecto do caso de estudo)

Atingir este nível significa que a gestão monitoriza e mede os níveis de conformidade com os procedimentos e que toma acções quando os processos não estão a produzir os efeitos esperados. Os processos estão constantemente a ser melhorados e em linha com as boas práticas.

3.4 Business as Usual

3.4.1 Introdução

O presente capítulo da dissertação tem como objectivo dar visibilidade sobre a forma como a transição para *Business as Usual* (BAU) foi abordada pela equipa de projecto.

A representação gráfica apresentada na figura 7 ilustra a visão de longo prazo da equipa de projecto. Após a primeira certificação ter sido alcançada, o foco das actividades da equipa deveria evoluir necessariamente para um estágio diferente, i.e., a conformidade com a s404 deveria ser percepcionada pela empresa como um resultado natural da sua actividade, não como uma obrigação legal. Por este motivo, era necessário, desde cedo, colocar no terreno um conjunto de acções que

potenciassem a equipa de projecto para outro patamar.

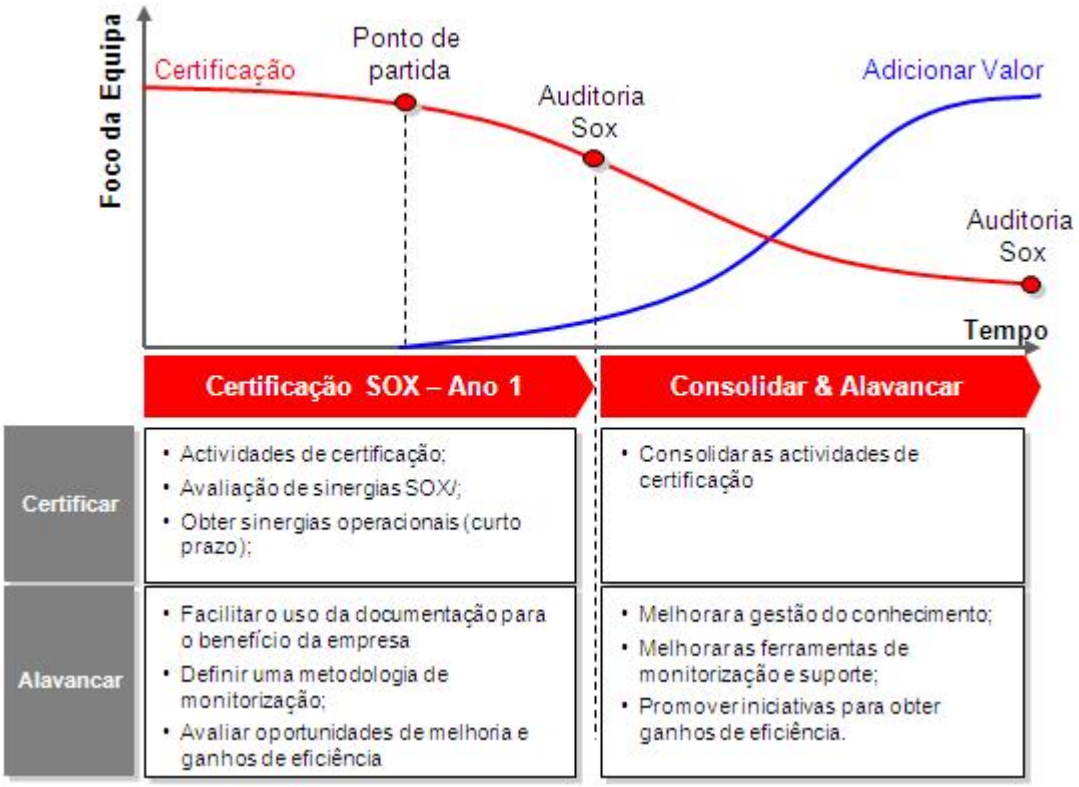

Figura 7 – Objectivos do projecto de *Business as Usual*

(Fonte: Empresa objecto do caso de estudo)

A organização endereçou este desafio consubstanciando-se no seguinte:

- Definição de um Modelo de Governo que explicasse o que deveria ser feito em cada situação, e quais as responsabilidades de cada um dos intervenientes;
- Adopção de uma estratégia de monitorização que permitisse controlar a evolução dos riscos associados à certificação.

3.4.2 «Modelo de Governo

A estrutura do modelo de governo era composta por dois vectores distintos, um relacionado com a definição dos processos de BAU, cujo objectivo era esclarecer

"como" a organização respondia às diferentes necessidades diárias, outro que definia as responsabilidades e funções de cada um dos intervenientes. Do cruzamento destes dois vectores resultava no Modelo de Governo.

3.4.2.1 Processos de BAU

A tabela seguinte explana os processos de BAU considerados bem como os objectivos definidos para os mesmos.

Processo de BAU	Objectivos
Gerir as Actividades de Negócio Diárias	• Assegurar o desenho dos controlos e a efectividade operacional; • Assegurar que os processos documentados são os seguidos pelas áreas de negócio; • Garantir que as actividades críticas de negócio ficam registadas apropriadamente; • Executar as actividades de controlo e registar as evidências correctas; • Implementar as acções necessárias para atingir os resultados planeados e promover a melhoria contínua; • Acautelar a disponibilidade dos recursos para a execução das actividades; • Nomear o Executante do Controlo e o Controlador do Processo.
Gerir a Mudança	• Definir o desenho do controlo e planear/executar as actividades de remediação do controlo, quando necessário; • Actualizar a documentação do processo e dos controlos

	sempre que for pertinente; • Definir, implementar e registar as acções correctivas e preventivas necessárias.
Gerir a Certificação	• Fazer o *sign-off* anual da documentação de Processo e Controlo; • Definir e executar o plano de *walkthroughs* dos processos e dos controlos; • Definir e executar o plano de testes dos controlos; • Avaliar as alterações dos processos, o desenho e a operacionalidade dos controlos e promover, se necessário, acções de remediação; • Executar a definição de âmbito periódica (processos e sistemas); • Rever e planear periodicamente as actividades relacionadas com a certificação.
Monitorizar	• Monitorizar a efectividade e a eficiência das actividades executadas nas áreas de negócio; • Monitorizar o desenho dos controlos, a efectividade operacional e a eficiência; • Monitorizar a efectividade dos processos relevantes para estrutura de controlo interno; • Monitorizar a efectividade e a eficiência da certificação.

Tabela 1 – Processos de *Business as Usual*

(Fonte: Empresa objecto do caso de estudo)

3.4.2.2 Funções e responsabilidades associadas à certificação

A definição de funções e responsabilidades procurou assentar na forma como a organização está estruturada, não adjudicando mais responsabilidades, mas sim procurando clarificar algumas que, usualmente, não estão tão visíveis. De forma pictórica as funções e responsabilidades podem ser definidas da forma ilustrada na figura 8.

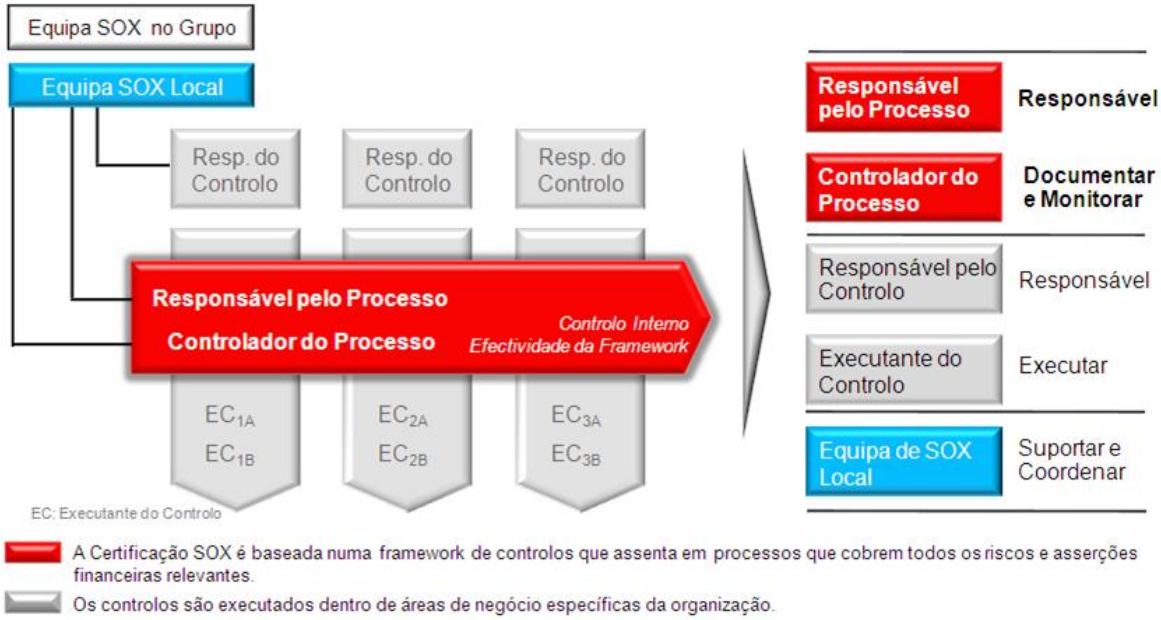

Figura 8 – Modelo de Governo

(Fonte: Empresa objecto do caso de estudo)

Responsável pelo processo

O Responsável pelo Processo é, por norma, um Director cuja área(s) organizacional(ais) tem o maior nível de interacção num determinado processo. As principais responsabilidades desta função são::

- Garantir que os requisitos da s404 estão incorporados em todos os processos/sistemas desenvolvidos e relevantes para SOX;
- Actualizar a documentação (formalização);
- Disponibilizar os recursos necessários para executar os processos e os controlos;

- Assegurar a avaliação do desenho dos processos e controlos sob a sua responsabilidade;
- Acautelar o desenho e a operacionalidade dos controlos;
- Validar anualmente, através da aprovação, que os processos estão documentados de forma precisa e que foram realizados os testes suficientes para garantir que o desenho e a operacionalidade dos controlos está certificada;
- Nomear os Controladores de Processo sob a sua responsabilidade;

Controlador do Processo

Dado que o Responsável pelo Processo é, por norma, um Director, não é exigível que este tome a execução de determinadas tarefas. Por esse motivo, foi criada a figura do Controlador do Processo. Esta função é extremamente exigente, na medida em que assentam nesta pessoa todas (ou quase todas) as responsabilidades de executar as responsabilidades do Responsável pelo Processo. As responsabilidades desta função são:

- Garantir a actualização da documentação de Processo e Controlo;
- Avaliar a efectividade da *framework* de controlos;
- Assegurar a efectividade da *framework* de controlo interno;

Responsável pelo Controlo

Em linha com o que sucede com o Responsável pelo Processo, o Responsável pelo Controlo é igualmente o Director que tem uma responsabilidade sobre uma determinada área da organização. O facto de existirem dois directores nestes dois vectores promove a resolução de conflitos entre áreas. Assim, quando existe um problema dentro da mesma área o Director dessa área soluciona, quando é entre áreas diferentes existe uma relação de pares que evita o conflito. As principais responsabilidades desta função são:

- Acautelar que os controlos internos executados na(s) sua(s) área(s) estão efectivos;
- Caso os controlos fiquem não efectivos, o Responsável pelo Controlo deve assegurar a sua remediação e se aplicável substitui-lo. Deve, igualmente, notificar o Responsável pelo Processo;
- Responsável pela nomeação dos executantes de controlo;

Executante do Controlo

O executante do controlo não é obrigatoriamente o colaborador que executa o controlo, podendo ser a pessoa que garante que determinada tarefa é executada. As suas tarefas principais podem definir-se da seguinte forma:

- Garante a execução dos controlos e a sua efectividade;
- Guarda a evidência da execução dos controlos num determinado período, conforme descrito na descrição do controlo;
- Caso o controlo fique não eficaz (não ser possível executar ou não aplicável), a situação deve ser formalmente comunicada por este ao Responsável pelo Controlo e ao Controlador do Processo.

Equipa de SOX Local

A equipa de SOX Local assume o papel de coordenação e de suporte da certificação, assegurando que a certificação é mantida de forma robusta. A sua actividade tem as seguintes responsabilidades:

- Monitorizar a efectividade da certificação como um todo;
- Suportar todos os envolvidos na certificação;
- Suportar os Responsáveis dos Controlos e dos Processos nas actividades de documentação;
- Monitorar a qualidade e a precisão da documentação de processo;

- Supervisionar a aplicação da metodologia de documentação de processo;
- Assegurar a revisão periódica de acções com os Controladores de Processo e Executantes do Controlo;
- Comunicar regularmente à Equipa de SOX, ao IT e à Auditoria Interna Global;
- Reportar localmente ao CFO.

3.4.3 Estratégia de monitorização

A definição dos Processos de BAU e das Funções e Responsabilidades associadas à certificação da s404 representaram, sem dúvida, um passo muito importante na concretização e no *rollout* do projecto para BAU. Contudo, esta definição não era suficiente, sendo preciso garantir que tudo o que estava (ou tinha sido) a ser implementado no terreno tinha continuidade, que os colaboradores não viam a certificação como um projecto cuja conclusão dependia do alcançar da primeira meta. Era fundamental garantir que a organização continuava alerta de forma ininterrupta. Por este motivo, foi despoletada uma iniciativa de monitorização da certificação que tinha os seguintes objectivos:

- Detectar as deficiências de forma atempada com impacto na certificação e promover a sua resolução atempada;
- Identificar a oportunidade de melhoria e promover as respectivas acções de implementação.

3.4.3.1 Metodologia de monitorização

A metodologia de monitorização assentava em quatro princípios básicos:

- Focos nas dimensões essenciais para a certificação SOX;
- Análise critica do nível de risco e maturidade de cada um dos elementos;
- Identificação do modelo de monitorização mais eficiente numa perspectiva de custo benefício;

- Planeamento detalhado das actividades de monitorização.

Com a excepção do último ponto, cujo foco reside essencialmente no planeamento das actividades de monitorização, todos os restantes podem ser ilustrados da seguinte forma:

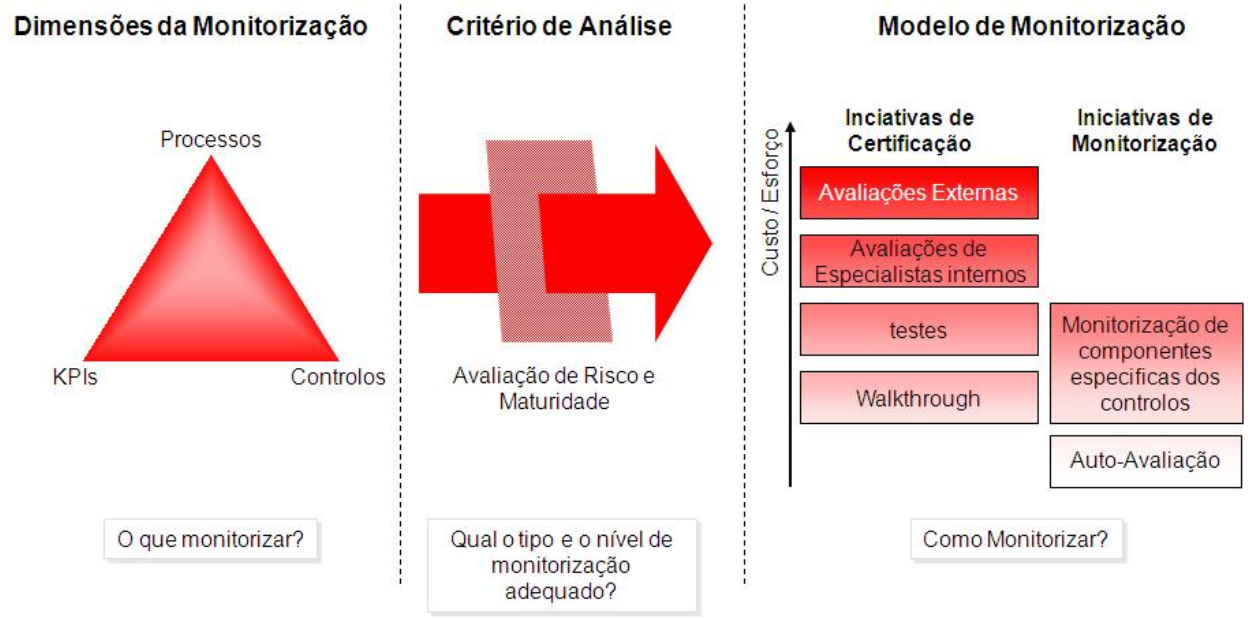

Figura 9 – Estratégia de monitorização

(Fonte: Empresa objecto do caso de estudo)

As secções seguintes explanam cada um dos vectores da estratégia de monitorização adoptada.

3.4.3.2 Dimensões da Monitorização

Key Performance Indicators – KPI's

Os indicadores de desempenho, embora não sejam críticos para a certificação da s404 revestem-se de uma importância muito elevada para a gestão, pois reflectem a forma como a empresa está a funcionar. A análise dos indicadores considerava o seguinte:

- Desempenho relacionado com a disponibilidade e nível de confiança dos dados;

- Se os resultados dos indicadores estavam dentro do nível adequado;
- Como é que os resultados do período corrente se comparam com os períodos passados;

Processos

Os processos são o elemento básico da certificação da s404, pelo que a sua monitorização é critica para garantir a sustentabilidade. A monitorização dos processos endereçava:

- Se a documentação dos processos reflectia a realidade da organização;
- Se o processo tinha um nível adequado de detalhe;
- A existência de um plano para assegurar a actualização do processo.

Controlos

Os controlos são o *core* da *framework* de SOX, sendo que a monitorização contínua da sua efectividade determina o nível de sucesso da certificação. A monitorização dos controlos incidia sobre:

- O controlo está a ser executado conforme está descrito (incluindo todas as características documentadas) e de acordo com a frequência determinada?
- As excepções detectadas pelos controlos estão a ser alvo de acções de acompanhamento?
- Estão a ser registadas as evidências necessárias para suportar a execução dos controlos?

Uma análise integrada destas três dimensões permite focar a atenção no que é efectivamente mais crítico e é fundamental para garantir uma monitorização adequada a todos os níveis.

3.4.3.3 Critério de Análise

A definição do critério de análise foi extremamente importante para definir o nível de monitorização adequado. Foram tidas em consideração as dimensões de análise atrás referidas e ainda um conjunto de *clusters* de análise distintos. A tabela em baixo resume aos critérios de análise.

Cluster	Processos	Controlos	KPI's
Relevância	Âmbito da certificação	Classificação dos controlos: Chave, significativos, standard	KPI's incluídos no sistema de gestão da empresas
Fiabilidade	Consistência da documentação	Última remediação (desenho dos controlos ou operacionalidade)	Precisão e disponibilização atempada dos dados
Estabilidade	Probabilidade de alteração	Nível de automatização	Nível de automatização da fonte dos dados, da colecção dos mesmos e da sua agregação
Maturidade	Antiguidade do processo	Antiguidade do controlo	Antiguidade do KPI
Frequência	Frequência da classe de transacção	Frequência de execução	Frequência de cálculo
Responsáveis	Nível de envolvimento do controlador do	Nível de conhecimento dos executantes dos	Nível de envolvimento do controlador do

	processo, conhecimento e nível de autonomia	controlos	processo, conhecimento e nível de autonomia
Efectividade do Desenho	Os processos são seguidos	Os controlos são executados conforme está descrito vão ao encontro dos objectivos de controlo	Razoabilidade do KPI
Operacionalidade	As actividades são executadas de forma recorrente em todas as ocorrências	As evidências de execução são as adequadas e são guardadas durante o período adequado de tempo	Os KPI's são calculados atempadamente e revisto contra os objectivos definidos.

Tabela 2 – Critério de análise da monitorização

(Fonte: Empresa objecto do caso de estudo)

3.4.3.4 Modelo de monitorização

Consoante o resultado obtido após a aplicação do critério de análise, definido atrás, a incidência e tipo de actividades de monitorização difere. A estratégia de monitorização não é algo estanque que se defina e depois aplique de forma indiscriminada ao longo do tempo, sendo preciso refinar a estratégia até atingir o ponto óptimo e depois continuar a aplicar o critério para assegurar que o mesmo continua nesse estádio.

O modelo de monitorização definido para a organização em estudo assentou em dois pontos fundamentais: o aumento da frequência e/ou o âmbito da aplicação das iniciativas relevantes para a certificação – já descritas no capítulos anteriores – e a

adopção de iniciativas de monitorização, nomeadamente:

- **Monitorização de componentes específicas dos controlos** – Os controlos são compostos por várias características ou atributos. Embora os controlos sejam vistos como um todo, a probabilidade destes falharem está profundamente ligada ao risco de cada um dos atributos falhar. Um controlo pode estar não eficaz ou correr o risco de vir a estar não eficaz, apenas porque um determinado atributo não está a ser executado ou está a sê-lo de forma ineficiente. Este tipo de monitorização é semelhante a um teste (nomeadamente no que diz respeito à dimensão da amostra e executantes), mas proporciona uma monitorização focada nos aspectos críticos dos controlos, potenciando uma identificação atempada de controlos ineficazes. Foi utilizado nas zonas que apresentavam um maior risco para a certificação. A figura 10 ilustra este tipo de estratégia quando comparada com as actividades normais relevantes para a certificação.

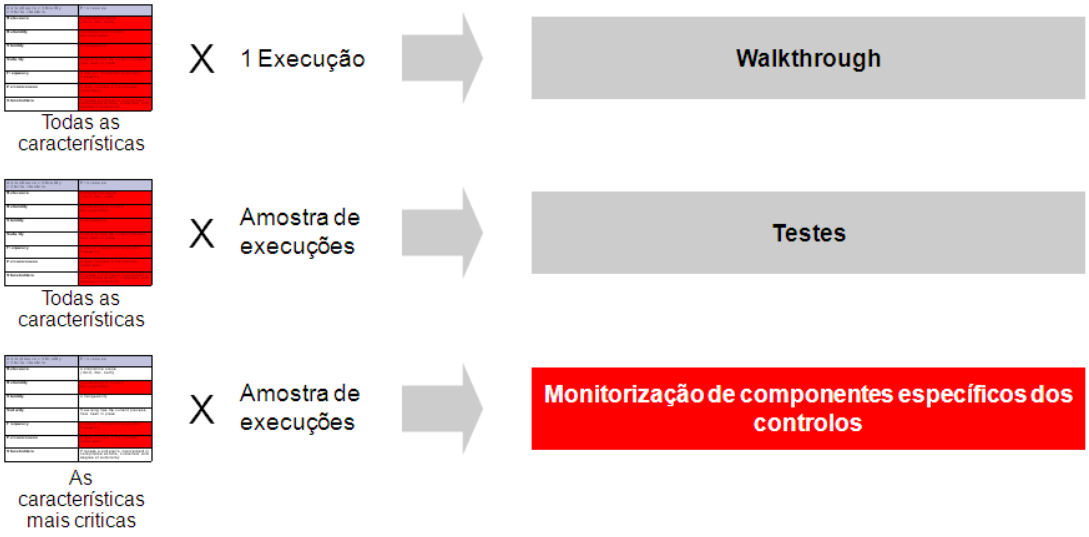

Figura 10 – Monitorização de componentes específicos dos controlos

(Fonte: Empresa Objecto do caso de estudo)

- **Autoavaliação** – Este tipo de iniciativa tem por base a elaboração de um questionário, com perguntas cirúrgicas sobre as actividades relevantes para a certificação, que depois é enviado para as áreas organizacionais responderem. A autoavaliação alerta a organização para as actividades

relevantes para a certificação e disponibiliza, à equipa que gere a certificação, informação actualizada sobre a forma como a organização percepciona os Processos, Controlos e KPI's e acerca da execução dos controlos propriamente dita.

3.4.3.5 Resultados da Monitorização

A aplicação da estratégia de monitorização na organização em estudo produziu dois resultados distintos, a identificação de deficiências e de oportunidades de melhoria, agregados pelas três dimensões de análise definidas. A figura 11 descreve de forma sucinta os resultados:

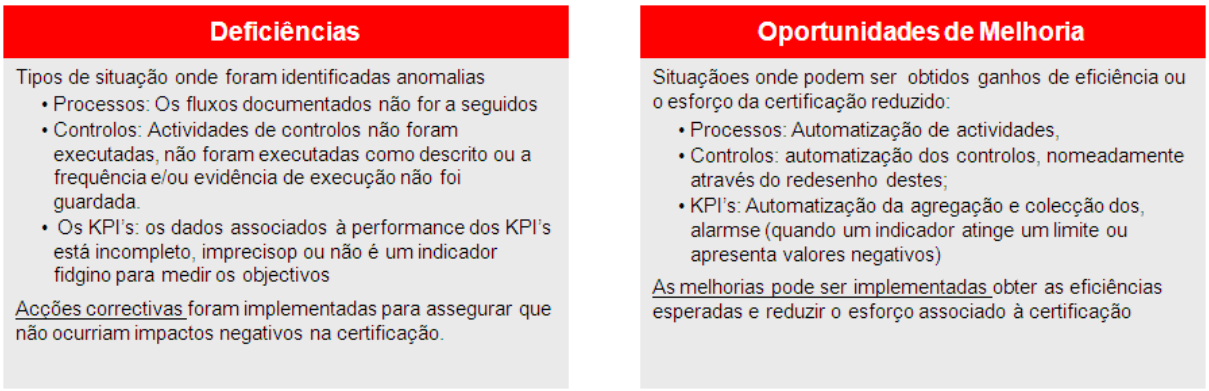

Figura 11 – Resultados da monitorização

(Fonte: Empresa objecto do caso de estudo)

Estes resultados eram partilhados com as áreas organizacionais, através de um portal comum, de modo que estas despoletassem as acções de correcção necessárias e/ou promovessem a implementação de oportunidades de melhoria que visassem o aumento da eficiência e eficácia.

4 Conclusão

4.1 Revisão bibliográfica

O passado recente de algumas organizações trouxe a público um conjunto de práticas fraudulentas levadas a cabo por gestores de renome, reconhecidos pelos *media* e analistas como a "nata" dos executivos de topo. Estas práticas foram dissimuladas pela gestão através de movimentos financeiros ilícitos que contornaram os controlos internos definidos pelas organizações, de forma a permitir tais acções.

A empresa auditora, deveria, na perspectiva do autor, ter detectado as acções ilegais levadas a cabo pela gestão, (a revisão bibliográfica detalha os pormenores). Reconhecidamente, o nível de envolvimento da *Arthur Andersen* com as organizações em estudo, conduziu a problemas de conflito de interesse que levaram à não aplicação dos princípios de auditoria exigidos para empresas daquela dimensão.

A Lei Sarbanes Oxley surge como resposta aos escândalos, relatados na revisão bibliográfica, impondo apertados requisitos de controlo interno sobre o reporte financeiro e cumulativamente responsabilizando a gestão pelo conteúdo deste.

A atribuição de novas responsabilidades à SEC e a criação do PCAOB constituem-se como medidas preventivas, para evitar situações similares às relatadas, pois fomentam um maior equilíbrio entre as organizações e as entidades reguladoras.

Finalmente, o facto da Lei *Sarbanes Oxley* não definir um método ou uma estratégia para atingir a conformidade com os seus requisitos, tem motivado, de uma forma crescente, a adopção de políticas efectivas de Gestão de Risco por parte das organizações. Este tipo de evolução acaba por ser natural, pois potencia um maior alinhamento entre a organização e os seus objectivos e permite responder de uma forma sistemática e cumulativa a todo um conjunto de normativos que as organizações estão actualmente sujeitas.

4.2 Caso de Estudo

Dada a multiplicidade de temáticas abordadas no caso de estudo o autor da dissertação dividiu as conclusões relacionadas com o caso de estudo em cinco blocos distintos:

- Organização e Gestão de Projecto;
- Metodologia adoptada;
- *General IT Controls*;
- *Business as Usual*;
- Principais lições retiradas do Caso de Estudo;

4.2.1 Organização e Gestão de Projecto

A organização do projecto foi de facto um dos vectores mais importantes para o sucesso da iniciativa. A forma como o projecto foi delineado e colocado em prática teve em consideração todas as melhores práticas de gestão de projecto. De forma sucinta, podemos concluir que em termos de organização e gestão de projecto os seguintes pontos contribuíram de uma forma decisiva para o sucesso do mesmo:

- Apoio incondicional da gestão de Topo;
- Constituição de uma equipa de projecto com os *skills* adequados para levar a cabo todas as actividades necessárias;
- Definição de um plano de projecto claro, com *milestones* intermédias e *deliverables* fixados no inicio do mesmo;
- Definição de funções e responsabilidades, bem como dos fóruns de decisão;
- Implementação de uma politica de comunicação com a organização;
- Monitorização regular das *milestones* e *deliverables* definidos.

Em linha com as conclusões do autor da dissertação, Marchetti (2005) defende que para atingir a conformidade com a s404 da Lei Sarbanes Oxley é fundamental

definir em primeira instância um plano de projecto, escolher a equipa adequada para o fazer e constituir órgãos consultivos e/ou decisores para as resoluções mais criticas para o resultado final. A definição de um plano de projecto que contemple etapas intermédias e que permita medir os progressos é igualmente importante para Marchetti, pois apenas deste modo é possível medir o progresso face aos objectivos delineados.

4.2.2 Metodologia Adoptada

A adopção de uma metodologia centrada no risco permitiu à empresa focar-se no essencial. A aplicação de critérios de materialidade permitiu definir *thresholds* que serviram como filtro para a definição do âmbito da s404 (Processo de Negócio e de GITC). Os critérios de relevância financeira, levaram a que apenas os processos críticos da organização fossem seleccionados como relevantes para a s404 e, por conseguinte, a lista de sistemas relevantes foi reduzida ao mínimo (o racional de definição dos âmbito dos sistemas de informação está explicado em cima no caso de estudo).

4.2.3 *General IT Controls*

A definição de uma *framework* genérica de riscos e controlos, baseada nas melhores práticas do mercado (nomeadamente o *CObIT*), permitiu em primeira instância avaliar com acuidade o nível de maturidade do controlo interno relacionado com os SI e definir, numa segunda fase, de forma sistemática e consistente um plano para colmatar as lacunas encontradas.

A *framework* de controlos genérica facilita, igualmente, o processo de documentação e avaliação do nível de maturidade de controlo interno da organização, na medida em que disponibiliza linhas orientadoras para avaliar o desenho e a operacionalidade dos controlos.

A avaliação do desenho e da operacionalidade dos controlos em momentos diferentes possibilita a identificação de eventuais problemas conceptuais de desenho dos controlos antecipadamente, despistando problemas nos controlos chave que suportam os processos de reporte financeiro aquando dos testes

operacionais.

4.2.4 *Business as Usual*

A transição para BAU revestiu-se de uma importância muito grande, pois permitiu clarificar juntos dos principais responsáveis da organização o que era necessário acautelar após terminada a fase de projecto. Para o efeito, a criação de um modelo de governo com uma definição clara de responsabilidades e funções e de processos que explicam como as actividades a serem levadas a cabo, potenciou a absorção das temáticas em causa pela organização.

A monitorização da certificação é sem sombra de dúvidas fundamental para garantir que a organização continua alerta, de forma contínua, para os eventuais problemas que possam aparecer no dia a dia. A execução dos *walkthroughs* e dos testes periódicos para avaliar a conformidade dos controlos não é suficiente para manter uma certificação sustentada, sendo necessário investir activamente numa monitorização, definindo, com critério, o que se vai monitorar no sentido de ser o mais abrangente e eficaz possível.

Anand (2006) defende que a qualidade e a eficácia dos processos/controlos de uma organização depende essencialmente do nível de monitorização a que estes são sujeitos. Se os processos/controlos estiverem constantemente a ser avaliados e monitorizados, a organização consegue detectar eventuais problemas atempadamente e reagir e/ou modificar os processos/controlos em vigor no sentido de os tornar mais eficientes e robustos. Não obstante o facto de, numa fase inicial, este processo poder ser reactivo, o mesmo deve evoluir para um estádio de integração com os restantes processos da organização.

4.2.5 Principais lições retiradas do Caso de Estudo

Alinhado com o descrito no caso de estudo e com as conclusões enunciadas atrás, o autor da dissertação considera pertinente enaltecer aquelas que, no seu entender, constituem boas práticas a seguir em futuros projectos semelhantes. Os quatro pontos seguintes não são exaustivos, mas sintetizam as principais aprendizagens constantes no caso de estudo apresentado:

- Constituição de uma equipa de projecto dedicada única e exclusivamente em atingir a conformidade com a s404;
- Definir com clareza e precisão o âmbito do trabalho;
- Comunicar e envolver a organização na prossecução dos objectivos do projecto, transmitindo um sentimento de pertença;
- Garantir a sustentabilidade da certificação através do desenvolvimento de um Modelo de Governo e da adopção de uma estratégia de monitorização.

4.3 Limitações de Dissertação

A limitação temporal imposta para a realização da presente dissertação, aliada à abrangência do tema escolhido, fez com que a revisão bibliográfica não fosse mais exaustiva e que apenas os temas principais sobre a empresa em estudo fossem apresentados.

O facto da revisão bibliográfica e o caso de estudo não incidirem demasiado em componentes técnicas, limita a partilha de potenciais conclusões e melhores práticas relativamente a temas específicos, nomeadamente de cariz tecnológico.

Por fim, a impossibilidade de partilhar o nome da empresa em estudo e respectivo sector de actividade, restringe a realização de um *benchmark* com a indústria ao nível de maturidade de controlo interno.

4.4 Propostas para investigações futuras

Alinhado com as limitações apresentadas em cima e com o facto dos objectivos do presente trabalho serem abrangentes, o autor considera que existe espaço para dissecar alguns dos temas apresentados, bem como desenvolver outros relacionados.

Seria interessante pegar nos vários temas apresentados nos casos de estudo e aprofundá-los, explorando as componentes técnicas, organizacionais e sociológicas associadas às mudanças que um projecto semelhante ao apresentado requer.

Igualmente motivador, será explorar a forma como as empresas sujeitas ao normativo consolidaram os requisitos implementados durante o ano 1 da certificação e de que forma a sustentabilidade da mesma foi desenvolvida e sustentada, nomeadamente com o aparecimento do *Auditing Standard* Nº5. Que impacto estas mudanças têm nas metodologias adoptadas no ano 1 e de forma é que as organizações reagiram.

Finalmente, e na perspectiva do autor, aquele que constitui o maior desafio, desenvolver uma metodologia consolidada de *Enterprise Risk Management*, que permita sem esforços adicionais, responder não só aos requisitos da Lei *Sarbanes Oxley*, como também a todos os normativos a que as organizações actualmente estão sujeitas.

Bibliografia

Anand, Sanjay (2006), *Sarbanes Oxley Guide for Finance and Information Technology Professionals*, Hoboken, New Jersey: Jonh Wiley & Son, Inc.

Bainbridge, Stephen M., *The Complete Guide to Sarbanes-Oxley*

Beresford Dennis R., Katzenbach Nicholas deB. e Rogers, C.B. Jr., *REPORT OF INVESTIGATION BY THE SPECIAL INVESTIGATIVE COMMITTEE OF THE BOARD OF DIRECTORS OF WORLDCOM, INC.*

Billing, Michael e Evans, Kristen (2005), *A Sarbanes-Oxley road map: Improving real estate data, dialogue and decision making in support of good corporate governance*, Journal of Corporate Real Estate, 7, 1, pp. 23-33.

Buyer, Martha (2005), *Keep Your SOX On: Managing Compliance*, Business Communications Review, 35, 9, pp.17-19.

Charan, Ram e Useem, Jerry (2002), *Why companies fail*, Fortune, Vol. 145, Num. 11; pp. 50-58.

CobIT Framework, *Control Objectives, Management Guidelines, Maturity Models*, Edition 4.1, IT Governance Institute, USA, 2007

Cunningham, Colleen (2006), *The Enron Trial and Its Link to Sarbanes-Oxley, Financial Executive*, 22, 2, pag. 6.

Gramling, Audrey A.e Hermanson, Dana R. (2007), *THE SEC'S PROPOSED GUIDANCE FOR MANAGEMENT'S ASSESSMENT OF INTERNAL CONTROL*, Internal Auditing, 22, 2, pp. 38-41

Green, Scott (2004), *Manager's Guide to the Sarbanes Oxley Act*, Hoboken, New Jersey: Jonh Wiley & Son, Inc.

Harrast Steven A. e Mason-Olsen, Lori (2007), *Can Audit Committeees Prevent Management Fraud?*, The CPA Journal, 77, 1, pp. 24-27.

Healy, Paul M e Palepu, Krishna G (2003), *The Fall of Enron*, The Journal of Economic Perspectives, 17, 2, pp. 3-26.

http://www.sec.gov/about/whatwedo.shtml, (acedido em 29.05.2007)

Juras, Paul E., Martin, Dale R. e Aldhizer III, George R. (2007), *Adapting Six Sigma to Help Tame the SOX 404 Compliance Beast*, Strategic Finance, 88, 9, pp. 36-41.

Kinaga, Patricia A. (2006), *Sarbanes-Oxley and Whistleblowers: What Happens When Employees Bring Retaliation Claims?,* Employee Relations Law Journal, 32, 1, pp. 39-46.

Kranacher, Mary-Jo (2006), *Whistleblowing: The Devil is in the Details*, The CPA Journal, 76, 7, pag. 80.

Lander, Guy P. (2004), *What is Sarbanes Oxley?*, New York: McGraw-Hill.

Levinsohn, Alan (2003), *WorldCom reforms trump Sarbanes-Oxley*, Strategic Finance, 85, 5, 2003, pp. 61-62.

Lipman, Frederick D. (2006), *TEN Best Practices For Audit Committeees*, Financial Executive, 22, 8, pp. 49-51.

Marchetti, Anne M. (2005), *Beyond Sarbanes-Oxley Compliance*, New Jersey: Jonh Wiley & Son, Inc.

Mehta, Stephanie N. (2001), *Can Bernie bounce back?*, Fortune, Vol. 143, Num. 2; pp. 84-88.

Pandit, Ganesh M., Subrahmanyam, Vijaya e Conway, Grace M. (2005), *Audit Committee Reports Before and After Sarbanes-Oxley*, The CPA Journal, 75, 10, pp. 42-44.

Paul, Jack W. (2005), *Exploring PCAOB Auditing Standard 2: Audits of Internal Control*, The CPA Journal, 75, 5, pp. 22-27.

Public Company Accounting Oversight Board Strategic Plan 2007 - 2012

Raiborn, Cecily e Schorg, Chandra (2004), *The Sarbanes-Oxley Act of 2002: An Analysis of and Comments on the Accounting-Related Provisions*, Journal of Business and Management, 10, 1, pp. 1-13.

Rieger, John R. (2006), *Auditor Independence Checklist*, AFP Exchange, pp. 18-19.

Roth, James (2007), *MYTH vs. REALITY: Sarbanes-Oxley and ERM*, The Internal Auditor, 64, 2, pp. 55-61.

SARBANES-OXLEY ACT OF 2002 (2002), United States of America Congress (2nd Session, 25-02-2002)

Sherman, Scott (2002), *Enron: Uncovering the uncovered story*, Columbia Journalism Review, 40,6, pp. 22-28.

THORNBURGH, DICK, UNITED STATES BANKRUPTCY COURT SOUTHERN DISTRICT OF NEW YORK In re: *WORLDCOM*, INC., et al.

Welytok, Jill G. (2006), *Sarbanes Oxley for Dummies*, Indianapolis: Wiley Publishing, Inc.

Wright, Bob (2002), *Restoring trust: The work of America*, Vital Speeches of the Day, 69, 5, pp.150-152.

Wright, Carl N., Booker, Quinton (2005), *Auditors' Need for a Cooling-off Period*, The CPA Journal 75, 12, pp. 24-29.

Zekany, Kay E., Braun; Braun, Lucas W. e Warder, Zachary T. (2004), *Issues in Accounting Education*, 19, 1, pp. 101-117.

Zimmermann, Susan E. e Thompson, Michelle L. (2006), *SOX COMPLIANCE: DCAA Disclosure and Cost-Control Strategies*, Contract Management, 46, 6, pp. 32-35.