

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



ISCAL

ANÁLISE DOS COMPONENTES DE
CONTROLO INTERNO DO MODELO
COSO - ESTUDO DO CASO NA
EDP – ENERGIAS DE PORTUGAL

Ana Margarida Marta de Paiva Amaro (20140189)

Lisboa, outubro de 2016

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

ANÁLISE DOS COMPONENTES DE
CONTROLO INTERNO DO MODELO
COSO - ESTUDO DO CASO NA
EDP – ENERGIAS DE PORTUGAL

Ana Margarida Marta de Paiva Amaro (20140189)

Proposta de dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica de Mestre Ana Isabel Marinho Pires, professora da área científica de Riscos Empresariais e de Controlo Interno.

Lisboa, outubro de 2016

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas. Mais acrescento que tenho consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

Dedicatória

Quero agradecer o apoio da minha família que sempre esteve presente, em especial aos meus irmãos, à Catarina e ao Luis pela paciência e pelo tempo que não pude estar com eles.

Aos meus pais agradeço a força, o incentivo e o apoio ilimitado.

À Nana e à Alexandra pela amizade incondicional e pelo apoio que sempre me deram. A vós também vos peço desculpa, pelo fato de por vezes não poder estar presente ao longo deste ano.

Aos colegas do mestrado que me têm vindo a acompanhar desde o início, pela amizade e companheirismo.

Aos amigos, que por vezes não pude estar presente, mas sempre foram compreensivos.

Agradecimentos

Desde já agradecer à Prof.^a Ana Marinho Pires, por ter aceite este desafio comigo.

Um especial agradecimento à Dr.^a Ester Carvalho, por ter embarcado neste projeto e sempre que foi solicitada a sua ajuda este sempre presente.

Um obrigado enorme às minhas chefias hierárquicas e colegas do trabalho, por terem sido compreensivos, por sempre me terem apoiado e, acima de tudo, motivado.

Resumo

De uma forma geral, todas as empresas devem deter de um sistema de controlo interno, sendo a grande questão a sua adequação face à organização. Uma adequada implementação deste sistema confere uma das melhores defesas contra o insucesso do negócio e um forte condutor do desempenho do mesmo. A avaliação deste sistema, integrada no componente monitorização e geralmente a cargo da auditoria interna, revela-se ser cada vez mais importante, porquanto concorre para a determinação da sua eficácia.

O enfoque do estudo será no controlo interno, atendendo à relevância que assume enquanto componente da gestão empresarial e por materializar o que é necessário a uma organização para que atinja os seus objetivos.

O objetivo principal da dissertação é apresentar uma visão clara e concreta desta problemática, fazendo um estudo aprofundado do modelo COSO, nomeadamente dos seus componentes.

Assim, para a aproximação com o real, a metodologia a ser utilizada é o estudo de caso, onde se irão realizar entrevistas e questionários, procedendo-se à sua análise e avaliação.

Neste âmbito, será realizada uma análise da consubstanciação de cada um dos componentes do modelo COSO no Sistema de Controlo Interno do Grupo EDP.

Palavras-Chave: Controlo Interno, COSO - *Committee of Sponsoring Organizations of the Treadway Commission*, Auditoria Interna, Risco de Auditoria

Abstract

In a general way, all companies must have an internal control system, being the big question its adequacy to the organization. An adequate implementation of this system gives one of the best defenses against the business failure and a strong indicator of its performance. This systems evaluation, integrated into the monitoring component and usually done by internal audit, proves to be increasingly important, as it contributes to the determination of its effectiveness.

The study will focus on the internal control, being in account that its relevance assumes as a business management component and by materializing what needs to be implemented for an organization to achieve its goals.

The main purpose of this work is to present a clear and concrete vision of this problematic, making a depth study of the COSO model, namely its components.

Therefore, to get closer to the real, the methodology to be used occurs through a case study, where it will take place interviews and questionnaires, proceeding to its analysis and evaluation.

In this context, it will take place a diagnosis of the consubstantiation of each of the components of the COSO model in the Internal Control Systems of the EDP Group.

Keywords: *Internal Control, COSO - Committee of Sponsoring Organizations of the Treadway Commission, Internal Auditing.*

Índice

Índice de quadros e tabelas	<i>x</i>
Índice de figuras.....	<i>xii</i>
Lista de Anexos.....	<i>xiii</i>
Lista de Abreviaturas.....	<i>iv</i>
1. Introdução.....	1
1.1. Enquadramento do tema	1
1.2. Relevância do Estudo.....	2
1.3. Objeto e Objetivo.....	2
1.4. Metodologia e Estrutura.....	3
2. Controlo Interno	5
2.1. Perspetiva Histórica.....	5
2.2. Conceito.....	6
2.3. Objetivos do Controlo Interno	9
2.4. Relatórios e modelos de Controlo Interno	10
2.4.1. Relatório Treadway	10
2.4.2. Modelo COSO	11
2.4.3. Relatório Cadbury	12
2.4.4. Modelo COBIT	13
2.4.5. Relatório Turnbull	14
2.4.6. CoCo	16
2.4.7. SOX Act.....	17
2.5. Tipologia de controlos	18
2.6. Recolha e registo do Sistema de Controlo Interno	19
2.7. Avaliação do Controlo Interno	21
2.8. O Controlo Interno e a Fraude	25
2.9. Limitações do Controlo Interno.....	28
3. Modelo COSO	30
3.1. Origem do modelo	30
3.2. Modelos COSO	31
3.2.1. <i>Internal Control – Interated Framework</i>	32
3.2.1.1. Componentes do modelo COSO	35
3.2.2. Princípios e Áreas de Foco	37
3.2.3. <i>Enterprise Risk Management – Integrated Framework</i>	41
3.3. Eficácia e Eficiência do Controlo Interno.....	44
3.4. Responsabilidades.....	47
4. Auditoria Interna.....	49
4.1. Função do Sistema de Controlo Interno na Auditoria Interna.....	49

4.2.	Atividades de monitorização.....	54
4.3.	Normas internacionais de auditoria interna	55
4.4.	O risco no processo de auditoria interna	58
5.	Estudo Empírico.....	60
5.1.	Enquadramento do Estudo	60
5.2.	Metodologia do Estudo Empírico	60
5.3.	Componentes da análise.....	62
5.3.1.	Caracterização da entidade.....	63
5.3.2.	Modelo de análise	67
5.3.2.1.	Entrevista	67
5.3.2.2.	Questionário	67
5.3.3.	Recolha de Dados.....	68
5.4.	Análise e Tratamento dos Dados.....	68
5.4.1.	Ambiente de Controlo.....	69
5.4.2.	Avaliação de Risco	71
5.4.3.	Atividades de Controlo.....	73
5.4.4.	Informação e Comunicação.....	74
5.4.5.	Atividades de Monitorização.....	76
5.5.	Conclusões	79
	Conclusão.....	82
	Limitações	83
	PROPOSTA PARA FUTURO ESTUDO	83
	Bibliografia	84
	Sites consultados.....	87
	AnexoS.....	88

Índice de quadros e tabelas

Tabela 1 – Cabeçalho da *check-list*

Índice de figuras

Figura 1 – Cubo COBIT

Figura 2 – Triângulo da Fraude

Figura 3 – Estrutura do modelo COSO 1992 e 2013

Figura 4 – Associação das Componentes, Princípios e Nº de Áreas de Foco do Modelo COSO

Figura 5 – Estrutura do modelo COSO – ERM

Figura 6 – Organograma IPPF

Figura 7 – *Branding* da marca EDP

Lista de Anexos

Anexo 1 – Formas de registo do controlo interno

Anexo 2 – Áreas de Foco

Anexo 3 – Organograma DAI

Anexo 4 – Taxonomia dos riscos do Grupo EDP

Anexo 5 – *Check-list* de Controlo Interno

Anexo 6 – Código de Conduta (capa) – Grupo EDP

Anexo 7 – Estrutura Organizacional do Grupo EDP

Anexo 8 – Modelo de Responsabilidades do Sistema de Controlo Interno e do Relato Financeiro (capa) – Grupo EDP

Anexo 9 – Formação dos colaboradores da DAI – Grupo EDP

Anexo 10 – Plataforma de recrutamento – Grupo EDP

Anexo 11 – Manual do Sistema de Controlo Interno e do Relato Financeiro (capa)

Anexo 12 – SCI no Universo do Grupo EDP

Anexo 13 – Modelo das linhas de defesa – Grupo EDP

Anexo 14 – Intranet «edpon» - Grupo EDP

Anexo 15 – Formação SCIRF – Grupo EDP

Anexo 16 – *Regulations on Whistleblowing Procedures* – Grupo EDP

Anexo 17 – Aplicação de Controlo Interno – Grupo EDP

Anexo 18 – Formação iBPMS – Grupo EDP

Lista de Abreviaturas

AAA – *American Accounting Association*

AC – Antes de Cristo

AICPA – *American Institute of Certified Public Accountants*

APPC – Associação Portuguesa de Peritos Contabilistas

AS – *Auditing Standard*

CEO – *Chief Executive Officer*

CFO – *Chief Financial Officer*

CI – Controlo Interno

CICA – *Canadian Institute of Chartered Accountants*

CLC – Certificação Legal de Contas

COBIT – *Control Objectives for Information and related Technology*

COSO – *Committee of Sponsoring Organizations of the Treadway Commission*

DAI – Direção de Auditoria Interna

DC – Depois de Cristo

DF – Demonstração Financeira

DGR – Direção da Gestão do Risco

DRA – Diretriz de Revisão/Auditoria

ECIIA – *European Confederation of Institutes of Internal Auditing*

EDP – Energias de Portugal

EUA – Estados Unidos da América

ERM - *Enterprise Risk Management*

Fed – *Federal Reserve*

FEI – *Financial Executives Institute*

IAASB – *The International Auditing and Assurance Standards Board*

IFAC – *International Federation of Accountants*

IIA – *The Institute of Internal Auditors*

INTOSAI - *The International Organization of Supreme Audit Institutions*

IPAI – Instituto Português de Auditoria Interna

IPPF – *International Professional Practices Framework*

ISA – *International Standard on Auditing*

ISACA – *Information Systems Audit and Control Association*

ISAE – *International Standard on Assurance Engagements*

IT – *Information Technology*

NAA – *National Association of Accountants*

ND – Norma de Desempenho

NI – Norma Interpretativa

NYSE – *New York Stock Exchange*

OROC – Ordem dos Revisores Oficiais de Contas

PCAOB – *Public Company Accounting Oversight Board*

PR – Prática Recomendada

SAP – *Statement on Audit Procedure*

SAS – *Statement on Audit Standards*

SCI – Sistema de Controlo Interno

SCIRF – Sistema de Controlo Interno do Relato Financeiro

SEC – *Security and Exchange Commission*

SOX - Lei Sarbanes-Oxley

TC – Tribunal de Contas

1. INTRODUÇÃO

1.1. ENQUADRAMENTO DO TEMA

Entende-se por controlo interno, segundo a Diretriz de Revisão/Auditoria (DRA) 410, como:

[s]istema de controlo interno" significa todas as políticas e procedimentos (controles internos) adoptados pela gestão de uma entidade que contribuam para a obtenção dos objectivos da gestão de assegurar, tanto quanto praticável, a condução ordenada e eficiente do seu negócio, incluindo a aderência às políticas da gestão, a salvaguarda de activos, a prevenção e detecção de fraude e erros, o rigor e a plenitude dos registos contabilísticos, o cumprimento das leis e regulamentos e a preparação tempestiva de informação financeira credível.

(DRA 410, para. 4)

A definição de controlo interno reflete sobre conceitos fundamentais. O controlo interno é um processo, ou seja, representa um recurso para chegar a um objetivo, numa ou mais categorias. Efetuado por pessoas a todos os níveis da organização e não composto estritamente por políticas. Nele é expectado que providencie uma garantia razoável, não significativamente à sua totalidade.

O COSO (Committee of Sponsoring Organizations of the Treadway Commission), define controlo interno como:

[u]m processo realizado pelo Conselho de Administração, Direção e outros membros da organização com o objetivo de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos:

- Eficácia e eficiência das operações;
- Fiabilidade da informação financeira;
- Cumprimento das leis e normas estabelecidas.

(Internal Control - Integrated Framework, p. 3)

O modelo COSO representa o modelo de aplicação genérico a qualquer organização. Este modelo possui recomendações para a gestão das organizações, no sentido de avaliação, relato e melhorias dos sistemas de controlo, de modo que o seu “cliente preferencial”, destinatário primeiro, são os gestores.

Este é representado por um processo que tem a finalidade de possibilitar uma garantia razoável quanto à realização dos objetivos nas seguintes categorias: eficácia e eficiência das operações, fiabilidade do relato financeiros e conformidade com leis e regulamentos aplicáveis.

O controlo interno através do modelo COSO identifica cinco componentes interrelacionados, derivados da forma como a gestão gere o seu negócio e como se integra com o processo de gestão. Os componentes dividem-se em ambiente do controlo, avaliação do risco, atividades de controlo, informação e comunicação e atividades de monitorização.

1.2. RELEVÂNCIA DO ESTUDO

Este estudo centra-se na importância do controlo interno. É um tema pertinente, atual e relevante na gestão das empresas, muito devido à resposta ao risco que afeta o alcance dos objetivos das organizações, bem como a outros constrangimentos.

Entende-se como um contributo à ciência pela investigação de uma matéria relevante, aplicado a uma empresa real, onde é implementado o modelo COSO. Contribui ainda para a reflexão de um tema significativo na atual situação económica a nível mundial, pois através de um eficaz e eficiente sistema de controlo interno é possível ajudar a garantir que as diretrizes da gestão ou administração são levadas a cabo. Estas encontram-se diretamente relacionadas com o alcance dos objetivos da entidade, nomeadamente a fiabilidade do relato financeiro, eficácia e eficiência das operações e conformidade com leis e regulamentos aplicáveis.

O estudo de caso, relaciona-se de uma forma financeira e social ao tema a abordar, pelo diagnóstico do sistema de controlo interno numa organização privada de elevada importância no mercado português. De notar, que na economia é o sector privado que impulsiona o crescimento económico, estando por sua vez sob maior supervisão e controlo tanto das entidades reguladoras, como dos próprios clientes.

1.3. OBJETO E OBJETIVO

O presente trabalho tem como objeto de estudo a apreciação do modelo de controlo interno COSO, este reconhecido como estrutura modelo para desenvolver, implementar e conduzir o processo de controlo interno, assim como a avaliação da sua eficácia.

O trabalho tem como um dos seus principais objetivos a demonstração de que o funcionamento eficaz de um sistema de controlo interno, verificado pelo departamento de auditoria interna, é uma ferramenta de elevada importância no apoio à gestão, através do estudo dos componentes e princípios da sua estrutura. É através destes que iremos conduzir ao aprofundamento do tema no estudo de caso.

A empresa a abordar do ramo energético a laborar no mercado português é a EDP. Esta tem como *core business* produtos energia elétrica e gás natural, encontrando-se no processo de produção, distribuição e comercialização dos mesmos. A entidade incorpora na sua gestão o sistema de controlo interno, formalizado através do SCIRF - Sistema de Controlo Interno do Relato Financeiro, tendo com base nas melhores práticas internacionais e nos modelos de referência COSO e COBIT.

Com o presente trabalho objetiva-se a averiguação e um conhecimento aprofundado sobre matérias relacionadas com o sistema de controlo interno, níveis e tipos de controlo, evolução e limitação do controlo interno, formas de registo e avaliação do controlo interno, o estudo do modelo COSO e os respetivos componentes e a relação entre si.

Numa segunda instância é feita a abordagem real, onde o objeto de estudo tem como base dados fornecidos pela Direção de Auditoria Interna, nomeadamente do núcleo de Controlo Interno, para que, acima de tudo, se valide o que foi abordado anteriormente, bem como o Relatório e Contas e os Relatórios de Auditoria Interna.

1.4. METODOLOGIA E ESTRUTURA

O tema estudado é inserido no âmbito das unidades curriculares de Auditoria Interna e Riscos Empresariais e Controlo Interno de uma forma geral incidindo em particular sobre o controlo interno e a estratégia empresarial.

Para abordar a parte teórica do tema irá ser apresentado como base a leitura de documentação, ou seja, da pesquisa bibliográfica e estado de arte, não só específica da matéria como também de uma forma genérica, de modo a atingir a compreensão dos conceitos e linguagem utilizada pelos autores.

Com a leitura da revisão bibliográfica irá ser possível cruzar informação e conseguir uma opinião formada e realizar o trabalho proposto de uma forma mais concisa.

Para a abordagem prática, com o caso de estudo, pretende-se relacionar os temas mencionados acima, tanto gerais com a informação obtida da entidade objeto de estudo.

Analisar e validar a informação recolhida com o auxílio de colaboradores da entidade e da informação retirada do Relatório e Contas e de auditoria interna. O estudo de caso irá seguir a orientação de uma análise qualitativa, pois permite estudar uma entidade de uma forma aprofundada. Neste tipo de estudo procura-se investigar ideias e descobrir significados partindo dos intervenientes nos processos. Tendo como hipótese de estudo uma abordagem geral dos componentes do modelo COSO aplicados a uma empresa do ramo energético, diagnosticando-os quanto à sua eficácia.

No fim do período de desenvolvimento, é expectável, através do diagnóstico do funcionamento do sistema de controlo interno, numa empresa com grande relevância no mercado português, poder afirmar que este se encontra alinhado com o modelo COSO em estudo.

2. CONTROLO INTERNO

2.1. PERSPETIVA HISTÓRICA

Por volta de 1929, o *American Institute of Certified Public Accountants* (AICPA) e a *Federal Reserve* (Fed) definiam o controlo interno como o exame ou avaliação de demonstrações financeiras realizada por contabilistas independentes. Antes dos anos 40 e para quem estudava a matéria, o agora denominado como controlo interno, inicialmente era conhecido como *internal check*¹. O *internal check system*, segundo Zhang (2014: 99) é referido com um processo que providencia eficácia na organização e nas operações e, previne a ocorrência de erros e operações ilegais. Como principal característica a segregação de funções, na medida em que nenhum colaborador ou departamento detém autoridade total de acesso a qualquer parte dos processos da entidade.

O *internal check* detém duas vantagens básicas reconhecidas, segundo Zhang. A primeira é que existem poucas oportunidades de dois ou mais colaboradores ou departamentos inconscientemente realizarem o mesmo erro. Em segundo, a possibilidade de dois ou mais colaboradores ou departamentos conscientemente executarem fraudes em conluio. Esta forma de verificação ou exame representa a base do controlo organizacional, reduzindo erros e fraudes de forma eficaz. Contudo, o *internal check* apenas representa uma parte do controlo interno, por não ir ao encontro de todos os requisitos deste último, nomeadamente nos objetivos, conteúdo e métodos.

No fim dos anos 40, o controlo interno veio comutar o *internal check*. Em 1949, o AICPA relatou sobre o *Internal Control: Elements of a Coordinated System and its Importance to Management and the Independent Public Accountant*, Special Report no Comité de Procedimentos de Auditoria. Foi aqui que o conceito de Controlo Interno se tornou oficial. Aqui ficaram reconhecidos métodos, medidas e objetivos usados na guarda de ativos, inspeção da exatidão da informação contabilística, aperfeiçoamento da eficiência de operações e na promoção da implementação de políticas de gestão.

Mais tarde, por volta de 1958, o Comité de Auditoria do AICPA, redefiniu o Controlo Interno, dividindo-o em Controlo Contabilístico e Controlo de Gestão. O primeiro diretamente relacionado com a fiabilidade da informação contabilística e o segundo com o alcance da eficiência operacional e da gestão.

¹ *Internal Check* (eng) – Verificação/Revisão/Exame Interno (port)

Durante os anos 70, após investigação da SEC e do Comité do Watergate² deterem grandes empresas envolvidas em donativos e transações ilegais, a atenção com o Controlo Interno foi reforçada. Desta forma, foi dado maior enfoque quanto à conceção do Sistema de Controlo Interno e aos métodos de auditoria foram aperfeiçoados em termos de qualidade e eficácia. Mais tarde, em 1985, a organização COSO foi criada, com o objetivo de planificar métodos e metodologias para prevenir e evitar fraudes nas demonstrações financeiras da entidade.

Desde os anos 90 até ao início do séc. XXI, com a ocorrência de grandes escândalos e crises financeiras, surgiu a preocupação em reforçar as medidas de controlo interno e da existência de normativo quanto a esta matéria. Pode-se ter como exemplo a Lei *Sarbanes-Oxley* (SOX), as diretivas comunitárias e, o código de bom governo da Comissão do Mercado de Valores Mobiliários. No decorrer do séc. XXI, após a implementação de normativos quanto ao controlo interno, foi dado destaque o tema da gestão do risco, em que, se aplicado de forma adequada, permite que «toda a entidade esteja estrategicamente alinhada e opere com vista a uma finalidade comum, facilitando o sucesso.» (Inácio; 2014:27)

2.2. CONCEITO

Foi em 1934, que surgiu a primeira definição de controlo interno, pelo AICPA, reconhecida pela SEC, que segundo a SAS n. °1, diz:

[o] controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas adotadas num negócio a fim de garantir a salvaguarda dos ativos, verificar a adequação e fiabilidade dos registos contabilísticos, promover a eficiências operacional e encorajar a adesão às políticas estabelecidas pela gestão.

Mais tarde, foi com a emissão da SAP n.º 54 – *The Auditor's study on evaluation of internal control*, que o AICPA redefiniu o controlo interno subdividindo-o em:

- Controlo Administrativo como um plano de organização, procedimentos e registos relacionados com os processos de decisão que conduz à autorização das transações pelo Órgão de Gestão;

² Comité do Watergate convocado pelo Senado dos Estados Unidos para investigar o escândalo do Watergate. Este caso levou o Presidente Nixon a ser julgado pela Suprema Corte dos Estados Unidos, pelo envolvimento deste em operações ilegais e criminosas, onde consequentemente foi aberto um processo constitucional de cessação de mandato. (Fonte: <http://www.history.com/topics/watergate>)

- Controlo Contabilístico como um plano da organização, procedimentos e registos relacionados com a salvaguarda de ativos e a confiança nos registos financeiros que, consequentemente, são elaborados no sentido de proporcionar uma certeza razoável acerca de:
 - As transações serem executadas de acordo com uma autorização geral ou específica da gestão;
 - As transações serem registadas de forma a permitir a preparação das DF em conformidade com os princípios contabilísticos geralmente aceites e a manter o registo contabilístico dos ativos;
 - Salvaguarda dos ativos, permitido o acesso apenas a que detenha autorização do Órgão de Gestão; e
 - O registo contabilístico dos ativos ser comparado, em intervalos de tempos razoáveis, com os ativos existentes e medidas apropriadas são tomadas sempre que quaisquer diferenças sejam verificadas.

Posteriormente, com o crescente número de fraudes de relato financeiro, surgiu a necessidade de existir uma definição de controlo interno consistente e reconhecido de forma geral. Iniciativa esta dada pelo *Committee of Sponsoring Organizations of Treadway Commission*, com a publicação do *Integrated Framework*, em 1992, onde foi apresentado o conceito de Controlo Interno com o maior nível de concordância, nomeadamente:

[o] controlo interno é um processo realizado pelo Conselho de Administração, Direção e outros membros da organização com o objetivo de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos:

- Eficácia e eficiência dos recursos;
- Fiabilidade da informação financeira;
- Cumprimento das leis e normas estabelecidas.

(§3 *Integrated Framework*)

Para Sawyer (2003: 82) existe uma definição alternativa para controlo interno, tal como se segue:

The employment of all the means devised in an enterprise to promote, direct, restrain, govern, and check upon its various activities for the purpose of seeing that enterprise objectives are

met. These means of control include, but are not limited to, form of organization, policies, systems, procedures, instructions, standards, committees, charts of accounts, forecasts, budgets, schedules, reports, records, checklists, methods, devices, and internal auditing.

De acordo com o COSO, citado por Morais e Martins (2013: 29), a definição integral, subjacentemente, os seguintes conceitos fundamentais:

- Processo – o objetivo é transmitir que o controlo interno é um meio para atingir um fim e não um fim em si mesmo. É constituído por um conjunto de acções que envolve todas as atividades, processos e tarefas da entidade;
- Levado a cabo por pessoas – o objetivo é transmitir que o controlo interno não é somente um manual de políticas e documentos, mas também de pessoas em cada nível da entidade. O sistema de controlo interno é concebido e implementado por pessoas, afetando a atuação de todos os membros da entidade;
- Confiança razoável – o objetivo é transmitir que por muito bem que esteja concebido sistema de controlo interno, somente pode proporcionar um certo grau de segurança à entidade. Não oferece uma segurança total, uma vez que não consegue eliminar a totalidade dos riscos, apenas os minimiza;
- Concretização de objetivos – o objetivo é transmitir que o controlo interno é concebido para permitir a consecução de objetivos, gerais e específicos, nas diferentes categorias e que devem ser consistentes e coerentes.

Ainda nos anos 90, com a dependência das tecnologias de informação, manifesta-se a necessidade da existência de um referencial direcionado para este tema. Posto isto, surgiu o modelo *Control Objectives for Information and related Technology* (COBIT). Este adaptado do modelo COSO, orientado a ambientes tecnológicos, emanado pelo ISACA.

A lei SOX³ criada pelo senador Paul Sarbanes e Michael Oxley, com entrada em vigor em 2002, veio introduzir mudanças na legislação da regulação da prática financeira e de *corporate governance*⁴. Esta norma visa a proteção de investidores de possíveis atividades contabilísticas fraudulentas.

³ Lei SOX: explanada no subcapítulo 3.4.6. SOX ACT

⁴ Segundo www.soqlaw.com: *corporate governance* passou a deter mais importância desde que foi introduzida a SOX Act, em 2002. Desta forma o *corporate governance* representa o sistema de normas, práticas e processos pelo qual uma entidade é direcionada e controlada.

Em 2004, o modelo COSO é expandido e então introduzindo o conceito de ERM – *Enterprise Risk Management*. Com a incorporação deste tema, a gestão encontra-se habilitada a determinar quantitativamente, o risco que a entidade se encontra preparada e, está de acordo a aceitar, de maneira a criar valor.

Em 2013, o modelo original do COSO foi revisto, atualizado e modernizado, pois desde 1992 foi sentida uma grande mutação no risco do negócio, resultando numa maior necessidade ao nível da competência e responsabilidade.

Pode-se concluir que não existe um sistema de controlo interno *standard*, pois este deve ser adaptado às constantes mudanças na entidade e no ambiente externo, relativamente às alterações regulamentares, ou seja, deve adaptar-se à realidade em que se encontra.

2.3. OBJETIVOS DO CONTROLO INTERNO

Segundo o *The Institute of Internal Auditors* (IIA), na atividade de auditoria interna é imperativo avaliar a adequação e eficácia dos controlos de forma a responder aos riscos da entidade, operações e sistemas de informação, nos seguintes pontos:

- Fiabilidade e integridade da informação financeira e operacional;
- Eficiência e eficácia das operações;
- Salvaguarda dos ativos; e
- Conformidade com as leis, regulamentos e contratos.

(International Professional Practices Framework (IPPF): 2130 – Control)

Segundo Baptista da Costa, o controlo interno os objetivos consistem:

- a) no plano da organização que proporciona uma apropriada segregação de responsabilidades funcionais;
- b) num sistema de autorização e procedimentos de registos a fim de proporcionar um controlo contabilístico razoável sobre os activos, passivos, réditos e gastos;
- c) em sãs práticas a serem seguidas no desempenho dos deveres e das funções de cada um dos departamentos de uma empresa;
- d) em existir pessoal de qualidade compatível com as respectivas responsabilidades.

(Baptista da Costa; 2010: 223-224)

Para Coelho Inácio (2014: 25), os objetivos atingem três categorias diferentes:

- Objetivos operacionais: eficiências e eficácia das operações da entidade, incluindo os fins operacionais e financeiros, e a salvaguarda de ativos contra perdas;
- Objetivos de relato: respeitam à informação financeira e não financeira interna e externa e podem abranger a confiabilidade, tempestividade, transparência, ou outros conforme estabelecido pelos reguladores, organismos de regulação reconhecidos ou as políticas da entidade;
- Objetivos de conformidade: aderência às leis e regulamentos a que a entidade está sujeita.

Assim, o conceito de controlo interno, de forma mais abrangente, tem objetivos que não se encontram apenas relacionados com as demonstrações financeiras, detém também matéria relativa à eficácia e eficiência que por norma relacionam-se com as operações e são de conformidade com as leis, regulamentos e regras.

2.4. RELATÓRIOS E MODELOS DE CONTROLO INTERNO

O controlo interno, ao longo dos tempos, tem sofrido modificações e atualizações, como se pode ter constatado no ponto da «Perspetiva histórica» neste capítulo. Comumente são conhecidos o Relatório *Treadway*, Modelo COSO, Relatório *Cadbury*, Modelo COBIT, Relatório *Turnbull* e, reconhecidos como antecedentes e sistematizadores ao *SOX Act*.

2.4.1. RELATÓRIO TREADWAY

O primeiro relatório na ótica do controlo interno foi emitido em 1987 nos Estados Unidos da América, especificamente sobre a temática do combate à fraude do relato financeiro. O objeto da *National Commission on Fraudulent Financial Reporting*⁵, formada em 1985, era de desenvolver recomendações que fossem práticas, razoáveis nas circunstâncias, justificadas pelos benefícios a atingir, de forma a serem implementadas sem encargos extraordinários.

Para a emissão deste relatório, a Comissão teve o contributo do AICPA, IIA, *American Accounting Association* (AAA), *Financial Executives Institute* (FEI), *National Association of Accountants* (NAA), tendo como presidente C. Treadway, Jr.

⁵ *National Commission on Fraudulent Financial* (eng): Comissão Nacional sobre Relato Financeiro Fraudulento (port); conhecida como *The Commission* (eng) – *A Comissão* (port).

A Comissão tinha como principal objetivo uniformizar o conceito de controlo interno, pela existência de várias opiniões e pareceres sobre este tema, com a inexistência de entendimento sobre o conceito e missão. Ficou neste relatório definido o conceito de relato financeiro fraudulento como: «*intentional or reckless conduct, wether act or omission, that results in materially misleading financial statements*». (*Report of the National Commission on Fraudulent Financial Reporting*; 1987: 2). O âmbito em que atua encontra-se direcionado para empresas públicas, geralmente detidas por investidores públicos.

Os três maiores objetivos do Relatório Treadway são:

1. *Consider the extent to which acts of fraudulent financial reporting undermine the integrity of financial reporting; the forces and the opportunities, environmental, institutional, or individual, that may contribute to these acts; the extent to which fraudulent financial reporting can be prevented or deterred and to which it can be detected sooner after occurrence; the extent, if any, to which incidents of this type of fraud may be the product of a decline in professionalism of corporate financial officers and internal auditors; and the extent, if any, to which the regulatory and law enforcement environment unwittingly may have tolerated or contributed to the occurrence of this type of fraud.*
2. *Examine the role of the independent public accountant in detecting fraud, focusing particularly on whether the detection of fraudulent financial reporting has been neglected or insufficiently focused on and whether the ability of the independent public accountant to detect such fraud can be enhanced, and consider whether changes in auditing standards or procedures -- internal and external -- would reduce the extent of fraudulent financial reporting.*
3. *Identify attributes of corporate structure that may contribute to acts of fraudulent financial reporting or to the failure to detect such acts promptly.*

(Report of the National Commission on Fraudulent Financial Reporting; 1987: 2)

2.4.2. MODELO COSO

O modelo COSO representa o modelo de controlo interno comumente aceite a nível mundial e, o mais utilizado nos EUA. (Inácio; 2014:34 *apud* Perry e Warner, 2005) Esta situação deve-se ao facto de este modelo estar implícito às *Internacional Standard on Auditing* (ISA) do *The International Auditing and Assurance Standards Board* (IAASB). Visto este ser o modelo adotado no presente trabalho, o seu desenvolvimento será feito num capítulo próprio.

2.4.3. RELATÓRIO CADBURY

A origem do relatório Cadbury, em maio de 1991 e publicado em dezembro de 1992, pelo Comité de *Corporate Governance*, composto pelo *Financial Reporting Council*, pelo *Stock Exchange* e profissionais da contabilidade. Este comité constituído como forma de responder à falta de confiança e honestidade por parte dos investidores e responsabilidade das empresas cotadas, no seguimento do colapso financeiro do grupo *Coloroll* e do consórcio de Polly Peck e Asil Nadir.

As recomendações emanadas no relatório, direcionadas para entidades registadas na Inglaterra, focam-se nas funções de controlo e reporte da gestão, bem como da função da auditoria. Estas com o objetivo de mitigar os riscos e falhas relacionadas com o *corporate governane*. É através da abordagem baseada no *compliance*, o cumprimento de leis e regulamentos, que o relatório se torna mais eficaz.

Os componentes centrais presentes no Código Cadbury, são:

- *that there be a clear division of responsibilities at the top, primarily that the position of Chairman of the Board be separated from that of Chief Executive, or that there be a strong independent element on the board;*
- *that the majority of the Board be comprised of outside directors;*
- *that remuneration committees for Board members be made up in the majority of non-executive directors; and*
- *that the Board should appoint an Audit Committee including at least three non-executive directors.*

(University of Cambridge - *The Cadbury Report*: <http://cadbury.cjbs.archios.info/report>)

No que diz respeito ao controlo interno, o relatório Cadbury, no §4.32, recomenda que os administradores devem emitir uma opinião no Relatório e Contas, respeitante à eficácia do sistema de controlo interno e que os auditores devem elaborar um parecer sobre este último. Segundo o §5.16 uma parte essencial para a gestão eficiente de uma entidade, é necessário um Sistema de Controlo Interno eficaz. Cabe aos profissionais de contabilidade e de quem elabora o relatório e contas, desenvolver:

- a. Um conjunto de critérios para avaliar a eficácia;
- b. Orientações para as empresas da forma como os administradores devem reportar; e

- c. Orientações para os auditores sobre os procedimentos de auditoria relevantes e como estes devem reportar.

(*Cadbury Report*; 1992: §5.16)

2.4.4. MODELO COBIT

O modelo COBIT – *Control Objectives for Information and Related Technologies* detém uma estrutura semelhante ao modelo COSO, porém, focado em ambientes tecnológicos. Este é constituído por um guia de boas práticas, mantido pelo ISACA.

Publicado em 1996, com o objetivo de «*to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals*» (COBIT 5).

O modelo COBIT faz a relação dos objetivos de controlo das tecnologias de informação com os objetivos de negócio. Como requisitos de informação detém a qualidade, fidedignidade e segurança, atribuindo como critérios a fiabilidade, conformidade, integridade, confidencialidade, disponibilidade, eficácia e eficiência.

O modelo foi criado com as seguintes características principais:

- Centrado no negócio, pois está focado nos objetivos da entidade, numa ótica de recursos informatizados, nomeadamente aplicações, informação, infra-estruturas e pessoas;
- Orientado para os processos, dentro dos seus 4 domínios;
- Baseado em controlos, definindo-os para todos os 34 processos;
- Guiado pela mensuração, onde se encontra um modelo de maturidade desenvolvido para cada um dos processos, permitindo identificar o desempenho atual da organização, o estado do setor, o alvo de melhoria da empresa e o caminho a percorrer do atual para o objetivo.

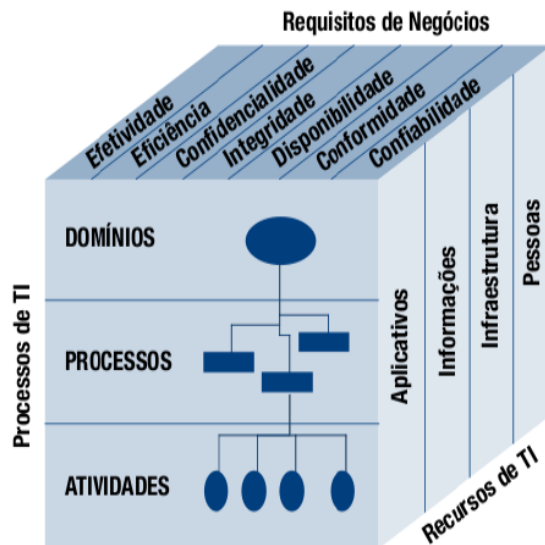


Figura 1 – Cubo COBIT
 Fonte – COBIT Framework

Este modelo identifica 34 processos de IT, cobrindo desde o planeamento estratégico até à implementação, suporte na produção e monitorização. Os processos encontram-se agrupados segundo 4 domínios: planeamento e organização; aquisição e implementação; entrega e suporte; e monitorização.

No COBIT5, foi desenvolvida a aplicabilidade deste modelo na gestão de risco, com a possibilidade de ser usado em simultâneo com outros *standards* já existentes. Com os sete princípios de gestão de risco, é tido como um modelo facilitador e com elevados benefícios. Ainda assim, para melhor entendimento deste modelo é necessário possuir formação adequada, pela sua extensa documentação e terminologia técnica.

2.4.5. RELATÓRIO TURNBULL

O relatório Turnbull, publicado 1999, define as melhores práticas sobre o controlo interno para as empresas da Inglaterra. Em 2005, o *Financial Reporting Council (FRC)*, emitiu uma versão atualizada das orientações, intitulada *Internal Control: Guidance for Directors on the Combined Code*. Em 2014, substituída pelo *Risk Guidance*.

O relatório indica à Administração as respetivas obrigações resultantes do *Combined Code*, no que diz respeito à adoção e manutenção de um eficaz controlo interno ou boas auditorias e controlos de forma a assegurar a qualidade dos relatórios financeiros, bem como na descoberta de qualquer fraude.

As orientações do relatório visam:

- *reflect sound business practice whereby internal control is embedded in the business processes by which a company pursues its objectives;*
- *remain relevant over time in the continually evolving business environment; and*
- *enable each company to apply it in a manner which takes account of its particular circumstances.*

(Financial Reporting Council: Internal Control – Revised Guidance for Directors on the Combined Code; 2005: § 5)

As orientações emanadas no relatório têm como base a adoção de uma abordagem baseada no risco, aquando do estabelecimento do SCI e na revisão da sua eficácia. O relatório foca-se na manutenção de um bom sistema de controlo interno e os respetivos elementos, no processo de revisão da eficácia do controlo interno e no parecer da administração relativa ao controlo interno.

No §18 do relatório é referido que a todos os colaboradores são-lhes destacadas responsabilidades sob o controlo interno como parte do alcance dos objetivos da organização. Desta forma, tal como descrito no §19, o sistema de controlo interno, deve englobar políticas, processos, tarefas, comportamentos e outros aspetos da organização que em conjunto contribuam para o alcance dos objetivos.

No relatório Turnbull, §20, as componentes do sistema de controlo interno, incluem:

- o ambiente de controlo da organização,
- as atividades de controlo;
- os processos de informação e comunicação;
- os processos para monitorizar a sua eficácia.

A administração da organização e a gestão, segundo Turnbull, são identificadas como responsáveis pelas divulgações sobre o controlo interno no relatório e contas, pela revisão e monitorização da eficácia do sistema de controlo interno, assim como garantir que o fez.

Para tal, a administração deverá promover uma avaliação anual, por forma a proceder à sua declaração sobre controlo interno, de forma a assegurar que foram considerados todos os aspetos relevantes do ano.

2.4.6. COCO

Em 1995, o *Canadian Institute of Chartered Accountants* (CICA), publicou o *Criteria of Control Framework* (CoCo). Tem como objetivo o auxílio dos órgãos de gestão na implementação e avaliação do ambiente de controlo, de forma a atingir os objetivos, tanto a nível operacional como estratégico.

Esta metodologia atribui responsabilidades específicas à administração, pois é esta quem define a estratégia. Para tal, deve ter em conta os riscos na definição do controlo, ultrapassando a abordagem contabilística e de segurança dos ativos, preconizada no modelo COSO.

É ao nível dos objetivos, que o modelo CoCo é considerado mais amplo do que o COSO, visto pretender assegurar não só a fiabilidade do relato financeiro, mas sim de qualquer relato, tanto interno como externo, bem como no que respeita à aderência às leis e regulamentos, onde aqui são incluídas as políticas internas.

No modelo CoCo, são estabelecidos quatro critérios de controlo:

- Objetivo, estabelece um juízo do sentido da organização, endereça os seus objetivos, missão, visão, estratégica, riscos, oportunidades, políticas e indicadores de desempenho;
- Empenho, transmite a identidade da organização e endereça os seus valores éticos, políticas de recursos humanos, autoridade, responsabilidade e confiança mútua;
- Capacidade, relacionado com a competência da organização ao nível do conhecimento, habilidade e ferramentas, processos de comunicação, informação, coordenação e atividades de controlo;
- Monitorização e aprendizagem, prestando um sentimento de evolução da organização, integrando, revisão de ambientes externos e internos, monitorização do desempenho contra os objetivos, desafia assunções, reavalia as necessidades de informação e dos sistemas, definição de procedimentos de acompanhamento e avaliação da eficácia do controlo.

Segundo o modelo CoCo, a avaliação do controlo interno, é feita exclusivamente por recursos da própria organização, com a possibilidade de serem integrados outros modelos existentes, como o COSO e, realizado em intervalos de tempo.

Desta forma, o controlo, de acordo com o CoCo, é eficaz quando presta uma segurança razoável de que a organização irá atingir fielmente os objetivos a que se propôs.

2.4.7. SOX ACT

A Lei Sarbanes-Oxley, em inglês designada por *SOX Act*, foi publicada em 2002 e fundada pelos senadores Paul Sarbanes, democrata de Maryland e, Michel Oxley, republicano de Ohio.

Esta estabelece requisitos para proteger acionistas e o público em geral de erros e fraudes no relato financeiro, bem como na melhoria da precisão de divulgações administrativas. Promulgada após escândalos no início dos anos 2000, nomeadamente da Enron, Tyco, WorldCom, Arthur Anderson, Xerox, entre outras.

Tem como objetivo final restabelecer o nível de confiança da informação emanada pelas entidades, através da prevenção de possíveis fraudes nas demonstrações financeiras, garantido a transparência e credibilidade das informações divulgadas na tentativa de recuperar a confiança dos investidores.

A Lei SOX veio exigir que as *Public Company's* dos Estados Unidos da América e respetivas filiais europeias, assim como as sociedades estrangeiras registadas num dos mercados bolsistas dos EUA, instalassem, no respetivo comité de fiscalização, procedimentos de receção, aceitação e tratamento das queixas recebidas em matéria de contabilidade, controlos contabilísticos internos ou outros assuntos nesta área; e a transmissão confidencial e anónima pelos colaboradores de preocupações nestas matérias.

A SOX é de aplicação mundial, desde que tenham ações cotadas na *Securities and Exchange Commission* (SEC), nomeadamente na bolsa de Nova Iorque (NYSE – *New York Stock Exchange*) ou no NASDAQ. Esta procura aumentar os controlos, a segurança e transparência do negócio, na divulgação de informação, nos registos contabilísticos e na administração financeira. Estabelece também, as responsabilidades do CEO e do CFO, medidas sobre proteção da fraude, nomeadamente pressupostos para a independência do auditor, rotação das empresas que prestam serviços de auditoria, proteção dos instrumentos de comunicação de práticas indevidas.

Relativamente à avaliação pela gestão do SCI sobre o relato financeiro e subsequente avaliação pela auditoria, merecem destaque as secções 302 e 404. A secção 302 preconiza que cabe ao CEO e CFO conceber uma declaração sobre a correção do relato financeiro e

sobre a responsabilidade pela implementação e eficácia do SCI e a sua avaliação. A secção 404 estabelece que o relatório de controlo interno, em cada relato anual, terá de mencionar a responsabilidade da gestão pelo controlo interno, abarcando uma avaliação da sua eficácia. Sobre esta avaliação, irão pronunciar-se os auditores no decurso da auditoria financeira.

A *SOX Act* impactou o controlo interno pela uniformização dos processos, pela racionalização dos procedimentos de controlo interno, pela documentação dos controlos, pelas atividades manuais e automáticas, na importância das IT e respetivas aplicações, como *user developed applications* e respetivos controlos.

A Lei SOX, beneficia o papel crítico do controlo interno, como um processo executado por órgãos da gerência ou outras pessoas da entidade que impulsionam o sucesso dos negócios em três categorias:

- Eficácia e eficiências das operações;
- Confiança nos relatórios financeiros; e
- Cumprimento das leis e regulamentos aplicáveis.

2.5. TIPOLOGIA DE CONTROLOS

Segundo Inácio, «[q]ualquer sistema de controlo interno deve incluir os controlos adequados» (2014: 32). Assim, é necessário que estes se encontrem classificados, por forma a facilitar a sua identificação. De uma forma mais arcaica, estes podem subdividir-se em controlos primários e secundários.

Como controlos primários tem-se:

- Controlos preventivos que impedem a ocorrência de eventos indesejáveis, considerados controlos *à priori*, que entram imediatamente em funcionamento. Como exemplo deste tipo de controlo tem-se a segregação de funções: necessidade de duas assinaturas num tipo de pagamento, verificação da exatidão matemática das faturas antes do pagamento.
- Controlos detetivos geram alertas, para detetar e corrigir, após o evento indesejado, considerados controlos *à posteriori*. Estes controlos são eficazes quando detetados antes da ocorrência de danos materiais. Por exemplo, a elaboração de reconciliações bancárias, realização de contagens físicas, quando um conjunto de faturas submetidas

para processamento e, existe a possibilidade de serem rejeitadas pelo sistema informático, caso inclua pagamentos idênticos a apenas um fornecedor.

- Controlos corretivos corrigem os efeitos negativos de eventos indesejáveis. Como exemplo, tem-se relatórios de artigos obsoletos, lista de reclamações de clientes.
- Controlos orientativos ou diretivos provocam ou encorajam a ocorrência de eventos desejáveis, de forma a produzir efeitos positivos para prevenir eventos indesejáveis. Estes podem incluir manuais de políticas e procedimentos, formação dos colaboradores e descrição do trabalho.

Como controlos secundários, tem-se:

- Controlos compensatórios, que mitigam, podem reduzir o risco quando os controlos primários não são eficazes, ou seja, compensam fraquezas de controlo noutras áreas da entidade. Por si só, não reduzem o risco a nível aceitável. A falta de segregação de funções, por exemplo, quando se encontra em loja apenas um colaborador aquando do fecho da mesma e não existe ninguém com quem conferir valores de caixa.
- Controlos complementares entrelaçam-se com outros controlos, de forma a reduzir o risco, ou seja, existe sinergia de controlos que leva a uma maior eficácia. A separação das funções de contabilidade e de quem recebe e faz a guarda dos valores é complementada pela obtenção de validações pelo banco.

2.6. RECOLHA E REGISTO DO SISTEMA DE CONTROLO INTERNO

De acordo com o AICPA, o estudo e avaliação do sistema de controlo interno apropriado servirá como base de confiança, bem como determinará a extensão dos procedimentos de auditoria, através do levantamento e recolha de informação sobre o controlo interno.

Segundo Inácio, «[u]ma das melhores formas de registar o controlo interno é a elaboração de um manual [...] que possa ser consultado por todos os intervenientes e que não seja uma peça estática [...]». (2014: 51)

Para poder elaborar o manual de controlo interno, usualmente, como forma de levantamento de informação, são utilizados os procedimentos de observação e indagação, através de entrevistas ou questionários. Os dados recolhidos, normalmente utilizados para a análise inicial, podem ser do tipo organigramas, manuais de descrição de funções, manuais de

políticas e procedimentos e medidas de controlo interno e, quaisquer outras informações, como por exemplo, ordens de serviço, instruções de serviço, comunicações internas, entre outras, desde que relacionadas com aspetos do controlo. (Baptista da Costa; 2010: 235)

Para que possa ser registada a informação sobre o sistema de controlo interno, subsistem quatro formas de o fazer. (Anexo 1)

O questionário padronizado, em formato de *check-list*, onde se encontram presentes um conjunto de procedimentos de controlo, de acordo com a área, que se espera que estejam a ser aplicados. No questionário, as possíveis respostas são «Sim, Não ou Não Aplicável», podendo ou não, constar uma coluna para «Observações» para fazer referências a outros pontos no relatório.

Este tipo de questionário apresenta as seguintes vantagens:

- É um meio bastante objetivo;
- Trata-se de uma abordagem disciplinada e sistemática de avaliação;
- Muito fácil de utilizar quer por pessoas experientes quer inexperientes;
- Permite um registo periódico dos procedimentos e controlos em prática;
- Ajuda a supervisão do processo de levantamento por parte dos auditores responsáveis;
- Fornece um caminho a seguir pelo auditor ao mostrar as áreas de fraqueza.

(Inácio; 2014: 52)

Porém, apresenta também algumas desvantagens:

- Pode levar a uma abordagem estereotipada, que não atende às especificidades da entidade em causa e, como sabemos, o controlo interno deve ser adaptado às diferentes realidades;
- Pode tornar-se “mecânico”, quer para quem está a responder quer para quem o está a analisar o que pode levar ao enviesamento dos resultados;
- O nível de detalhe também pode tornar-se limitador que por excesso, o que os torna restritivos, quer por defeito, o que os torna demasiado genéricos.

(Inácio; 2014: 52)

A narrativa representa uma forma de registo através da discriminação de informação de forma mais detalhada das medidas de controlo existentes. Tem como inconveniente o fato de estar mais propensa a deter muita informação pormenorizada, resultando na «perda de visão rápida e global do conjunto da área descrita e dos seus aspetos mais significantes». (Baptista da Costa; 2010: 239). Usualmente, é descrito numa coluna o procedimento e medidas do SCI e numa outra coluna as alterações a introduzir, se for o caso, o novo procedimento.

O uso de fluxogramas é feito através da representação gráfica, em que se recorre á simbologia para representar procedimentos e medidas de controlo. Esta forma de registo, em relação a outras, é representada de forma mais clara, simples e concisa. Contudo, pode não ser de fácil preparação e exige o conhecimento mais profundo e específico.

Os fluxogramas, segundo Baptista da Costa, podem assumir dois formatos: fluxograma vertical ou horizontal. O fluxograma vertical apresenta a sucessão de procedimentos de forma vertical, ou seja, descendente. Este fluxograma destaca a documentação em detrimento das secções em que os mesmos são originados ou por onde circulam. O fluxograma horizontal é representado pela sucessão de procedimentos de forma horizontal, atravessando colunas, cada uma representando as secções ou áreas envolvidas.

A forma mista é representada pela conjugação do fluxograma e a narrativa. «A base de registo é o fluxograma, sempre que se represente uma operação complexa, faz-se um “corte” no fluxograma e utiliza-se a narrativa para descrever o procedimento complexo.» (Inácio; 2014: 53)

2.7. AVALIAÇÃO DO CONTROLO INTERNO

Uma das melhores defesas contra o insucesso do negócio, bem como um condutor importante de *performance*, encontra-se na existência de um sistema de controlo interno eficaz. Por sua vez, este requer a existência da gestão de riscos e, assim, possibilitar a criação e preservação de valor. Para além destes objetivos, é também necessário identificar e acompanhar os objetivos através da avaliação do controlo interno.

Na avaliação do controlo interno encontra-se associada a gestão de riscos que visa:

- Estabelecer prioridades de controlo acerca do negócio;
- Representar o custo efetivo que traduza uma vantagem competitiva;

- Evitar que a avaliação do controlo se envolva em processos morosos de análise e verificações detalhadas.

(Morais e Martins; 2013: 40)

A primeira avaliação do controlo interno, dá-se aquando da elaboração do plano de Auditoria. É nesta avaliação que se irão basear os procedimentos a tomar, o alcance e profundidade dos testes nas auditorias. É importante para o auditor conhecer, rever e avaliar o sistema de controlo interno para, desta forma, determinar o grau de confiança a aplicar quando coloca em prática os procedimentos de amostragem. Aquando da existência da Comissão de Auditoria nas entidades, é esta quem avalia o controlo interno ao mais alto nível.

As principais etapas a seguir, segundo Morais e Martins (2013: 40), são:

- 1 - Descrição do sistema a fim de verificar a sua eficiência e se, efetivamente existe ou não procedimentos de controlo adequados;
- 2 - Verificação da descrição do sistema, que consiste na obtenção da prova de que o sistema descrito pelo auditado reflete o que realmente existe, entre outras, pelas seguintes razões:
 - a) O auditor pode ter efetuado interpretação indevida das informações recebidas sobre a descrição dos subsistemas;
 - b) O auditor pode ter sido induzido em erro pelo pessoal da entidade;
 - c) O auditor pode ter obtido unicamente uma informação parcial do sistema.
- 3 - Execução de testes de conformidade, que consistem na avaliação preliminar da existência efetiva do controlo interno estabelecido em cada um dos subsistemas. É através desta avaliação que o auditor vai determinar a probabilidade do sistema auditado produzir dados fiáveis.
- 4 - Execução de testes substantivos com o objetivo de obter um grau de confiança razoável de que os procedimentos de controlo estão a ser aplicados de acordo com o pré-estabelecido.

O controlo interno pode ser avaliado tanto pelos auditores internos como externos. Na auditoria interna, segundo Morais e Martins (2013: 41) esta faz-se com o objetivo de expressar opinião acerca da eficácia e eficiência da gestão da entidade, pois auxilia-a nas suas funções. Na auditoria externa, com o objetivo de verificar a conformidade das

operações, com vista a satisfazer as necessidades de terceiros, relativamente à credibilidade da informação financeira. Esta é feita através do levantamento e registo do controlo interno, identificando os pontos fracos e fortes.

A avaliação pelo auditor interno centra-se na preocupação da eficiência e eficácia do sistema e, não apenas na fiabilidade da informação, eficiência das operações e o cumprimento de legislação e regulamentos. Quando o auditor interno realiza uma auditoria, este emite uma opinião sobre o sistema de controlo interno, através de recomendações para melhoria e no acompanhamento do processo de implementação e execução das recomendações.

No âmbito da gestão do risco, após serem dadas as recomendações e, o auditado expõe os planos de ação, as respostas por si emitidas podem ser do tipo:

- De forma a reduzir o risco, em que são introduzidas medidas de controlo de forma a mitigar o risco e assim, aplicadas as recomendações de controlo emanadas no relatório, pelo auditor;
- O auditado/entidade aceita o risco, por vezes acontece quando o nível de risco é reduzido ou quando está associado a processos que também têm oportunidades relevantes;
- Quando se dá a partilha ou diversificação do risco, neste caso pode-se estar, ou não, perante medidas de controlo. No entanto, deve-se, sempre que possível, verificar os controlos das atividades que se partilham.

O processo de avaliação dos controlos inicia-se com a recolha da informação, seguido da aplicação dos testes e respetiva avaliação. Inicialmente, na avaliação preliminar, é determinado como os objetivos de sistema de controlo são afetados, ou seja, é feita a análise ao sistema de controlo interno.

De seguida, aplicam-se os testes de conformidade e substantivo aos controlos. Os testes de conformidade determinam quando os controlos – chave encontram-se em cumprimento, isto é, averigua se o sistema de controlo está implementado e executado de acordo com o que tinha sido estabelecido e, se os procedimentos de controlos estão a ser aplicados. Os testes substantivos têm como objetivo a confirmação de que os objetivos de controlo estão a ser atingidos, através da verificação dos efeitos dos controlos.

Na avaliação preliminar determina-se a adequação dos controlos. Se estes forem adequados realizam-se testes de conformidade e se os resultados forem positivos, realizam-se, com

maior ou menor profundidade, os testes substantivos. Se, pelo contrário, os controles forem inadequados, os testes substantivos são realizados de imediato, reforçando-os em quantidade e/ou profundidade. (Inácio; 2014: 57)

Os princípios-chave de avaliação e aperfeiçoamento do controle interno, segundo o IFAC⁶, representam boas práticas para avaliar e melhorar o sistema de controle interno. Os princípios facilitam a avaliação e aperfeiçoamento, na medida em que destacam áreas onde a aplicação das orientações de desenvolvimento e implementação do SCI falham.

Os princípios – chave, emanados pelo IFAC, no guia de boas práticas, são:

- Suporte dos objetivos da entidade

O controle interno deve ser usado para suportar a entidade no alcance dos objetivos, através da gestão dos riscos, enquanto cumpre com as leis, regulamentos e políticas da entidade.

- Determinar funções e responsabilidades

A entidade deve determinar as várias funções e responsabilidades relativas ao controle interno, incluindo a gestão, a todos os níveis, colaboradores e todos os fornecedores, bem como todos os que colaboram para a entidade atingir os objetivos.

- Promover uma cultura motivacional

A gestão deve promover uma cultura motivacional, de modo a que os colaboradores se sintam motivados, para atuarem em linha com a estratégia da gestão do risco e das políticas de controle interno.

- Ligação com o desempenho individual

A gestão deve fazer a ligação do alcance dos objetivos do controle interno com os objetivos de desempenho individual, pré-estabelecidos para esse colaborador.

- Garantir competência suficiente

Todos os indivíduos da entidade devem deter competências suficientes para garantir que as respetivas responsabilidades relacionadas com o controle interno são totalmente satisfeitas.

⁶ No guia de boas práticas, publicado em junho de 2012, intitulado por *Evaluating and Improving Internal Control in Organizations*.

- Responder ao risco

Os controlos devem sempre ser desenvolvidos, implementados e aplicados de forma a responder a riscos específicos, as suas causas e consequências.

- Comunicar de forma regular

A gestão deve assegurar comunicações regulares relativas ao SCI, bem como dos resultados, para toda a entidade, para assegurar que os princípios do controlo interno são totalmente compreendidos e aplicados por todos.

- Monitorizar e avaliar

O SCI deve ser regularmente monitorizado e avaliado. A identificação de riscos elevados, falhas no controlo ou eventos fora dos limites aceitáveis de risco representam sinais de que o SCI é ineficaz e detém necessidades de aperfeiçoamento.

- Proporcionar transparência e prestação de contas

Compete à gestão reportar periodicamente às partes interessadas, sobre o perfil de risco, bem como a estrutura e desempenho do SCI da entidade.

2.8. O CONTROLO INTERNO E A FRAUDE

A fraude, segundo o IIA, é definida como

[q]ualquer ato ilegal caracterizado por um engano intencional, ocultação ou violação da confiança. Estes atos não dependem da utilização de ameaças de violência ou da força física. As fraudes são perpetradas por indivíduos e por organizações para conseguir dinheiro, bens ou serviços para evitar pagamentos ou perda de serviços ou para obter vantagens pessoais ou de negócio

(IPFF Glossário; 2012)

Segundo a *ISA 240 – The Auditor’s Responsibilities Relating to Fraud in na Audit of Financial Statements*, as distorções nas demonstrações financeiras podem ser o resultado de erro ou fraude. O erro ocorre quando a distorção não é intencional, através de enganos no processamento de dados, estimativas incorretas resultantes de descuidos ou enganos na aplicação de políticas. Por outro lado, a fraude refere-se a um ato intencional, praticado por uma ou mais pessoas, onde são perpetrados enganos com o fim de obter vantagens ilícitas ou ilegais.

Associado à fraude de relato financeiro, citado na ISA 240, este pode estar relacionado com o facto de os gestores ignorarem de forma deliberada os controlos que de outra forma podiam parecer que estavam a funcionar eficazmente, ou seja, a gestão ignora os controlos. Porém, é à gestão da entidade e aos responsáveis pela governação, que cabe a responsabilidade pela prevenção e deteção da fraude. É importante que a entidade crie uma cultura de honestidade e de comportamentos éticos, enfatizando a prevenção da fraude. É através da implementação e manutenção de adequados sistemas contabilísticos e de controlo interno que se pode reduzir, e não eliminar, a possibilidade de fraude. (Baptista da Costa; 2010: 256)

Podem ainda ser distinguidos os conceitos de roubo e fraude. De acordo com Inácio (2014: 63 *apud* Albrecht et al⁷, 2006), roubo é quando se força alguém a dar algo que é dela, através do uso de armas ou força física, enquanto que fraude é quando se retira algo a alguém enganando-a.

Na ocorrência da fraude são tidos como base três componentes. Estes componentes, formulam o triângulo da fraude, desenvolvido na década de 50 por Cressey, que originou da seguinte hipótese:

Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.

Foi através desta hipótese que se formaram as seguintes componentes:

- A pressão representa a razão que motiva o crime, ou seja, que cria a necessidade. Esta pode ser devido a dificuldades financeiras, doença grave, vício ou até a insatisfação por parte dos colaboradores.
- A oportunidade é definida como o método como o crime é cometido. O indivíduo necessita deter os meios para cometer a fraude. Associado a esta componente, está o facto de não existirem controlos ou estes encontrarem-se ultrapassados. São necessários controlos preventivos para proteger contra a possibilidade da ocorrência de fraude.

⁷ Albert, S., Albert, C e Albert, A. (2006); *Fraud examination. Second edition*, Thomson, South-Western

- A racionalização corresponde ao ato de mentalização de que o crime é aceitável. O indivíduo necessita de se justificar de modo a que o ato torne aceitável ou justificável. Usualmente são utilizados como justificações o fato de o indivíduo estar apenas a pedir emprestado, que tinha o direito ao bem, que tinha de cometer o crime pois a família não tinha como se sustentar, entre outros.



Figura 2 – Triângulo da Fraude

Fonte: <http://www.acfe.com/fraud-triangle.aspx>

Surgem, desta forma, os alertas de fraude, comumente conhecidos como *red flags*. Estes são representados por sinais de que algo pode acontecer, tais como, perdas de documentos, incumprimento sistemático de normas, pagamentos em duplicado, sinais exteriores de riqueza, existência de cópias ao invés de originais, entre muitos outros.

No âmbito da avaliação do risco de fraude, cabe aos auditores internos:

- Sensibilizar e recomendar ao órgão de gestão para difundir uma cultura de fraude;
- Dissuadir a fraude através da avaliação da adequação da eficácia do sistema de controlo interno, medindo o grau de exposição ao risco;
- Detetar a fraude no desenvolvimento do trabalho de auditoria, estando alerta a situações em que o controlo interno possa estar enfermo, avaliando a necessidade de investigação mais profunda;
- Investigar a fraude, no que diz respeito à sua extensão, quais os procedimentos e meios utilizados, respondendo às questões quando, como, o quê e a quem;
- Informar a fraude por meio de um relatório, devendo contar as conclusões, as evidências que serviram como base para detetar a fraude;
- Resolução de incidentes de fraude, representam os pontos-chave a implementar para mitigar a fraude, como por exemplo, implementar ou reforçar controlos, complementar procedimentos, entre outros.

Ao criar medidas de controlo, para atingir os objetivos do controlo interno, está-se a diminuir as oportunidades de cometer fraude. Nas entidades em que se encontram implementadas medidas de segregação de funções, controlos de acessos, entre outros, torna-se mais difícil ao perpetrador de cometer a fraude, pois a sua deteção é mais rápida e direta. Nos casos em que a fraude é cometida pela gestão, sendo estes uma das peças fundamentais na criação de um ambiente de controlo, torna-se mais difícil a deteção, para colmatar esta situação é criado um órgão de fiscalização de sociedade independente.

2.9. LIMITAÇÕES DO CONTROLO INTERNO

É importante a este ponto ter em conta, e como constatado no próprio conceito, que por melhor que os controlos sejam desenvolvidos, estes apenas podem providenciar segurança razoável e não de forma absoluta. Desta forma, podem ser classificados um conjunto de fatores inerentes ao controlo interno:

- Fatores económicos: dimensão da empresa, relação custo/benefício e transações pouco usuais;
- Fatores humanos: interesse da gerência/administração, interesse e competência do restante pessoal e atitude permissiva à fraude;
- Fatores tecnológicos: utilização de tecnologias de informação;
- Fatores de mutabilidade: alterações na estrutura da administração, na gestão, no processo produtivo e outros.

(Inácio; 2014: 29)

Com dois dos fatores inerentes de controlo interno, acima descritos, a organização encontra-se menos apta para conseguir atingir os seus objetivos. (Pfister; 2009: 30) Por exemplo, através do fator humano, podem incorrer erros e omissões ou até perpetração de uma fraude.

Aquando do desenvolvimento e implementação do controlo interno é necessário ter conta a relação de custo-benefício. Segundo Pfister (2009: 31), a otimização dos custos totais é possível quando os custos operacionais para o controlo interno são balanceados com o custo do erro aquando da tomada de decisão, perda de ativos e no risco residual.

Se o sistema de controlo interno for eficaz em relação aos custos, ou seja, desenvolvido segundo um rácio de custo-benefício, previamente limitado, isto significa que o custo da implementação de um controlo, não excede os benefícios que se espera extrair do mesmo.

Cabe à gestão realizar o mapeamento de julgamentos e estimativas quantitativas e qualitativas na avaliação do custo-benefício.

O fator humano detém uma grande importância em todo este ponto. O ser humano pode sempre errar por distração, fadiga, negligência, incompreensão de instruções, erros de julgamento e apreciação, os considerados erros não intencionais. Quanto aos erros intencionais, estes relacionam-se com a falta de integridade, que resultam em comportamentos fraudulentos, podendo ter resultado de conluio na entidade e fora. (Inácio; 2014: 30)

Para além das falhas intencionais ou não, a gestão pode sempre sobrepor-se aos controlos e, não seguir com as políticas e procedimentos para ganhos pessoais ou para omitir a verdadeira conjuntura da entidade.

O controlo interno contribui para minimizar este tipo de erros e falhas, porém não consegue garantir total segurança. É importante a integridade da gestão e dos colaboradores que laboram para o interesse do sucesso da entidade.

A limitação de recursos tecnológicos, que por vezes encontra-se relacionada com fatores económicos, contribuem não só de forma positiva como também negativa. Estas tornam vulnerável o acesso aos dados, porém permitem a uniformização da aplicação dos procedimentos de controlo. O fato de serem introduzidos nas próprias tecnologias, podem permitir que sejam acedidos de forma não autorizada e alterados inadequadamente. (Inácio; 2014: 31)

Como visto anteriormente, a atualização do conceito de controlo interno tem vindo a acompanhar a mutabilidade vivida no tempo e no espaço, pois sabe-se que não existe um controlo interno padronizado e imutável. São várias as modificações que levam a que o controlo interno deixe de estar adequado, nomeadamente na «mudança de titulares de capital ou de controlo, mudança na gestão, nos órgãos de governo das sociedades ou outro pessoal, ou alterações no mercado ou na indústria da entidade.» (Inácio; 2014: 31)

Conclui-se que as limitações do sistema de controlo interno determinam a exatidão dos resultados a produzir. É importante à gestão deter conhecimento das limitações na tomada de decisões, pois são estes quem mais utiliza a informação monitorizada e produzida pelo controlo interno.

3. MODELO COSO

3.1. ORIGEM DO MODELO

Para conseguir determinar origem do modelo, é necessário recuar no tempo, nomeadamente ao período compreendido entre 1970 e início de 1980. Este período foi caracterizado pelo insucesso de grandes entidades, devido à inflação, elevadas taxas de juro e abordagens à contabilidade muito agressivas, isto é, uso de métodos mais antiquados, não tão usuais, como por exemplo do LIFO⁸ ao invés do FIFO⁹ ou no uso de métodos de depreciação que beneficiem o ativo, entre outros.

O insucesso de muitas entidades deu-se com a crise financeira, causada pela apresentação de Relatórios e Contas fraudulentos, ainda que fossem auditados e mostrassem que pelas contas a entidade não detinha quaisquer problemas financeiros. Após várias tentativas de correção, através de legislação, as lacunas dificilmente detinham melhorias era bem-sucedidas.

Foi com a constituição do grupo do setor privado, o *National Commission on Fraudulent Financial Reporting*, que foi possível através de estudos mais aprofundados a estes casos que levavam ao relato financeiro fraudulento, que foi possível obter resultados significativos que pudessem vir a mudar a forma como se aborda este tema. Na comissão faziam parte o *American Institute of Certified Public Accountants* (AICPA), o *Institute of Internal Auditors* (IIA), a *Financial Executives Institute* (FEI), o *American Accountant Association* (AAA) e o *Institute of Management Accountants* (IMA). Fizeram também parte, representantes de área industrial, contabilidade pública, entidades de investimento e o *New York Stock Exchange* (NYSE).

A nomenclatura da comissão, proveniente do primeiro presidente da *SEC Commission*, James C. Treadway, Jr., na altura ficou conhecida como *Treadway Commission*. Nos dias que correm, é mais usual a utilização do acrónimo COSO, que expressa o *Committee of Sponsoring Organizations of The Treadway Commission*.

O comité COSO tem como missão fornecer liderança através do desenvolvimento de *frameworks* e orientações no que concerne à gestão do risco, controlo interno e dissuasão da

⁸ LIFO – *Last In First Out*

⁹ FIFO – *First In First Out*

fraude. A sua conceção teve com objetivo melhorar o desempenho organizacional e de governança e, na redução de fraude nas entidades.¹⁰

O foco inicial relaciona-se com a temática do controlo interno na qual contribuíram as falhas do relato financeiro fraudulento. O primeiro relatório emanado pelo COSO, o Treadway Report, em 1987, advertia a gestão para que esta se pronunciasse acerca da eficácia do sistema de controlo interno. Este relatório dá ênfase aos elementos de um SCI eficaz, onde inclui um ambiente de controlo forte, um código de conduta, um comité de auditoria competente e envolvido e, uma gestão forte. Não obstante à importância destes elementos, foi necessário definir o termo controlo interno, para que fosse consistente, reconhecido e aceita a nível mundial. Mais tarde, em 1992, foi emitido o relatório, denominado de *Internal Control – Integrated Framework* (ICIF) onde foram abordados todos estes temas. (Moeller; 2007: 3)

Em 2004, o COSO emitiu um segundo relatório, o *Enterprise Risk Management – Integrated Framework*, conhecido como *COSO-ERM*. Este foca-se no envolvimento da gestão, ou seja, o *corporate governance* e a *gestão do risco*, representado uma expansão do ICIF.

A última atualização, em 2013, teve por base o ICIF, onde foram mantidos os objetivos e os componentes, com reforço no que respeita à ampliação dos objetivos operacionais e de relato e, na definição dos 17 princípios, por si associados com os diferentes componentes. (Inácio; 2014: 35)

A visão do COSO é ser um líder reconhecido a nível mundial, no que diz respeito ao desenvolvimento de orientações nas áreas do risco e controlo que permitam uma boa governação organizacional e redução da fraude.¹¹

3.2. MODELOS COSO

Tal como referido acima, são vários os modelos de controlo interno, porém o mais utilizado e que apresenta maior aceitação a nível mundial, em parte devido ao fato de estar subjacente às *International Standards on Audit*, do IAASB, é o modelo COSO.

¹⁰Tradução própria: *The Committee of Sponsoring Organizations' (COSO) mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.*

¹¹ Tradução própria: *COSO's vision is to be a recognized thought leader in the global marketplace on the development of guidance in the areas of risk and control which enable good organizational governance and reduction of fraud.*

3.2.1. INTERNAL CONTROL – INTEGRATED FRAMEWORK

A definição de controlo interno, com a publicação do ICIF, veio estabilizar a preconização que se detinha com este, nomeadamente na interpretação que cada um fazia, levando à criação de confusão entre quem aplicava este conceito, quem o legislava e regulava.

Em 1992, com a publicação do ICIF, foi possível estabelecer a definição de controlo interno, de modo a que respondessem às necessidades de todas as partes e que fosse colocada à disposição orientações para todas as entidades. Desta forma, o controlo interno ficou definido como

[u]m processo realizado pelo Conselho de Administração, Direção e outros membros da organização com o objetivo de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos:

- Eficácia e eficiência das operações;
- Fiabilidade da informação financeira;
- Cumprimento das leis e normas estabelecidas.

(Internal Control - Integrated Framework, p. 3)

As três categorias de objetivos encontram-se diretamente relacionadas com os objetivos da entidade, no que seja relativo a desempenho e rendibilidade, de recursos, bem como no que diz respeito à informação que é apresentada às partes interessadas, por forma a que detenham toda a informação e esta seja a verdadeira imagem da entidade e, para tal que seja cumprida a legislação a que está sujeita. *(Internal Control – Integrated Framework)*

Cabe à gestão, com a supervisão da administração, definir os objetivos da entidade de acordo com a missão, visão e estratégias da entidade. Quando os objetivos do controlo interno estão em pleno funcionamento, pode-se afirmar que o sistema de controlo interno opera de forma eficaz e eficiente. *(Internal Control – Integrated Framework)*

Em 1992, a edição do ICIF pelo COSO constituiu um grande auxílio para as empresas cotadas publicamente a aderirem ao *SOX Act Section 404*, respeitante à “Avaliação da Gestão dos Controlos Internos”.

Mais tarde, e após a entrada do COSO-ERM, com os avanços tecnológicos, o ambiente regulador encontra-se mais exigente, com penas mais severas, também com a globalização os negócios aumentam e evoluem mais rapidamente. Todos estes fatores em conjunto,

levaram a que a estrutura original do modelo fosse ultrapassada. Com a valorização da eficiência operacional e, com a nova estrutura, foi possível cobrir as áreas mais críticas do negócio no que respeita ao relato, ao *compliance* e à gestão das operações. Posto isto, são facilmente observáveis as mudanças na estrutura do modelo.

A estrutura do modelo COSO, é configurada através de uma estrutura tridimensional, onde se interligam os componentes, os objetivos do controlo interno e os níveis de controlo a serem aplicados na entidade, departamento, unidade operacional e função, tal como apresentado na figura 6. Este caracterizado por um cubo, com linhas, que representam os cinco componentes, linhas no topo retratam as três categorias dos objetivos e, as colunas, no cubo de 1992, apenas estavam divididas por unidades e atividades, em 2013, foram substituídas pelas dimensões da entidade.

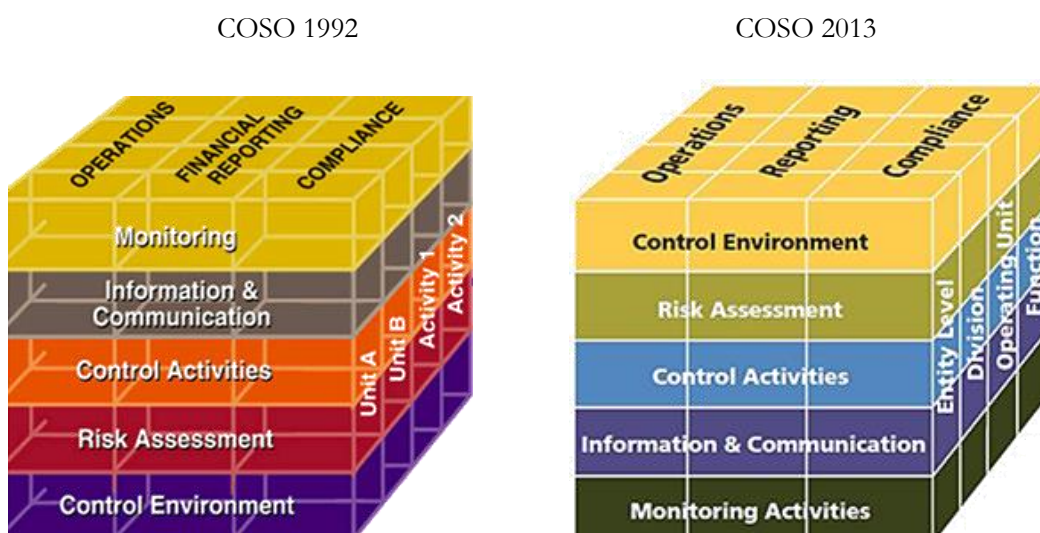


Figura 3 – Estrutura do modelo COSO 1992 e 2013
 Fonte – www.coso.org

No cimo do cubo, as categorias de objetivos, de 1992 para 2013, mantiveram-se, passando o relato financeiro apenas a relato. Esta mudança é refletida na abrangência da aplicação da *framework*, não cingindo apenas ao nível de relato financeiro, podendo assim aplicar-se ao relato interno e externo e, de medidas não financeiras.

Na face do cubo, pode-se observar que os componentes trocaram de ordem e que a categoria monitorização passou para atividades de monitorização, mantendo-se as restantes com o mesmo conceito. Esta última modificação prende-se com a perceção de monitorização como uma série de atividades desencadeadas como parte de cada um dos restantes componentes.

No lado do cubo, a estrutura organizacional, foi onde se obteve a maior mudança, relativamente ao modelo de 1992. A alteração encontra-se alinhada com o COSO-ERM, de forma a ilustrar que uma estrutura de controlo interno eficaz atravessa toda a entidade, a todos os níveis funcionais, de forma dependente e independente. Ainda que haja esta correlação com o modelo ERM, estes mantem-se separados.

Em 2013, deu-se a introdução dos princípios (abaixo detalhados) necessários para um controlo interno eficaz. Há que notar, que a gestão da entidade pode não achar relevante qualquer um dos princípios, baseado numa qualquer circunstância. Porém, a não presença e funcionamento de um dos princípios revela-se ser uma deficiência no sistema de controlo interno. É também, com o auxílio dos princípios, que a gestão pode, de forma mais bem-sucedida, reconhecer problemas e assegurar a eficácia do controlo interno e, no relato financeiro externo auxiliar na prevenção de fraquezas materiais ou nas deficiências mais expressivas.

Pode-se observar que o modelo do COSO agrupa os objetivos em três categorias:

- A eficácia e eficiência das operações da entidade, incluindo objetivos de desempenho a nível operacional e financeiro, bem como na salvaguarda de ativos contra perdas.

Os objetivos operacionais relacionam-se com a consecução da missão e visão da entidade, ou seja, a razão fundamental da existência da mesma. A missão e visão das entidades varia consoante as escolhas da gestão no que respeita ao modelo operacional, a indústria em que opera, assim como o próprio desempenho da entidade. As opções da gestão podem variar desde a nível de desempenho financeiro, de produtividade, qualidade, práticas ambientais, inovação, etc. Quando estas não se encontram bem definidas, na medida em que se encontram alinhadas com a missão e visão, os recursos podem ser mal direcionados.

- O reporte, referente à comunicação financeira e não financeira, interna e externa.

Engloba a fiabilidade, oportunidade, transparência e outras características definidas pelos reguladores, organismos de normalização ou políticas da entidade.

- A conformidade com as leis e regulamentos aos quais a entidade está sujeita.

Este objetivo relaciona-se com a capacidade de aderência a leis e regulamentos a aplicar, nomeadamente quais as aplicáveis ao negócio da entidade.

Os objetivos devem ser examinados pela aplicabilidade para cada atividade e unidade operacional da entidade. Cada combinação de atividade ou unidade e objetivo deve abordar cada um dos cinco componentes.

A relação entre objetivos e componentes é representada por uma relação direta, na medida em que, através dos componentes, direcionados para cada estrutura organizacional, que a entidade necessita de se focar para alcançar objetivos.

3.2.1.1. Componentes do modelo COSO

As cinco componentes do modelo interrelacionadas, funcionam como um todo, pois focando-se no alcance dos objetivos:

- O **ambiente de controle** representa a consciencialização e as ações da gestão e do órgão de gestão, relativo ao sistema de controlo interno e a sua importância dentro e fora da entidade, fornecendo disciplina e estrutura e, influenciando a consciência de controlo de todas as pessoas da entidade.

Cabe à estrutura de governação e alta administração estabelecer uma norma sobre a importância do controlo interno, bem como de normas de conduta esperadas, onde são incluídos um conjunto de fatores, como integridade, competência, estrutura organizacional, atribuição de autorizações e responsabilidades. Estes fatores determinam parte das limitações do controlo interno, encontrando-se associadas ao risco de existência de distorções. (Inácio; 2014: 38)

A esta componente encontram-se associados os cinco primeiros princípios do COSO de 2013.

- A **avaliação de riscos** é a identificação e análise dos riscos que podem deter impacto para a realização dos objetivos, permitindo obter sustentação na forma como devem ser geridos.

Para avaliar os riscos, é necessário determinar o grau de risco, ou seja, da sua significância à frequência com que ocorre e, como deve ser gerido e ações a tomar de forma a mitigá-lo. A avaliação de riscos é caracterizado por ser uma atividade com um processo dinâmico e contínuo.

Neste componente podem-se ver associados os quatro seguintes princípios do COSO de 2013.

- As **atividades de controlo** incluem as políticas e procedimentos que asseguram que os objetivos são alcançados, que mitigam o risco, assim como asseguraram a que as ações identificadas para responder aos riscos foram tomadas.

Os controlos podem ser preventivos ou detetivos. Os primeiros previnem a ocorrência de erros, são fundamentais para a eficácia e eficiência do sistema de controlo interno. E controlos detetivos, que permitem detetar os erros, detêm grande importância na medida em que após a ocorrência do erro é necessário corrigi-lo, sendo para tal necessário manter informações dos procedimentos.

Aqui são incluídos os princípios 10 a 12 do modelo COSO de 2013.

- A **informação e comunicação** revela-se necessária para que a entidade cumpra as responsabilidades de controlo interno, é feito através da identificação, recolha e troca de informação entre os colaboradores para que levem a cabo as suas responsabilidades.

O sistema de informação e comunicação numa entidade deve garantir que subsiste a compreensão clara do papel e responsabilidades dentro da estrutura do sistema de controlo interno de cada estrutura organizacional.

É através de comunicações internas que a informação privilegiada é transmitida por toda a organização, fluindo em todas as direções, desta forma todos os colaboradores sabem quais as responsabilidades que lhes são atribuídas. As comunicações de ordem externa permitem à entidade obter informação relevante e, fornece informações a terceiros, como resposta a requisitos e expectativas.

Os princípios 13 a 15, do modelo COSO (2013) estão associados a esta componente.

- A **monitorização de atividades** é um processo que avalia a qualidade do desempenho do controlo interno, permitindo uma adequada manutenção deste. Este processo deve ser contínuo, para que permita a maximização das características do controlo interno. (Inácio; 2014: 48)

Desta forma, a monitorização proporciona informação sobre os restantes componentes e se funcionaram efetivamente para permitirem o alcance dos objetivos. Pela importância do componente, esta temática a aprofundar o capítulo 4.2.

Esta componente está presente nos dois últimos princípios do modelo COSO de 2013.

3.2.2. Princípios e Áreas de Foco

Os princípios mencionados acima, representam conceitos fundamentais associados às componentes. É através da aplicação de todos os princípios que uma entidade pode deter um controlo interno eficaz, pois estes são originados diretamente dos componentes, ou seja, todos os princípios aplicam-se aos objetivos operacionais, de divulgação e de conformidade. Segundo COSO de 2013, os princípios associados aos componentes encontram-se descritos da seguinte forma:

- **Ambiente de controlo**

1 – A organização demonstra ter um compromisso com valores éticos e de integridade.

O órgão de administração deve estabelecer normas padrão e mecanismos de forma a que a organização entenda e adira ao que é eticamente correto e, defina o processo e recursos para interpretar e abordar desvios.

2 – Os órgãos de direção são independentes dos da gestão e dos supervisores responsáveis pelo desenvolvimento e desempenho do controlo interno.

É necessário o órgão de administração conhecer o negócio, as expectativas dos acionistas, clientes, colaboradores, investidores e do público em geral, bem como os requisitos jurídicos e regulamentares e riscos relacionados.

3 – O conselho de administração estabelece, juntamente com a supervisão estruturas, linhas de reporte e níveis de delegação de competências e responsabilidades alinhadas com os objetivos da entidade.

O órgão de administração estabelece a estrutura organizacional e as linhas de reporte necessários de forma a planear, executar, controlar e avaliar periodicamente as atividades da entidade.

4 – A organização compromete-se a atrair, desenvolver e manter os colaboradores com as competências necessárias para o cumprimento dos objetivos.

Para tal, é necessário a existência de políticas e práticas para a definir as competências necessárias na organização, que providenciam um conjunto de procedimentos detalhados para executar e avaliar o desempenho, bem como para determinar ações corretivas, se necessários.

5 – A organização mantém os colaboradores conscientes das suas responsabilidades pelo controlo interno com vista ao alcance dos objetivos.

O conselho de administração mantém o diretor executivo consciente por compreender os riscos que a entidade se depara e, estabelece os requisitos do sistema de controlo interno de suporte ao alcance dos objetivos da organização.

- **Avaliação de riscos**

6 – A organização estabelece objetivos suficientemente claros, a fim de permitir a identificação e avaliação de riscos relacionados com os objetivos.

Este princípio encontra-se organizado em três secções, nomeadamente os três objetivos: operacionais, de relato financeiro externo, não financeiro externo e interno e, de *compliance*.

7 – A organização identifica os riscos à realização dos objetivos por toda a organização e analisa os riscos como base para determinar a gestão dos mesmos.

É caracterizado por ser um processo contínuo, que habilita a organização a atingir os objetivos, devendo para tal considerar os riscos a todos os níveis, por forma a poder tomar alguma ação corretiva atempadamente

8 – A organização considera a possibilidade de existência de fraude na avaliação dos riscos com impacto no alcance dos objetivos.

A este nível, é importante considerar os vários tipos de fraude, avaliar os incentivos e pressões, as oportunidades, bem como atitudes e racionalização.

9 – A organização identifica e avalia alterações que possam ter impacto significativo no sistema de controlo interno.

As mudanças mencionadas podem ser do tipo: ambiente externo, modelo de negócio, administração, bem como operações, tecnologias de informação, relação com os prestadores de serviço.

- **Atividades de controlo**

10 – A organização seleciona e desenvolve atividades de controlo que contribuem para a mitigação dos riscos relacionados com o alcance dos objetivos, para níveis aceitáveis.

Para selecionar e desenvolver atividades de controlo, é crucial ter em consideração os fatores específicos da organização, nomeadamente relacionados com o negócio da mesma, desta

forma, determinar os processos relevantes. A este ponto é importante integrar a avaliação do risco.

11 – A organização seleciona e desenvolve atividades de controlos gerais de tecnologias que suportem o alcance dos objetivos.

Com a maior dependência do uso de tecnologias, é imperativo o recurso aos controlos de atividades nas infraestruturas tecnológicas, no processo de gestão de segurança, bem como na aquisição, desenvolvimento e manutenção.

12 - A organização seleciona e desenvolve atividades e controlos através de políticas que estabelecem expectativas e definem procedimentos que coloquem essas políticas em prática.

Por forma a suportar a implementação de atividades de controlo, é necessário estabelecer políticas e procedimentos. É, por sua vez, também indispensável realizar avaliações, numa base periódica, para poder tomar ações corretivas atempadamente.

- **Informação e comunicação**

13 – A organização obtém ou gera e utiliza informação com qualidade e relevância para apoiar o funcionamento do controlo interno.

Para tal, identifica os requisitos de informação, verifica as fontes dos dados (internas ou externas), realiza o processamento da informação relevante e, tem em conta a conservação da qualidade da informação durante o processo, tudo isto, considerando o rácio custo/benefício.

14 – A organização comunica internamente informação, incluindo objetivos e responsabilidades de controlo interno, necessárias para suportar o seu funcionamento.

Por forma a comunicar informação de controlo interno internamente, é necessário ter em conta o público-alvo, mantendo assim vários métodos e linhas separadas de comunicação. Importante, também, manter uma linha de comunicação direta com o órgão de administração.

15 – A organização comunica com entidades externas sobre matérias que afetam o funcionamento do controlo interno.

A comunicação externa, tal como a interna, deve manter vários métodos e linhas separadas de comunicação. Deve permitir a receção de comunicações externas.

- **Monitorização de atividades**

16 – A organização seleciona, desenvolve e executa avaliações contínuas e independentes para se certificar de que todos os componentes de controlo interno estão presentes dentro da organização e, se estes se encontram a funcionar.

Por forma a realizar as avaliações é essencial ter em conta os processos de negócio, ajustar o âmbito e frequência destas, com o recurso a trabalhadores qualificados. Dar uso a uma base de entendimento para estabelecer planos para avaliações contínuas e independentes. Ter em consideração a monitorização nos vários níveis da organização, bem com aos prestadores de serviços. Quando possível, recorrer à tecnologia no contexto da monitorização.

17 – A organização avalia e comunica as deficiências de controlo interno de forma atempada às partes responsáveis por tomar as medidas corretivas, incluindo o conselho de administração e órgão de direção.

Por forma a superar as deficiências, estas são, após avaliação, reportadas ao órgão do processo analisado, mantendo reportes e realizando *follow-ups* aos planos de ação estabelecidos pelos detentores do processo.

A cada um destes princípios encontram-se associadas áreas de foco, explicadas de forma sucinta acima (Anexo 2), perfazem um total de 87. Estes encontram-se subdivididos da seguinte forma:

Componentes	Princípios	Nº de Áreas de Foco					
<table border="1"> <tr><td>Control Environment</td></tr> <tr><td>Risk Assessment</td></tr> <tr><td>Control Activities</td></tr> <tr><td>Information & Communication</td></tr> <tr><td>Monitoring Activities</td></tr> </table>	Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring Activities	1. Compromisso com integridades e valores éticos.	4
	Control Environment						
	Risk Assessment						
	Control Activities						
	Information & Communication						
	Monitoring Activities						
	2. Conselho de administração de supervisão independente.	4					
	3. Estruturas, linhas de reporte, autoridade e responsabilidade.	3					
	4. Atrair, desenvolver e reter trabalhadores competentes.	4					
	5. Responsáveis pelo controlo interno.	5					
	6. Objetivos claros e específicos.	15					
	7. Riscos identificados para a realização dos objetivos.	5					
	8. Considerar o potencial para a fraude.	4					
	9. Identificação e avaliação de mudanças significativas.	3					
	10. Selecionar e desenvolver atividades de controlo.	6					
	11. Selecionar e desenvolver controlos gerais de Tecnologias de Informação.	4					
	12. Controlos implementados através de políticas e procedimentos.	6					
13. Qualidade da informação obtida, gerada e utilizada.	5						
14. Comunicação interna da informação de controlo interno.	4						
15. Comunicação externa da informação de controlo interno.	5						
16. Condução de avaliações contínuas ou separadas.	7						
17. Avaliação e comunicação das deficiências de controlo interno.	3						

Figura 4 – Associação das Componentes, Princípios e Nº de Áreas de Foco do Modelo COSO
Fonte – Própria

Embora seja reconhecido que o controlo interno garante uma segurança razoável, este também possui limitações. O controlo interno não possui capacidade de impedir decisões ou acontecimentos externos à entidade que esta não detenha controlo, ou seja, o sistema de controlo interno pode estar implementado de forma eficaz e eficiente e no entanto apresentar falhas. Estas situações resultam da falha e tendência no julgamento humano aquando da tomada de decisões decorrentes de erros ou falha do próprio. A possibilidade que o órgão de gestão, colaboradores e terceiros detém em sobreporem-se ao controlo interno, por vezes em coluio entre estes.

3.2.3. ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK

O modelo *Enterprise Risk Management* (ERM) incorpora o *Integrated Framework* alargando-o para o tema da gestão do risco empresarial. A necessidade de definir o conceito de gestão de risco, levou a que o COSO, em conjunto com a *Pricewaterhouse Coopers* (PwC), em 2001, desenvolvessem um conceito comum e consistente. O resultado desta união foi o *COSO ERM Framework*, onde foram desenvolvidos os principais tópicos de controlo, tornando-os mais abrangentes e extensos, no que à gestão de riscos diz respeito.

A falência e escândalos de grandes empresas, como a *Enron*, *Tyco International*, *Peregrine Systems* e *WorldCom*, levaram a que muitos investidores, colaboradores e terceiros entrassem em prejuízo, conduzindo assim a uma maior preocupação com o *corporate governance* e com a gestão do risco. De forma a colmatar esta situação, foi desenvolvido o *COSO ERM*, com princípios e conceitos fundamentais, através de uma linguagem comum, com direções e orientações claras.

O *ERM Integrated Framework* (2004; 2) define gestão de riscos da empresa como

[u]m processo efetuado numa entidade pelo conselho de administração, direção e demais empregados, aplicado na definição da estratégia em toda a entidade, desenhado para identificar potenciais eventos que possam afetar a entidade, e gerir os riscos de acordo com o apetite ao risco, de forma a providenciar segurança razoável no que diz respeito ao alcance dos objetivos da entidade.¹²

Assim como o *Internal Control – Integrated Framework*, também o *Enterprise Risk Management* detém uma estrutura tridimensional, a face, representada pelos componentes,

¹² Tradução própria. Original: *process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

o topo com os objetivos e as colunas configuradas pelas unidades da entidade. Tal como no modelo anterior, existe um relacionamento direto entre as faces do cubo, nomeadamente, a entidade pretende alcançar os objetivos através da aplicação dos componentes da gestão de riscos, aplicado a qualquer uma das unidades da entidade.

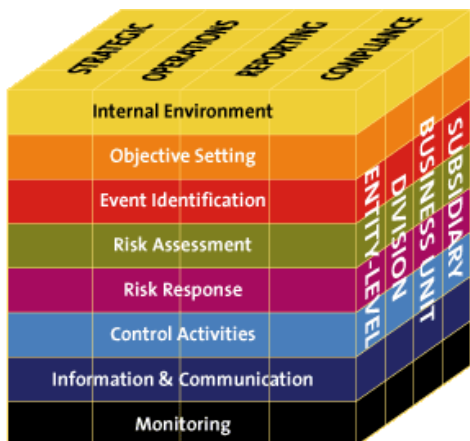


Figura 5 – Estrutura do modelo COSO – ERM

Fonte – www.coso.org

Em comparação com o modelo ICIF, pode-se observar que neste modelo subsistem mais componentes, designadamente:

- Na **definição de objetivos** estratégicos, estes devem cobrir operações, o relato e as atividades de conformidade. A definição de objetivos é um pré-requisito à identificação de eventos, à avaliação de riscos e às respostas aos riscos.

Devem ser objetivos gerais de forma a alcançar a missão e visão da entidade, para depois selecionar, desenvolver e implementar objetivos a nível operacional, de relato e de conformidade.

Não só devem estar em linha com a missão, como também ser compatíveis com o apetite ao risco. A entidade deve estabelecer qual o apetite ao risco tolerável, ou seja, que a entidade está disposta a aceitar. (Moeller; 2007)

- A correta **identificação de eventos**, quer sejam gerados interna ou externamente, pode afetar a realização dos objetivos da entidade de forma positiva. Na identificação de eventos, estes podem surgir como riscos, oportunidades ou ambas as situações. Um ponto importante nesta fase é a análise de informação existente de forma a poder evitar riscos e tirar partido das oportunidades. (Moeller; 2007)
- Após a identificação e avaliação, segue-se a forma de **resposta aos riscos**, podendo esta ser, evitar, reduzir, partilhar ou aceitar os riscos. É responsabilidade da

gestão rever a probabilidade do risco estimado e o potencial impacto e, após balancear os custos e benefícios associados, desenvolver estratégias apropriadas para responder ao risco. (Moeller; 2007)

Tal como o ICIF, também o ERM detém limitações, desde o julgamento humano, que leva a erros e equívocos, o coluio entre indivíduos, a possibilidade de a gestão poder desabilitar o processo da gestão de riscos, inclusive na resposta ao risco e nas atividades de controlo e, a necessidade de considerar os custos e benefícios associados às respostas aos riscos.

O modelo COSO ERM, sendo mais abrangente que o ICIF, detém como pontos principais, segundo Moeller (2007; 53-55), o fato de:

- O ERM ser um processo de gestão de riscos, que pelas suas características não é estático. Pelo facto de ser flexível, é difícil estabelecer regras específicas e restritas, é, portanto, necessário que haja uma série de passos documentados de forma a rever e avaliar potenciais riscos, para a entidade poder tomar ações tendo em conta um conjunto de fatores.
- O ERM é implementado pelos colaboradores da entidade, pois são estes que detêm o conhecimento das suas funções. O processo da gestão do risco deve ser feito por quem se encontra informado da situação de risco, de forma a poder entender os fatores que o envolvem e das respetivas implicações.
- O ERM deve ser aplicado na escolha de estratégias por toda a entidade, através de uma abordagem que mistura atividades de baixo e alto risco.
- Deve ser tido em consideração o conceito de apetite ao risco. Alguns gestores podem aceitar riscos mais elevados e daí resultarem mais e melhores proveitos, encontrando-se dependente do risco que estes estão dispostos a aceitar de modo a alcançar os objetivos.
- O ERM faculta uma segurança razoável e não efetiva na concretização dos objetivos, isto é, independentemente do quão bem pensado e implementado se encontra o modelo, este não dá uma garantia segura dos resultados, colocando-se em causa o julgamento humano, como erros, falhas e fraudes bem como proveniente de fatores naturais adversos.
- O ERM foi desenhado de forma a auxiliar o alcance dos objetivos, quer seja através da manutenção de uma boa reputação, dentro e fora da entidade, através da

divulgação de relatórios financeiros credíveis e de operar em conformidade com leis e regulamentos.

Pode-se concluir que o modelo COSO-ERM é mais abrangente que o ICIF, pois segue orientações dirigidas ao risco, nomeadamente à avaliação e resposta ao risco. Cada área da entidade deve deter uma avaliação ao risco e registar o risco aceitável tendo em conta a estratégia da gestão. No compêndio de todos os relatórios das áreas, dever-se-á obter para cada atividade, o grau e tipo de risco, o detentor do mesmo e o plano de ação necessário para atingir os objetivos. (Pickett; 2003: 159)

3.3. EFICÁCIA E EFICIÊNCIA DO CONTROLO INTERNO

De uma forma geral, a descrição de eficácia e eficiência é representada pelo grau em que os objetivos estabelecidos são alcançados e que para tal devem-se encontrar estabelecidas métricas e critérios de mensuração apropriados à entidade.

De acordo com o AICPA, um sistema de controlo interno adequado, eficaz e eficiente pode ser caracterizado pelos dois tipos de controlo interno, administrativo e contabilístico. Porém, as matérias do âmbito do controlo interno estendem-se para além dos tipos de controlo. É necessário que estejam em consonância com os componentes apresentados no modelo COSO e, que acima de tudo, se encontre em funcionamento por forma a garantir eficiência e eficácia organizacional. (Gomes; 2014: 12)

Para o COSO, os três principais requisitos para um controlo interno eficaz passam por alcançar os objetivos de forma a cobrir, preferencialmente, todas as categorias de objetivos, cada uma das componentes e princípios relevantes devem estar presentes e a funcionar em conjunto de uma forma integrada.

Por presente entende-se que as componentes e princípios relevantes subsistem na construção e implementação do sistema de controlo interno para atingir objetivos específicos. Se estiver em funcionamento denota-se pelo facto de continuar a existir na condução do sistema de controlo interno de forma a alcançar os objetivos.

A funcionar em conjunto de forma integrada demonstra que no conjunto das componentes, em funcionamento, é possível reduzir, até um nível aceitável, o risco de não atingir um objetivo.

A gestão pode demonstrar que as componentes se encontram a operar em conjunto quando estão presentes e a funcionar e, quando as deficiências de controlo interno agregadas às componentes não resultam na determinação de que existem maior ou mais deficiências.

Para reduzir, a um nível aceitável, o risco de não alcançar os objetivos da entidade, os modelos estabelecem requisitos para um sistema de controlo interno eficaz, relacionando as três categorias dos objetivos. Para tal, é necessário que:

- Os cinco componentes e princípios relevantes estejam presentes e a funcionar. “Presente” refere-se à determinação de que os componentes e princípios pertinentes existem na conceção e implementação do sistema de controlo interno para alcançar os objetivos específicos. “Funcional” refere-se à determinação de que os componentes e os princípios relevantes continuam a existir nas operações e condutas do sistema de controlo interno para alcançar os objetivos específicos.
- Os cinco componentes funcionam em conjunto de forma integrada. A “operar em conjunto” refere-se à determinação de que todos os cinco componentes reduzem coletivamente, a um nível aceitável, o risco de não alcançar um objetivo. Os componentes não devem ser considerados de forma discreta; ao invés operam juntos como um sistema integrado. Os componentes são independentes com uma multiplicidade de inter-relações e ligações entre eles, em particular na maneira como os princípios interagem dentro e entre componentes.

(COSO 2013 – *Executive Summary*; 2013: 8)

Para que a administração e a estrutura de governança considere o sistema de controlo interno eficaz, é necessário que esta detenha segurança razoável quanto à eficiência e eficácia das operações, tendo em consideração eventos externos e a gestão destes, de forma a reduzir o impacto a um nível aceitável; de que a organização elabore divulgações em conformidade com as leis, normas e regulamentos e realize a respetiva observância.

Segundo Marçal e Marques (2011: 14) a obtenção de um sistema de controlo interno eficaz e eficiente, requer que se encontrem fundamentados um conjunto de princípios:

- A segregação de funções, pelo facto de haver separação de funções incompatíveis. Com o fim de precaver que uma pessoa detenha várias funções acessórias, de forma a impedir ou interpelar a prática de erros, irregularidades ou a sua simulação;

- O controlo de operações, com o objetivo de verificação de operações, deverá ser realizado por pessoas que não intervêm na realização da mesma, para que se cumpra o critério anterior;
- A definição de autoridade e responsabilidade foca-se na definição clara e rigorosa da estrutura de autoridade e responsabilidade de qualquer operação. Deve ser entendido por todos, através da fixação e delimitação de funções de cada um;
- As competências dos colaboradores devem encontrar-se devidamente adequadas ao exercício das suas funções, no que diz respeito a habilitações e experiência;
- O registo dos factos, nomeadamente os registos contabilísticos, que se destina a verificar a ligação entre os serviços, a acelerar o processo de registo das operações e, a fornecer a informação com rapidez, precisão e clareza à gestão.

Para um sistema de controlo interno eficaz não é apenas necessário seguir políticas e procedimentos, é também necessário usar o julgamento. A gestão aplica o julgamento quando:

- Aplica as componentes do controlo interno em relação às categorias de objetivos e princípios dentro da estrutura da entidade;
- Especifica os objetivos adequados e avalia os riscos de forma a concretizar esses objetivos;
- Seleciona, desenvolve e implementa os controlos necessários aos princípios; e,
- Avalia se as componentes estão presentes a funcionar e a operar em conjunto, se os princípios são relevantes para a entidade e estão presentes e em funcionamento e, avalia a gravidade das deficiências de controlo interno.

Uma auditoria com base no modelo COSO, pode garantir, segundo Gomes (2014: 16):

- Eficácia, através do teste de todos os cinco componentes de controlo, pois estes fornecem um suporte sólido que determina um grau de segurança provido dos controlos;
- Eficiência, pelo enfoque numa categoria de objetivos protege contra a problemática da abrangência indefinida, que pode acarretar elevados custos;
- Possibilidade de comparação, pelo uso de uma estrutura de auditoria e sistema de avaliação comum;

- Comunicação com os clientes, pela inclusão dos critérios do modelo COSO e dos respetivos conceitos; e,
- Ao Comité de Auditoria, pela introdução de relatórios baseados na estrutura do modelo, auxiliam a visualizar os pontos fortes e fracos do sistema de controlo interno.

A avaliação do sistema de controlo interno é importante e necessária ao trabalho dos auditores, pelo facto de que determina o risco de distorção material no planeamento de cada auditoria. Por sua vez, torna-se indispensável o conhecimento dos objetivos, componentes e tipologia dos controlos na avaliação do sistema de controlo interno.

3.4. RESPONSABILIDADES

A forma como o sistema de controlo interno é colocada em prática depende de cada parte interessada, ou seja, ainda que todos os colaboradores da entidade possuam alguma responsabilidade, esta aumenta tanto quanto o cargo que possuem.

A gestão é quem detém maior responsabilidade, pois é quem estabelece os princípios a serem cumpridos por toda a entidade, dentro dos fatores que afetem positivamente o ambiente de controlo, bem como avalia as capacidades e eficácia da gestão do risco da entidade.

A administração deve providenciar à gestão governança, orientação e supervisão, por sua vez, a gestão deve manter a administração informada dos riscos relevantes, bem como das ações que toma de forma a assegurar a gestão eficaz dos mesmos. A administração deve ter em conta a informação proveniente dos auditores internos e externos e terceiras partes interessadas. Cabe a estes avaliar o sistema de controlo interno em relação à aplicação dos princípios, com apoio dos componentes.

A gestão em concordância com os restantes colaboradores da entidade deve ter em consideração como as responsabilidades se encontram implementadas e, discutir com estes, formas de fortalecer o controlo.

A auditoria interna avalia a eficácia do sistema de controlo e contribui para que seja contínua, detendo o papel de monitorização. A auditoria externa pode rever e avaliar a eficácia do controlo interno no que respeita às demonstrações financeiras, como também em relação aos princípios, centrando-se em como a entidade selecionou, desenvolveu e aplicou os controlos que afetam os princípios dentro dos componentes do controlo interno.

Os reguladores apoiam-se nas estruturas dos modelos de controlo interno de forma a estabelecer expectativas, quer seja como forma de orientação ou em como conduzir uma avaliação pelas entidades que supervisionam. As expectativas para o controlo interno podem variar quanto ao que este pode ou não alcançar e relativamente ao consentimento do conceito de segurança razoável, para tal os reguladores e a gestão devem estar de acordo quanto à *framework* a utilizar e as suas limitações.

4. AUDITORIA INTERNA

4.1. FUNÇÃO DO SISTEMA DE CONTROLO INTERNO NA AUDITORIA INTERNA

«O controlo interno é o conceito mais importante e fundamental que um auditor interno deve entender.» (Pickett; 2003)

Por forma a entender esta integração, é necessário, inicialmente, interiorizar o conceito de Auditoria Interna. Um pouco como o controlo interno, também o conceito de auditoria encontra-se relacionado com o de segurança e com o grande objetivo de detetar fraudes. (Pickett, 2010)

Um pouco como todos os conceitos, várias organizações a nível internacional tentaram harmonizá-lo. Em 1999, o IIA aprovou a definição como uma «atividade independente, que garante objetividade e de consultoria destinada a agregar valor e melhorar as operações da entidade.», com a missão de «melhorar e proteger o valor da organização proporcionando segurança, assessoria e análise com base no risco.». Desta forma, a auditoria representa «uma atividade independente, que garante objetividade, de consultoria concebida para acrescentar valor e melhorar as operações da entidade».

Segundo o IFAC, a função de auditoria interna representa uma «atividade estabelecida ou providenciada a uma entidade. As suas funções incluem, entre outras coisas, examinar, avaliar e monitorizar o quão adequado e eficaz é o controlo interno.» (ISA 610, § 7. (a))

A função de auditoria interna na organização detém grande relevância estratégica para o sistema de governação, pois o objetivo da auditoria interna é o incentivo do cumprimento dos objetivos da entidade, no qual é desenvolvido o âmbito do trabalho.

A finalidade da presença da auditoria interna subsiste na avaliação e prestação de auxílio à administração, no desenvolvimento adequado das suas competências de gestão, disponibilizando conclusões, recomendações/comentários após a conclusão da auditoria. Através deste modelo, a auditoria interna, detém uma abordagem mais proactiva, com monitorização alinhada aos riscos, ao controlo interno e aos planos estratégicos, mediante um processo contínuo, podendo através deste acrescentar valor à entidade.

Desta forma, as responsabilidades da atividade encontram-se dependentes de orientações das políticas definidas pela direção, daí uma das funções da auditoria interna é função de apoio à direção.

De forma a determinar quais as avaliações a realizar, é concebido o planeamento de auditorias a realizar ao longo de um período, quer seja anual a trienal, deverá assentar, essencialmente na avaliação dos riscos associados, ganhos de oportunidade, impacto das operações no volume de negócios, utilização de recursos, impacto no apuramento dos resultados e na complexidade dos processos e subprocessos. (Pinheiro, 2010: 10)

O plano de auditoria deve ser logicamente relacionado com a identificação dos riscos da entidade. Estes, por sua vez, encontram-se diretamente relacionados com os objetivos estratégicos e operacionais. A relação entre estes dois fatores representa a principal vantagem do planeamento de auditoria com base de risco.

Segundo a DRA 400, a avaliação preliminar do risco de controlo representa o processo de avaliação da eficácia do sistema de controlo interno na prevenção ou deteção e correção de distorções materialmente relevantes. Esta avaliação contempla asserções relativas a cada saldo de conta ou classe de transações materialmente relevantes. A categorização do risco de controlo, pode estar compreendida entre mínimo, moderado e máximo, de acordo com os controlos. Estes, num nível máximo, demonstram que podem não dizer respeito a uma asserção contida nas demonstrações financeiras, ou que não são eficazes ou que ao avaliar a sua eficácia, estes revelam-se ineficientes.

De acordo com a Norma 2120.A1 do IIA, o risco deve ser alinhado com os objetivos de controlo interno e deve ser avaliada a eficácia e eficiência aos controlos, como resposta ao risco. Desta forma, os objetivos enumerados na norma são:

- Confiança e integridade da informação financeira e operacional;
- Eficácia e eficiência das operações;
- Salvaguarda dos ativos; e
- Cumprimento das leis, regulamentos e contratos.

Deste modo, surge a necessidade de realizar a gestão de riscos, de forma a minimiza-los, reforçando o sistema de controlo interno, o que leva à diminuição de perdas com a possibilidade de majorar os ganhos e, acima de tudo, atingir os objetivos propostos da entidade.

Surge assim o conceito de gestão de risco, que para o COSO, é:

[u]m processo desenvolvido pela administração, gestão e outras pessoas, aplicado na definição estratégica ao longo da organização, desenho para identificar potenciais eventos que podem

afetar a entidade, e gerir os riscos para níveis aceitáveis, fornecendo uma garantia razoável de que os objetivos da organização serão alcançados.

Ao conhecer os aspetos pertinentes do sistema de controlo interno, em simultâneo com as avaliações do risco inerente e do risco de controlo, é possível ao auditor a identificação de potenciais distorções materialmente relevantes, ter em consideração fatores que afetem o risco de distorções materialmente relevantes e a conceção de procedimentos de auditoria apropriados.

O risco inerente é definido como sendo a «susceptibilidade de um saldo de conta ou classe de transações conter uma distorção que possa ser materialmente relevante, considerada individualmente ou quando agregada com distorções noutros saldos ou classes, assumindo que não existem os respetivos controlos internos». (§5 DRA 400).

O risco de controlo é a «susceptibilidade de uma distorção, que possa ocorrer num saldo de conta ou numa classe de transações e que possa ser materialmente relevante, considerada individualmente ou quando agregada com distorções noutros saldos ou classes, não vir a ser prevenida ou detetada e corrigida atempadamente pelo sistema de controlo». (DRA 400; §7).

Na avaliação e gestão do risco, as normas internacionais referem a importância da auditoria interna, ao determinar se estes são eficazes, verificando se:

- Os objetivos da entidade sustentam e estão alinhados com a missão da organização;
- Os riscos significativos são identificados e avaliados;
- São seleccionadas as respostas adequadas que alinham os riscos com o apetite ao risco da organização; e
- A informação relevante sobre o risco é identificada e comunicada em tempo oportuno e transversalmente pela organização, permitindo aos colaboradores o cumprimento das respetivas responsabilidades.

Após a avaliação do sistema de controlo interno e avaliação dos riscos, procede-se ao exame e avaliação de informação, com o trabalho de campo. Segundo a *Performance Standard 2240 – Engagement Work Program*, os auditores internos devem desenvolver e documentar programas de forma a alcançar os objetivos.

Depois da análise e avaliação da informação, da comparação do expectável com o real, o auditor comunica os resultados, através do Relatório formal. É através deste que o auditor

comunica as conclusões do trabalho, aos respetivos destinatários. (*Performance Standard 240 – Criteria for Communicating*).

A conceção do relatório detém como vantagens incrementar a qualidade e quantidade homogeneização de auditorias, nomeadamente nos «procedimentos, modelos de conclusões e relatórios e *follow-up* das recomendações de forma permanente» (Morais e Martins, 2013: 172).

Por conseguinte, a auditoria interna reporta os aspetos negativos, isto é, as ineficiências detetadas, à gestão. Por sua vez, cabe à gestão providenciar diligências, suportando-as nas recomendações dadas, com o intento de atingir os objetivos da entidade. Segundo o Professor Ibraim Lisboa, «quanto mais informações úteis e oportunas ela (auditoria) fornecer à gestão, maior credibilidade será dada ao seu papel funcional.»

A monitorização do progresso, comumente conhecido como *follow-up*, segundo a ND – 2500, diz que «o responsável pela auditoria tem que estabelecer um sistema de monitorização do efeito dos resultados à gestão». Esta representa um processo, através do qual os auditores internos avaliam a adequação, a eficácia e oportunidade das medidas tomadas pela gestão em relação às recomendações dadas, incluindo as efetuadas pelos auditores externos.

O acompanhamento é feito através da monitorização dos planos de ação de modo a avaliar as ações corretivas. Segundo Morais e Martins (2013: 173), este consiste num processo de avaliação da adequação, de eficácia e oportunidade das medidas tomadas pelo Órgão de Gestão. Dá-se relevância aos resultados e resolução das questões, do que necessariamente às recomendações de auditoria.

Nos procedimentos de monitorização são tidos em conta tanto quanto maior for o risco associado. Segundo a NI 2500.A1, o «responsável de Auditoria Interna deve estabelecer um processo de seguimento para supervisionar e assegurar que as ações tomadas pelo Órgão de Gestão foram efetivamente implementadas ou que assumiram o risco de não as tomar».

Com a permanente monitorização é possível, através de avaliações regulares, estabelecer profundidade dos procedimentos futuros a efetuar, ou seja, é possível planear áreas alvo ou procedimentos a auditar e as respetivas atividades a realizar.

A monitorização das questões de uma Auditoria detém importantes fatores determinantes na realização do *follow-up*, que segundo Pinheiro são:

- A importância dos problemas identificados (se afectam o core business da empresa);
- O grau de esforço para corrigir os problemas e implementar as recomendações;
- A complexidade da acção corretiva;
- O tempo necessário à implementação da recomendação [...].

(Pinheiro; 2010: 178)

De notar, que a amplitude e profundidade do *follow-up* dependem do risco, importância das conclusões e alcance da Auditoria. No exame das respostas e acções corretivas é tendencialmente mais curto e direto. Por forma a não adular algo que o auditado possa ter respondido, deverá ser realizado por escrito. Na avaliação da adequação das respostas e acções, o seguimento é semelhante a uma auditoria, pois envolve procedimentos de auditoria, nomeadamente na realização de testes. Quanto à elaboração de relatórios, este deve ser feito sempre após a obtenção dos resultados. (Martins e Morais; 2013: 179)

Quanto à tipologia de testes, estes podem ser testes de procedimento ou conformidade, substantivos ou analíticos. Segundo o IIA, os testes de conformidade consistem nos procedimentos diretamente relacionados com a avaliação da eficácia da configuração e implementação dos controlos internos. Quando o auditor analisa o desenho do controlo, este avalia se o controlo encontra-se bem configurado de forma a prevenir ou detetar erros materiais. Como exemplo deste tipo de testes, tem-se a inspeção de documentos, relatórios ou ficheiros informatizados, observação da aplicação de controlos específicos, questionara gestão, supervisores e colaboradores. Nesta fase são realizados também os testes aos procedimentos, os quais aplicados às operações expressivas relativas aos objetivos do controlo interno.

Os testes substantivos, segundo o IIA, consistem na avaliação da integridade dos dados constantes nas evidências. A informação é devidamente tratada de forma a determinar a sua veracidade, classificação, precisão e se se encontra completa. É também feita a comparação com informação de diferentes fontes, de forma a determinar se a mesma se encontra exata ou com divergências. Por norma, a dimensão dos testes substantivos será tanto menor quanto melhor for o controlo interno existente no sistema (TC, Volume I, pág. 32).

Compete à equipa que realiza o seguimento efetuar a gestão permanente e sistemática do repositório, caso exista, das questões de auditoria, desta forma é imperativo realizar o acompanhamento tempestivo dos planos de ação, mantendo a articulação permanente com os auditados. A realização de *follow-up*, no âmbito da função de auditoria interna, ao monitorizar as questões de auditoria, monitoriza também o sistema de controlo interno, representando assim um ponto de grande importância para o controlo interno. Pode-se afirmar que uma adequada monitorização das questões leva a uma melhoria do sistema de controlo interno.

4.2. ATIVIDADES DE MONITORIZAÇÃO

Na atividade de auditoria interna, cabe a esta realizar a monitorização do sistema de controlo interno, pois é através da implementação de eficazes e eficientes sistemas de controlo interno que é possível obter informação fiável e que assim se mantenha. Para que tal suceda é imperativo que os sistemas detenham supervisão contínua.

Segundo o modelo COSO, na componente das atividades de monitorização, refere que as atividades de monitorização podem ser feitas através de atividades contínuas, inseridas nos processos a diferentes níveis da entidade, proporcionando informações oportunas ou através de avaliações independentes, com âmbito e frequência diferentes, estando dependente da avaliação de riscos, da eficácia das avaliações contínuas, bem como outras de considerações da administração. A combinação das duas avaliações assegura que a gestão dos riscos mantenha a eficácia ao longo do tempo.

As atividades contínuas devem ser executadas de forma contínua e como parte integrante das tarefas diárias da organização, complementadas por avaliações autónomas. Como participantes das ações de controlo, encontram-se primeiramente os colaboradores, através da execução e revisão das tarefas, seguido da formalização e comunicação das deficiências. Também os órgãos da gestão devem desenvolver ações de controlo sobre as áreas da sua responsabilidade, através da verificação da adequação da execução dos procedimentos por parte dos colaboradores. Também o órgão de administração realiza ações de controlo, porém focadas nas áreas de negócio e evolução dos objetivos da organização, assim como nas alterações internas e externas que possam comprometer a execução da estratégia e objetivos.

Este tipo de atividades é caracterizada por se encontrar, tipicamente, perto das operações de controlo, por oferecer oportunidades de identificação de fraquezas e, por representar, muitas das vezes, atividades de rotina realizadas ao nível da unidade de negócio.

As avaliações independentes devem ser realizadas por uma função de auditoria interna. Estas como parte das suas funções normais ou a pedido específico do órgão de gestão ou administração, com possível parecer dos Auditores Externos, aquando da emissão de parecer sobre o controlo interno. A razão pela qual na escolha da auditoria interna, prende-se pelo fato de estes possuírem qualificações a capacidade para realizar avaliações de forma eficaz, confiável e profissional, em comparação a uma empresa subcontratada.

As avaliações independentes são geralmente mais objetivas, através da validação dos resultados das atividades contínuas. Por regra, é feita com base no risco, isto é, áreas com maior risco são avaliadas mais frequentemente.

Os procedimentos de monitorização adicionais devem depender da natureza e significância dos riscos inerentes à atividade desenvolvida e da eficácia dos controlos específicos associados.

O processo de monitorização deve ser adequadamente documentado, através da identificação das alterações introduzidas ao longo do tempo. Por sua vez, a documentação que represente deficiências deve ser devidamente relatada, pelo fato de representar uma desvantagem real, percebida ou com potencial de melhoria. O relato das deficiências representa assim uma oportunidade de fortalecer o sistema de controlo interno e assim a probabilidade de os objetivos da organização serem alcançados.

Como parte da responsabilidade do órgão de administração, relativo ao processo de monitorização, cabe a estes designar o responsável pela função de auditoria interna e assegurar que esta função tem suficiente autoridade para desempenhar as suas competências, de forma independente, bem como possui recursos materiais e humanos adequados ao desempenho das tarefas.

4.3. NORMAS INTERNACIONAIS DE AUDITORIA INTERNA

A nível internacional, os responsáveis pela elaboração e emissão de normas de auditoria são o IFAC, dedicado sobretudo à auditoria externa, o INTOSAI, que se dedica à auditoria ao setor público e o IIA, à auditoria interna.

Em 1999, o IIA elaborou a sua estrutura de prática, designada de *Professional Practices Framework*, hoje em dia designada por *International Professional Practices Framework (IPPF)*. As IPPF têm com objetivo, segundo o IIA:

- Delinear princípios básicos que representem a prática de auditoria interna tal com ela deverá ser;
- Proporcionar um enquadramento para o desempenho e promoção de um vasto conjunto de atividades de auditoria interna que permitem acrescentar valor;
- Estabelecer uma base para avaliar o desempenho de auditoria interna; e
- Promover a melhoria dos processos e operações das organizações.

O quadro seguinte representa o organograma das IPPF:



Figura 6- Organograma IPPF

Fonte: <https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx>

Desde 2009, que é da responsabilidade do IPAI aplicar e traduzir as normas emanadas do IIA, com a designação de “Enquadramento Internacional de Práticas de Profissionais de Auditoria Interna”, as IPPF, com o objetivo de:

- Delinear os princípios básicos que representam a prática de auditoria interna;
- Fornecer uma estrutura para a execução e promoção de um amplo conjunto de atividades de auditoria interna;
- Estabelecer as bases para a avaliação de desempenho de auditoria interna; e
- Promover a melhoria dos processos e operações organizacionais.

Desta forma, as normas internacionais para a prática de auditoria reagrupam-se em três categorias:

- As Normas de Atributos pertencem à categoria 1000 e estão diretamente relacionados com as características das organizações e entidades que desempenham a atividade de auditoria interna.
- As Normas de Desempenho, pertencentes à categoria 2000, descrevem a natureza das atividades e proporcionam critérios de qualidade que permitem medir o desempenho das mesmas.
- As Normas de Implementação, desenvolvidas em torno das Normas de Atributos e de Desempenho, que visam facultar requisitos aplicáveis a atividades de garantia, através da avaliação objetiva ou, de consultoria.

É da responsabilidade do IIA, a emissão de orientações fortemente recomendadas, isto é, que a sua aplicação não é obrigatória, em que é esperado conformidade, a menos que seja aplicado o juízo profissional. Estas associadas a palavra «deveria» (*should*). Por outro lado, existem as normas que especificam um requisito incondicional, associada a palavra «deve» (*must*).

Supletivamente, são aplicáveis as normas e recomendações de auditoria, emitidas pela *International Federation of Accountants (IFAC)*.»

Para o presente trabalho, as normas de auditoria externa, que podem deter interesse, são:

- Conhecimento do Negócio – DRA 310 fornece orientações sobre o que se deve entender por conhecimento do negócio e quais os procedimentos a executar. Na emissão da CLC, o Revisor utiliza o conhecimento do negócio e avalia as demonstrações financeiras e as asserções nelas contidas estão, ou não, corretamente apresentadas e consistentes com a informação financeira recolhida.
- A Materialidade – DRA 320 estabelece parâmetros para o cálculo da materialidade, e estabelece os limites máximos e mínimos, permitindo deste modo a definição de um intervalo de valores que será apreciado em função do juízo profissional.

Materialidade, segundo a *ISA 320*, é um conceito de significado e importância relativos de um assunto, quer considerado individualmente, quer de forma agregada. Um assunto é material se a sua omissão ou distorção puder razoavelmente influenciar as decisões económicas de um utilizador. Ou seja, valor que provoca uma alteração

no parecer do auditor em caso de descoberta de erros que, individualmente ou no seu conjunto, sejam superiores ao valor pré-estabelecido para a materialidade.

A *ISA 300* diz que a determinação da materialidade pelo auditor é uma matéria de julgamento profissional e é afetada pela sua perceção das necessidades de informação dos utentes da mesma.

- Avaliação do Sistema de Controlo Interno – DRA 410 indica que compete ao Revisor efetuar o levantamento e avaliação do SCI existente na organização, e executar os procedimentos que permitam concluir sobre a sua conceção.
- Conceito de Risco – DRA 410 fornece ao revisor a definição do conceito de revisão/auditoria, e define-se como a suscetibilidade do revisor dar uma opinião inapropriada quando as demonstrações financeiras estejam distorcidas de forma materialmente relevante.
- Procedimento de Avaliação do Risco – ISA 315 indica que, mediante o seu juízo profissional, deve efetuar os procedimentos que se mostrem necessários para identificar e avaliar os riscos de distorção material, devido à fraude ou erro, ao nível global das demonstrações financeiras e ao nível de asserções quanto a classes de transações, saldos de conta e divulgações.
- Resposta aos Riscos Avaliados – ISA 330 clarificada refere que o revisor deve conceber e implementar respostas globais que permite tratar os riscos avaliados de distorção material ao nível das demonstrações financeiras e deve conceber e executar procedimentos adicionais de auditoria cuja natureza, tempestividade e extensão se baseie e forneça as respostas aos riscos avaliados de distorção material ao nível da asserção.

4.4. O RISCO NO PROCESSO DE AUDITORIA INTERNA

Tal como referido acima, a auditoria interna detém um papel essencial na avaliação da eficácia da gestão do risco na entidade. A sua avaliação deve ser feita com regularidade, quanto à sua quantificação, conteúdo e limitação. Com a avaliação dos riscos, a auditoria interna pode delinear o plano de trabalho, tendo em conta as áreas de maior risco, ou seja, as prioritárias.

De acordo com a Norma 2120.A1 do IIA, o risco deve ser alinhado com os objetivos de controlo interno e deve ser avaliada a eficácia e eficiência aos controlos, como resposta ao risco. Desta forma, os objetivos enumerados na norma são:

- Confiança e integridade da informação financeira e operacional;
- Eficácia e eficiência das operações;
- Salvaguarda dos ativos; e
- Cumprimento das leis, regulamentos e contratos.

Deste modo, surge a necessidade de realizar a gestão de riscos, de forma a minimiza-los, reforçando o sistema de controlo interno, o que leva à diminuição de perdas com a possibilidade de majorar os ganhos e, acima de tudo, atingir os objetivos propostos da entidade.

Surge assim o conceito de gestão de risco, que para o COSO, é:

[u]m processo desenvolvido pela administração, gestão e outras pessoas, aplicado na definição estratégica ao longo da organização, desenho para identificar potenciais eventos que podem afetar a entidade, e gerir os riscos para níveis aceitáveis, fornecendo uma garantia razoável de que os objetivos da organização serão alcançados.

Segundo o IIA, citado por Morais e Martins (2013: 134), a gestão dos riscos auxilia a cumprir com os objetivos da entidade, com os seguintes benefícios:

- Melhorar o conhecimento dos riscos e a gestão eficaz dos mesmos;
- Identificar de forma proactiva e forma a aproveitar oportunidades;
- Responder rapidamente às mudanças envolventes,
- Retribuição eficiente de recursos para gestão de riscos;
- Base comum no estabelecimento para compreensão e gestão de riscos;
- A gestão toma decisões de forma mais segura;
- Melhorar a previsão de possíveis impactos;
- Melhorar a credibilidade e confiança;
- Melhorar a reputação corporativa;
- Melhorar a probabilidade de êxito na implantação da estratégia.

5. ESTUDO EMPÍRICO

5.1. ENQUADRAMENTO DO ESTUDO

Historicamente o homem preocupa-se em conhecer e compreender o que o rodeia, manifestando o gosto por investigar. A investigação científica é o resultado dessa disposição em querer conhecer e dominar o mundo.

Quando se fala em investigação científica, levantam-se duas questões: “Qual é o problema?” e “O que devo fazer para o solucionar?”. E se, etimologicamente, investigar significa procurar, surgem de seguida tantas outras questões como: “O que procurar?”, “Com que objetivo?”, “Como procurar?” e “Procurar para quê?”. (Coutinho; 2014: 1-2)

Com a questão formulada e o objeto de estudo definido (Sistema de Controlo Interno do Relato Financeiro da EDP – Energias de Portugal, SA) irá passar-se à demonstração de que a o funcionamento eficaz e eficiente do controlo interno representa uma ferramenta importante à gestão, na medida em que suporta o alcance dos objetivos. Com o diagnóstico do sistema de controlo interno, através do estudo das componentes e princípios do modelo COSO, é possível emitir opinião quanto à eficácia e eficiência do mesmo.

Segundo Prodanov e Freitas, o estudo de caso consiste na recolha e análise de informação sobre o objeto de estudo com a finalidade de estudar aspetos variados da realidade deste, tendo em conta o tema da pesquisa. (Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico; 2013: 60) No âmbito do projeto e do objetivo que se pretende alcançar, foi definido que a melhor metodologia de investigação a aplicar é através do estudo de caso.

5.2. METODOLOGIA DO ESTUDO EMPÍRICO

O trabalho científico por si tem uma natureza própria, pela distinção que detém em relação a outros trabalhos no que respeita à abordagem que faz. Neste contexto, o indivíduo que realiza a pesquisa necessita ser isento de opiniões e objetivos. Independentemente do estudo em causa é necessário que haja um protocolo de investigação.

Segundo Oliveira, o protocolo de investigação necessita de obedecer a um conjunto de princípios, nomeadamente:

- Natureza lógica, isto é, é necessário que o trabalho detenha uma sequência a ser observada;

- Especificidade, na medida em que cada etapa deverá ser composta por um conjunto de tarefas e atividades;
- Caracter dinâmico, ou seja, ainda que exista uma lógica ou especificidade, o espírito crítico do investigador deve estar presente e ser flexível, por forma a que seja possível uma reavaliação se necessário.

(Métodos de Investigação: Da Interrogação à Descoberta Científica; 2014: 22)

O protocolo é por muitos entendido como uma «escada de passos sequenciais», necessário à prossecução de vários tipos de investigação. (Carrilho Ramos e Naranjo; 2014: 22)

O ponto de partida dá-se com a definição do problema. É necessário aqui saber o que é pretendido estudar. De acordo com Carrilho Ramos, problema científico representa o

[c]onhecimento da manifestação de um objeto que cria uma necessidade no sujeito, produto de antinomias que neste se geram; as referidas contradições não se podem resolver automaticamente, mas exigem um processo de investigativo para satisfazer o desconhecimento / a lacuna epistemológica da ciência.

(Métodos de Investigação: Da Interrogação à Descoberta Científica; 2014: 74)

De seguida, é feita a revisão bibliográfica onde o investigador elucida sobre o estado da arte, com a leitura de trabalhos prévios, de onde provém certezas de caminhos a percorrer. A conceção teórica não só admite a construção de hipóteses com base na dinâmica encontrada nos casos, como também permite definir a informação relevante. A lógica científica da conceção teórica orienta sobre o modo de organizar a exposição dos resultados.

No seguimento, é construído o modelo de análise, onde é apresentada a referência do resultado da literatura e apontado o caminho que o trabalho irá tomar. O modelo em análise neste trabalho é o estudo de caso, apoiado em diversos métodos empíricos de obtenção de informação, tais como, entrevista, questionário com profundidade em formato *check-list* e, através da observação de documentação disponível.

O que se procura não é a representatividade a nível quantitativo, mas sim qualitativo, ou seja, será dada importância à representatividade social e não representatividade estatística. Para tal, foi tido em conta a variabilidade que os sujeitos podem deter na amostra, bem como o conhecimento profundo que possuem da matéria e da organização. (Oliveira e Ferreira; 2014: 168 - 169) A escolha de elementos prendeu-se com a representatividade dos casos,

isto é, na riqueza e complexidade que poderá não ser obtida caso a amostra seja de grande dimensão.

Conclui-se, que é uma investigação qualitativa pela sua abordagem, permitindo explorar mais detalhes da organização, pela extensão no uso de estudos de casos, através da recolha de experiências relevantes, sempre com um guia teórico, na medida em que se baseia em doutrinas específicas de paradigmas científicos a suportar o estudo. (Lapan, Quartaroli e Riemer; 2011: 69)

De seguida, é feita a recolha e tratamento dos dados da realidade de forma a objetivar a pesquisa científica. Os dados são a informação da realidade e é esta que servirá para auferir se a questão inicial, através do modelo de análise, efetivamente detém uma resposta fiável e robusta. Com a dispersão de indivíduos são criados, conseqüentemente, agrupamentos de resultados artificiais. (Carrilho Ramos e Naranjo; 2014: 169 - 170). Para a tipologia de trabalho utilizada, parte de sujeitos apreciados refletem o conjunto de qualidades objetivas a alcançar, na essência explicativa do objeto de estudo.

A análise e interpretação da informação relacionada com o modelo e revisão é feita com o intento de responder a questões como «os dados confirmam a teoria?» ou «acrescentam algo de novo», com o intento final de responder à questão inicial. É através da compreensão dos resultados que se podem retirar as conclusões da pesquisa, retrospectivamente os objetivos propostos, bem como sugerindo projetos futuros.

5.3. COMPONENTES DA ANÁLISE

A principal componente da análise centra-se no estudo do controlo interno, com o objeto de estudo a EDP – Energias de Portugal, SA. O principal foco do estudo é o entendimento do funcionamento dos componentes de controlo interno na organização.

Tal como observável abaixo, apesar do sistema de controlo interno estar centrado no Relato Financeiro, o estudo irá ser realizado de uma forma mais abrangente, segundo os contornos do modelo COSO.

Para tal, foi selecionado um elemento da equipa de controlo interno da organização, onde se encontram alocados três colaboradores. Selecionado pela sua representatividade, na riqueza e complexidade que darão ao trabalho realizado.

5.3.1. CARACTERIZAÇÃO DA ENTIDADE

A EDP – Energias de Portugal, SA. encontra-se a laborar no mercado português desde 1976, com a denominação de EDP – Electricidade de Portugal, numa fase inicial, através da fusão treze empresas nacionalizadas em 1975.

Foi na década de 90 que a organização entrou no mercado internacional, nomeadamente no Brasil. Por esta altura, a entidade passa de empresa pública para sociedade anónima e, após a reestruturação, é criado o Grupo EDP.

Desde o início do novo milénio, foram sentidas grandes mudanças por parte da organização para se aproximar do cliente. Esta fase iniciou-se pelo *rebranding* e reposicionamento da marca, através da denominação para a que é conhecida hoje e pela total modificação do logótipo, com o objetivo de transparecer conforto, simplicidade e responsabilidade social. Esta era encontra-se também demarcada pela entrada em novas áreas do setor da energia, como o gás natural e energias renováveis e pelo fator de excelência de se tornar um líder mundial nos índices Dow Jones de Sustentabilidade.

Em 2011, deu-se um novo *rebranding* da marca, agilizando o logótipo a cada uma das empresas do Grupo. Em 2013, a empresa torna-se 100% privada, um processo que teve início em 1996, faseado por 6 períodos.

Atualmente, encontra-se a laborar em 14 países, com 9,7 milhões de clientes de eletricidade, ocupando o 208º lugar no ranking das empresas mais valiosas do mundo.

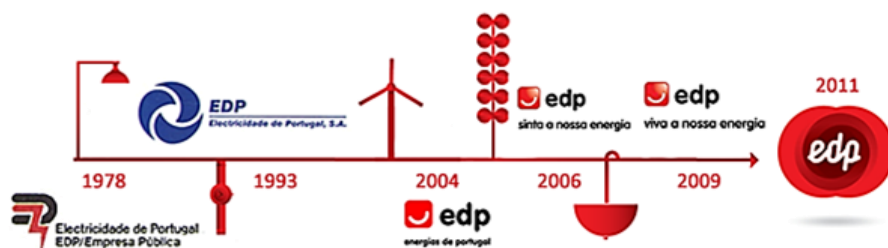


Figura 7 – Branding da marca EDP

Fonte – <https://www.edp.pt/pt/aedp/sobreaedp/marcaEDP/Pages/HistoriaMarca.aspx>

Sendo o negócio *core* da organização a energia, este encontra-se sob a alçada do Sistema Elétrico Nacional (SEM) regido segundo a Lei Base de Electricidade, que se divide em seis grandes áreas, nomeadamente as que a EDP integra: produção, transmissão, distribuição, comercialização, operação do mercado elétrico e operações logísticas facilitadoras da

transferência entre comercializadores pelos consumidores. No sistema elétrico, a EDP opera em Portugal, Espanha e Brasil.

O Sistema de Gás é regulamentado pelo Decreto-Lei no. 30/2006, de 15 de fevereiro e Decreto-lei no. 40/2006, de 26 de julho. Atualmente encontra-se dividido em sete segmentos: receção, armazenagem e regaseificação de Gás Natural Liquefeito (GNL), armazenagem subterrânea, transporte, distribuição e comercialização de gás natural, operação do mercado e operação da logística necessária à torça de fornecedores de gás natural. No sistema de gás, a EDP opera em Portugal e Espanha.

Dentro deste âmbito de negócio, por forma a assegurar que a organização alcance os objetivos a que se propõe, através de uma abordagem sistemática e disciplinada seja avaliada a eficácia dos processos, encontra-se centralizada na Direção de Auditoria Interna (DAI), consubstanciada a função de auditoria interna e controlo interno do Grupo EDP.

A função de auditoria interna, é uma função corporativa, dependente do Presidente do Conselho de Administração Executivo e supervisionada pela Comissão para as Matérias Financeiras/ Comissão de Auditoria.

No âmbito da função, a direção assegura auditorias financeira, operacional e normativa e, de sistemas de informação à EDP Portugal, HC Energía, Naturgás Energia, EDP Renováveis e Energias do Brasil. À data de 31 de dezembro de 2015, encontravam-se alocados 55 colaboradores que garantem os serviços das diversas áreas da Direção de Auditoria Interna do Grupo EDP. (Ver Anexo 4)

Desta forma, a auditoria financeira revê e avalia os sistemas de controlo que asseguram a fiabilidade e integridade da informação financeira elaborada, utilizada e divulgada pelo Grupo. A auditoria operacional e normativa revê os sistemas de controlo que asseguram o cumprimento da legislação e normativos aplicáveis, o cumprimento de políticas, procedimentos e normativos interno, a integridade e salvaguarda do património. A auditoria de sistemas de informação revê os sistemas de controlo que assegurem a fiabilidade e integridade dos sistemas de informação. (Relatório de Auditoria Interna; 2009: 11)

Para a gestão do sistema de controlo interno encontra-se centralizada na DAI uma área específica que detém este pelouro. A doutrina é formalizada através do Sistema de Controlo interno do Relato Financeiro, desenhado com base nas melhores práticas internacionais e nos modelos COSO e COBIT. Tem como função promover a monitorização, implementação e manutenção do Sistema de Controlo Interno do Relato Financeiro (SCRIF), supervisionar

a sua consistência e coerência interna e os controlos realizados pelos diferentes níveis de responsabilidade da estrutura organizativa. (Relatório de Auditoria Interna - EDP; 2015: 29).

Tem como objetivo

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

(EDP – Annual Report; 2011)

A DAI assegura assim o SCIRF do Grupo, com o objetivo de avaliar o sistema de controlo interno de forma independente e, propor e promover a implementação de medidas que contribuam para a eficácia através da melhoria e alinhamento de processos e sistemas.

A Direção de Gestão do Risco coordena os estudos de avaliação dos riscos do Grupo, segundo uma taxonomia específica (Anexo 3), com a finalidade de apoiar o Conselho de Administração Executivo no controlo e mitigação e fornecer análises integradas de retorno-risco. (Relatório & Contas - EDP; 2015: 197)

Com o sistema de controlo interno enraizado na cultura e gestão da entidade, é possível responder com maior rapidez aos riscos do negócio.

O modelo adotado no Grupo EDP tem em vista a identificação das empresas e/ou unidades de negócio, nas respetivas rubricas e processos relevantes para efeitos de relato financeiro, tem subjacentes análises de materialidade e risco.

Através deste modelo foi possível documentar, em 2015, 4.240 controlos, de entre eles, globais, ao nível da entidade, aplicativos, isto é, ao nível dos processos e, gerais de tecnologias de informação. Bem como, rever e documentar novos e já existentes processos e controlos.

Com a implementação desta doutrina, reforça-se a cultura de controlo, através de reuniões e documentos de apoio e é realizado o apoio, monitorização e controlo da resolução das não conformidades.

A avaliação do sistema de controlo interno para fins legais é feita por uma entidade independente de quem executa os controlos, nomeadamente um Auditor Externo, onde na sua avaliação incluiu:

[...] a obtenção do entendimento do sistema de controlo interno sobre o relato financeiro consolidado do Grupo, a avaliação do risco da existência de deficiências materialmente relevantes, o teste e avaliação do desenho, eficácia, conceção e funcionamento dos controlos baseados na avaliação do risco e a realização de outros procedimentos que considerámos necessários de acordo com as circunstâncias.

(Relatório Independente de Avaliação do Sistema de Controlo Interno sobre o Relato Financeiro do Grupo EDP; 2016: 2)

Segundo o manual, a avaliação do sistema de controlo interno do relato financeiro é descrita conforme a seguinte metodologia:

- I. Avaliação de desenho com o objectivo de avaliar o desenho dos controlos e emitir a opinião quanto à estrutura adequada para prevenir em tempo oportuno erros materialmente relevantes nas Demonstrações Financeiras e ou apropriação indevida de recursos do Grupo;
- II. Avaliação da eficácia operacional dos controlos, com desenho adequado, com o objectivo de confirmar se os controlos estão a ser executados de acordo com o desenho, se produzem os resultados desejados, se são realizados por profissionais com as qualificações e competências adequadas;
- III. Reporte à gestão dos resultados da avaliação decorrentes dos controlos seleccionados e testados pelo Auditor Externo.

(Relatório de Auditoria Interna; 2010: 21)

Assim, a avaliação realizada, pelo Auditor Externo sobre o Sistema de Controlo Interno sobre Relato Financeiro, permitiu concluir que este mantém, nos aspetos materialmente relevantes, um sistema «[...] consolidado, apropriado e eficaz [...] de acordo com os critérios estabelecidos pelo enquadramento normativo do controlo interno emitido pelo *Committee of Sponsoring of the Treadway commission* (COSO 2013) em relação aos processos de negócio e controlos globais [...]» (Relatório Independente de Avaliação do Sistema de Controlo Interno sobre o Relato Financeiro do Grupo EDP; 2016: 2)

Após a avaliação do auditor externo, de acordo com o Relatório de Atividades da Direção de Auditoria Interna de 2015, foi possível, com razoável grau de segurança, garantir a «mitigação do risco de fraude, a fiabilidade da informação e a qualidade na preparação das Demonstrações Financeiras».

5.3.2. MODELO DE ANÁLISE

O método empírico entendido como valoroso para obtenção de informação no estudo foi através de obtenção de informação qualitativa, nomeadamente inquérito, consubstanciado por entrevista e questionário, por meio de *check list*, bem como observação de documentação disponível.

5.3.2.1. *Entrevista*

A entrevista, segundo Cohen, Manion e Morrison, pode ser utilizada como o principal meio de recolha de informação relacionada com os objetivos da investigação, para testar ou sugerir novas hipóteses, bem como agregar-se a outros a outros métodos de investigação. (*Research methods in education*; 2007: 351) Segundo estes autores, a entrevista pode ser informal conversacional, entrevista guiada, *standardizada* aberta ou quantitativa fechada. Para o caso de estudo foi aplicada entrevista guiada e informal conversacional, pois apesar do tema ter sido definido antecipadamente e algumas das questões estivessem já definidas, alguns temas foram tratados no decorrer das conversas.

A entrevista decorreu no edifício da EDP com a Dr.^a Maria Ester Carvalho, coordenadora da área de controlo interno da organização, onde foi possível esclarecer os pontos principais ao trabalho desenvolvido. Nomeadamente:

- No passado a empresa encontrava-se cotada na bolsa de Nova Iorque e, como tal, encontravam-se sob alçada da Lei SOX. Ainda que ocorrido a saída da NYSE Euronext Lisbon (*New York Stock Exchange*)
- Encontra-se implementado o modelo COSO 2013;
- Ainda que regido pelo modelo COSO, o sistema de controlo interno está direcionado para o relato financeiro, com o objetivo de obter confiança nas Demonstrações Financeiras;
- O modelo então aplicado denomina-se de SCIRF – Sistema de Controlo Interno de Relato Financeiro;
- Os controlos encontram-se baseados no risco.

5.3.2.2. *Questionário*

Segundo Coutinho, num questionário «[...] as questões são apresentadas através de um formulário que o inquirido administra a si próprio [...]» exigindo um «[...] nível mínimo de

literacia de leitura que tem de ser equacionada tendo em conta a população alvo a quem se destinam [...]» (Metodologias de Investigação em Ciências Sociais e Humanas; 2014: 126 - 127)

A construção do questionário teve como base teórica a interpretação de variadas bibliografias devidamente descritas acima, bem como um conjunto de *check-lists* provenientes de artigos técnicos do Comité COSO, de publicações científicas e, de consultoras como a Deloitte e Ernest and Young.

Após construção da *check-list*, realiza-se a recolha dos dados com a aplicação do mesmo, seguido da organização e análise de conteúdo, permitindo a organização, apresentação e descrição dos dados. Com a interpretação dos factos, pode-se concluir sobre o tema.

A *check-list* encontra-se dividida em cinco grandes grupos, detalhadamente os cinco componentes do modelo COSO. Dentro de cada um destes componentes, encontram-se os respetivos princípios associados e, por conseguinte, a interpretação das áreas de foco. As respostas são fechadas, podendo colocar observações, caso haja necessidade.

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
1. Integridade e Valores Éticos				
1.1.	A integridade figura-se presente na empresa?			

Tabela 1 – Cabeçalho da *check-list*
Fonte própria

5.3.3. RECOLHA DE DADOS

A recolha de dados através da entrevista qualitativa permitiu a assunção de informação significativa, detalhada e útil na confirmação da exploração da *check-list* (Anexo 5). Esta última, permitiu recolher informações provenientes de reflexões mais aprofundadas, não tão fáceis de acesso caso tivessem sido abordadas através de estratégias mais quantitativas.

A leitura de relatórios de atividades da direção, bem como o Relatório & Contas, permitirá validar algumas das afirmações abordadas nos métodos inquisitivos. Após a entrevista foi possível obter da Dr.^a Ester material de análise que vem solidificar as asserções feitas.

5.4. ANÁLISE E TRATAMENTO DOS DADOS

Neste ponto é necessário relembrar a noção da aceção dos conceitos de eficácia e eficiência no âmbito do estudo. Como explanado acima, a descrição de eficácia e eficiência é

representada pelo grau em que os objetivos estabelecidos são alcançados e que para tal devem-se encontrar estabelecidas métricas e critérios de mensuração apropriados à entidade

Por outras palavras, irá averiguar-se a aderência do Grupo EDP ao modelo COSO, em que se estima se as componentes estão implementadas e em funcionamento e, se se encontram estabelecidos parâmetros e metodologias de aplicabilidade.

Por forma a esquematizar o tratamento dos dados e para melhor compreender a estruturação do modelo, a apresentação da análise será realizada por componentes do modelo, explicitando os princípios, com suporte em evidências.

5.4.1. AMBIENTE DE CONTROLO

O ambiente de controlo caracteriza-se por um conjunto de normas, processos e estruturas que providenciam a base para o desenvolvimento do controlo interno na organização.

Os sete fatores integrantes no ambiente de controlo são a integridade e os valores éticos, compromisso e competência, Conselho de Administração e Comité de Auditoria, filosofia da gestão e procedimentos operacionais, estrutura organizacional, atribuição de autoridade e responsabilidade e políticas de recursos humanos.

A DAI na sua função de auditoria interna avaliar o cumprimento das atividades no ambiente ético, bem como a eficácias das estratégias, metodologias, comunicações e outros procedimentos. Neste âmbito, fornece consultoria quanto ao alcance dos objetivos e auxilia a organização no estabelecimento de um programa robusto para melhorar a eficácia, assim como assegura que são tomadas medidas aquando da existência de desvios. (Relatórios de Atividades da Direção de Auditoria Interna – Grupo EDP)

É facilmente averiguável que no Grupo EDP existe um Código de Ética (Anexo 6), pela qual a organização rege a integridade e valores éticos, disponível a todos os colaboradores, para que guiem os seus comportamentos, atividades e decisões que envolvam a empresa. Este código, é tido com *standard*, que detém níveis de tolerância e associadas avaliações e medidas a tomar em caso de incumprimento.

Um dos compromissos do Grupo EDP, passa por aliar a conduta ética e de rigor profissional ao entusiasmo e iniciativa, através da valorização do trabalho em equipa, demonstrando que se encontram presentes normas de conduta que estabelecem comportamentos éticos para os colaboradores. (*website* do Grupo EDP)

A função de auditoria interna provê segurança e implementa políticas e práticas sobre a adequação e eficácia da estrutura organizacional, linhas de reporte e responsabilidades para se fazerem cumprir as atividades no âmbito do alcance dos objetivos.

A organização detém uma estrutura organizacional composta por linhas de negócio, nomeadamente eletricidade, gás e renováveis, Brasil, Participações e outras, onde se incluem EDP Soluções Comerciais, EDP Valor, EDP Projetos, entre outras. É perceptível que as linhas de negócio encontram-se devidamente estruturadas e compreensíveis de modo a que seja facilmente planear, executar, controlar e avaliar as atividades. (Anexo 7)

Encontram-se descritas no modelo organizativo (Anexo 8) as responsabilidades e funções de cada um dos intervenientes nas diversas atividades do Controlo Interno e nos diversos níveis da organização. A descrição das funções da DAI encontra-se explanado nos Relatórios de Atividades da Direção de Auditoria Interna pois está subdivida pelas áreas de trabalho da Direção.

Compete aos colaboradores manterem-se informados quanto aos objetivos da organização e com o auxílio do modelo organizativo estarem conscientes das suas responsabilidades e funções nas atividades de controlo interno. Para tal, compete à organização atrair, formar e manter os colaboradores habilitados à execução das suas tarefas. Neste âmbito, diz respeito à DAI a avaliação quanto à eficácia e eficiência das políticas e processos de recursos humanos e quanto às responsabilidades perante o controlo interno. (Modelo de Responsabilidades do Sistema de Controlo Interno e do Relato Financeiro)

A formação dos colaboradores da DAI, é feita tanto interna como externa, sendo a primeira a que detém maior percentagem de realização. A área formativa encontra-se subdividida em comportamental, gestão, organizacional e técnica, sendo esta última a que detém maior número de horas e percentagem de frequência, por se encontrar relacionada diretamente com a função de auditoria interna (exemplo: CIA, Amostragem em Auditoria, Gestão de Risco, entre outras). (Anexo 8) (Relatório de Atividades da Direção de Auditoria Interna; 2015: 38)

Na contratação de novos colaboradores, o Grupo EDP possui uma plataforma *on-line*, em que qualquer pessoa se pode candidatar, bastando apenas realizar o registo com os dados pessoais, habilitações académicas, conhecimentos, experiência profissional e anexar o *Curriculum Vitae*. A nível interno, pode-se averiguar ainda nos Relatórios de Auditoria Interna que, quase todos os anos existe a rotação de recursos humanos, tanto a nível interno da Direção, bem como dentro do Grupo EDP. (Anexo 9) (*website* de recrutamento EDP)

5.4.2. AVALIAÇÃO DE RISCO

A análise da avaliação de risco é representado por um processo dinâmico e interativo de identificação e avaliação dos riscos da organização, definindo ainda uma base de forma a os gerir.

A avaliação de risco inclui no seu método processos para identificar, analisar e responder ao risco, devem ser considerados níveis de tolerância de aceitação de risco e realizar discussões da importância do risco e a rapidez e persistência de propagação, bem como impacto e probabilidade. A avaliação de risco inclui recentemente a componente de avaliação do risco de fraude, explanado no Princípio 8.

Cabe à função de auditoria interna verificar que os objetivos são específicos, mensuráveis, alcançáveis, relevantes e limitados no tempo, por forma a permitir a identificação e avaliação dos riscos. Ter em conta que para a Direção de Auditoria Interna manter a sua independência organizacional, os auditores não devem desenvolver objetivos ao nível da organização. Para avaliação do risco poder ser completa é necessário que todos os riscos sejam aportados e em todos os locais geográficos em que o Grupo EDP opera. (Anexo 10 e Anexo 11)

A gestão do risco, centralizada na Direção da Gestão do Risco (DGR), permite acompanhar o risco de cada unidade de negócio de forma mais astuta. São estes quem identificam as principais componentes do risco, desde a sua causa, evento e impacto, englobado pelas fases de identificação, estratégia, gestão e controlo. («Um modelo global e integrado de gestão do risco»; 2015)

Na identificação é feita a atualização do inventário de riscos, a quantificação dos riscos, nomeadamente impacto e probabilidade e a priorização do risco. Na estratégia é definido o apetite ao risco e definição ou atualização de políticas de gestão do risco e planos de ação. É feita a gestão diária das posições em risco, no âmbito das políticas, bem como o robustecimento de cultura de gestão de risco. O controlo, por sua vez, monitoriza e reporta as posições em risco e realiza o acompanhamento da implementação das políticas e planos de ação. De maneira a facilitar o processo de identificação dos riscos, existe a possibilidade de recorrer ao COSO – ERM, pela sua especificidade neste âmbito.

Como alternativas aos planos de ação, a tolerância e gestão do risco pode passar por evitar, mitigar, reter ou aumentar. Quando se evita, é feita a eliminação da possibilidade de materialização do risco, como o caso do desinvestimento de uma linha de negócio. A mitigação pode ser feita pela redução, em que se diminui o impacto e/ou frequência do risco,

ou pela transferência, em que faz repassar o impacto do risco para terceiros. A retenção mantém de forma deliberada e consciente o risco na organização. Por último, quando se aumenta a exposição ao risco, é necessário ser de forma deliberada, como nos casos em que é feita a concentração numa linha de negócio.

A avaliação do risco é feita numa base anual, com base em indicadores de performance (*Key Performance Indicator* – KPI) e de risco (*Key Risk Indicator* – KRI), estas métricas têm como objetivo ajudar na decisão. Para a execução do KRI são utilizados, com uma volatilidade estável, um mapa de riscos anual, *dashboard* trimestral, em que inclui as condições macroeconómicas, fundo de pensões, custo de capital, risco de crédito e investimentos operacionais, e com maior volatilidade e grau de materialidade dos riscos-chave, os relatórios semanais de exposição ao mercado, exposição a contrapartes, riscos financeiros e P@R, V@R e EBITD@R¹³. («Um modelo global e integrado de gestão do risco»; 2015)

No ano de 2015, foi abordado o risco de fraude e respetivo acompanhamento e mitigação, através de lançamento de programas abrangentes de combate à fraude. Neste âmbito incluem-se as perdas técnicas de energia, seja por furto, desvio ou fraude. Esta abordagem foi também aferida nas sucursais, no âmbito das parcerias institucionais. Neste âmbito, é exigido aos auditores internos que detenham conhecimento suficiente para avaliar o risco de fraude, porém não é necessária que tenham a perícia de um colaborador que realiza estas tarefas diariamente. (Relatório de Atividades da Direção de Auditoria Interna; 2015)

No Grupo EDP, a realização da monitorização do processo de gestão de risco é feita pelo Conselho Geral de Supervisão, a discussão do processo de risco, controlo interno e auditoria, é realizada pelo Comité de Matérias Financeiras/ Comité de Auditoria e, a validação da implementação adequada de processos e controlos centrais e respetivas exceções, em exclusivo da DAI. (Anexo L)

A auditoria interna tem em conta a estrutura de risco da organização, para poder delinear o plano de atividades baseado no risco.

Na identificação e avaliação de riscos relevantes para as Demonstrações Financeiras são tidos em conta eventos relevantes, de representação fidedigna, comparáveis, atempados e compreensíveis, para o momento do registo contabilístico. Conclui-se que se encontram

¹³ EBITD@R : lucros antes de impostos, depreciação, amortização e custos de renda/reestruturação.

presentes os requisitos da Estrutura Conceptual, devidamente descritos no Relatório & Contas.

A função de auditoria interna identifica e avalia mudanças que podem impactar significativamente o sistema de controlo interno, aquando da avaliação periódica do risco, bem como no decorrer de uma auditoria interna. Quando tal acontece, comunica ao órgão de gestão por forma a antecipar mudanças que irão impactar a avaliação do risco.

5.4.3. ATIVIDADES DE CONTROLO

As atividades de controlo representam ações definidas por políticas e procedimentos que ajudam a que as orientações da gestão para mitigação dos riscos seja efetuada. Estas são executadas a todos os níveis da organização e nos vários estágios dos processos e ainda ao nível do ambiente tecnológico de suporte.

Os requisitos da *framework* do modelo COSO 2013 passam pela presença e funcionamento dos 17 princípios relevantes, bem como que todas as 5 componentes funcionem de forma integrada, de forma a criar maior atenção e enfatizar a eficácia do controlo interno de relato financeiro.

No processo de construção e implementação encontram-se envolvidas as Direções de Gestão de Risco e de Auditoria Interna. É aqui incluída a fase de avaliação de controlos, na medida em que é medido o nível de precisão, se se encontra a operar eficazmente através de *follow-ups*. Cabe à função de auditoria interna providenciar segurança, de que os controlos estabelecidos pela gestão, estão apropriadamente desenhados, implementados eficazmente e a operar como tinha sido estabelecido, de maneira a mitigar o risco para o alcance dos objetivos a níveis aceitáveis. («Um modelo global e integrado de gestão do risco»; 2015. Relatórios de Atividades da Direção de Auditoria Interna)

Como principais atributos, os controlos podem ser preventivos ou detetivos («Função do Controlo»), manual, automático ou semi-automático («Automatização»), autorização, comparação, reconciliação, restrição de acesso ou supervisão («Natureza do Controlo») e controlo chave ou *key control* ou controlo *standard* («Importância do Controlo»). A auditoria interna, nas suas avaliações, realiza sugestões de melhoria da eficácia e eficiência dos controlos. De notar, que é a gestão quem detém a responsabilidade do sistema de controlo interno. («Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP»)

Anualmente é feita a revisão de controlos relacionados com os princípios das demonstrações financeiras, que leva à documentação e revisão de novos controlos bem como redesenho de existentes. Neste âmbito, é realizada a auto-certificação do Sistema de Controlo Interno de Relato Financeiro (SCIRF), através do qual o Conselho de Administração Executiva, representado pelo CEO e CFO, emite um relatório de responsabilidade sobre o grau de segurança e fiabilidade da preparação e apresentação das Demonstrações Financeiras. Este modelo de controlo interno tem como base critérios de materialidade e risco. (Relatório de Atividades da Direção de Auditoria Interna; 2015: 30)

Uma das mais importantes atividades de controlo passa por assegurar segregação de funções, que no Grupo EDP vinha sendo identificado pelo Auditor Externo e, superado em 2014, aquando da entrada em funcionamento da ferramenta GACS – Gestão de Acessos e Segregação de Funções, totalmente concebida e desenvolvida pela área de Sistemas de Informação da DAI. (Relatório de Atividades da Direção de Auditoria Interna; 2014: 17)

Os controlos de IT, designados como controlo gerais de Tecnologias de Informação, regidos pelo modelo COBIT. A segurança de informação, reforçada com a criação da aplicação de procedimentos inerentes a gestão de acessos, definição de perfis e revisão de matrizes de incompatibilidade de funções, veio facilitar o processo de gestão do risco de sistemas de informação. (EDP – *Annual Report*; 2011)

No âmbito tecnológico, cabe à auditoria interna avaliar se os processos de *governance* suportam os objetivos e estratégias da organização. Assegura a eficácia, eficiência e completude dos controlos tecnológicos e, quando apropriado, recomenda melhorias específicas de atividades de controlo. Para preservar a independência do auditor, este não deve selecionar ou desenvolver atividades de controlo no âmbito tecnológico, porém podem fazer recomendações de controlos. (Relatórios de Atividades da Direção de Auditoria Interna)

Para assegurar as atividades de controlo interno no Grupo EDP, encontra-se centralizada na DAI uma área especializada que promove a «monitorização e manutenção do modelo de CI, assegura a fiabilidade e integridade da informação financeira, produzida internamente e divulgada ao mercado.» (Relatório de Atividades da Direção de Auditoria Interna; 2012: 7)

5.4.4. INFORMAÇÃO E COMUNICAÇÃO

A informação revela importância pela necessidade que a organização detém em que sejam desenvolvidas as responsabilidades de controlo interno que permitem alcançar os objetivos.

A gestão, por sua vez, obtém ou gera e usa informação relevante e de qualidade, tanto de fontes internas como externas, de forma a suportar o bom funcionamento do controlo interno.

Compete à função de auditoria interna avaliar periodicamente a fiabilidade e integridade das práticas da informação e, recomenda, de forma apropriada melhorias ou até a implementação de novos controlos ou salvaguardas.

É necessário que a informação seja comunicada de forma atempada, pois esta representa um dos elementos-chave para o sucesso do negócio, para obter operações eficazes e eficientes, bem como um sistema de controlo eficaz. Com o auxílio das novas tecnologias, a dispersão de informação tornou-se mais eficaz, contribuindo para uma estrutura eficiente de operações.

Compete ao gestor local do SCIRF coordenar e monitorizar a atualização da informação na aplicação de suporte, na medida em que coordena o levantamento, documentação e implementação do grupo de processos, procedimentos e controlos. Ainda inserido na função de auditoria interna, compete a estes providenciar segurança quanto à fiabilidade e integridade da informação, bem como associá-la ao risco de exposição. («Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP»)

A informação relevante à organização que carece conhecimento de todos os colaboradores é devidamente comunicada na página da Intranet do Grupo EDP (Anexo 14). Por forma a orientar e facilitar a divulgação de informação, tanto interna como externamente, subsistem manuais que descrevem as políticas e procedimentos. Assim, para rever periodicamente a qualidade da informação, são realizados testes à fiabilidade e atualidade da mesma, alinhados com as necessidades do órgão de gestão.

A comunicação interna de suporte do controlo interno a novos colaboradores e outros que se qualifiquem, é feita através de formação específica da matéria, por forma a receberem informação dos princípios do controlo interno, das componentes, operacionalização, funções e responsabilidades perante o SCIRF. (Anexo 15)

No seguimento do processo de comunicação de má conduta e atividades ilegais, foi aprovado no ano corrente (2016), a regulação dos procedimentos de *whistleblowing*¹⁴, faz a junção de regulamentação da SEC e, para os casos em que existe discrepância, prevalece a legislação portuguesa sobre a matéria. Esta regulação permite ao delator o seu anonimato. (Anexo 16)

¹⁴ *Whistleblowing*: processo de denúncia de quem tem e relata o conhecimento de atividades ilegais que podem ocorrer dentro da organização.

Como órgão de fiscalização, o Conselho Geral de Supervisão e o Comité de Auditoria foram-lhes atribuídas, como comissões especializadas, funções legas e estatutárias, tais como, promover o acompanhamento de forma permanente, avaliar os procedimentos internos relativos às matérias contabilísticas e de auditoria, assim como, a eficácia do sistema de gestão de riscos, do controlo interno e de auditoria interna, incluindo a receção e tratamento de reclamações e dúvidas.

A comunicação externa de informação do Grupo é realizada através do *website*, quando dirigidas ao público em geral, por carta, sempre que seja necessário informar clientes que possuem produtos da empresa, em particular aos acionistas, através do Relatório e Contas, entre outros. (*website* do Grupo EDP)

De notar que a comunicação atempada numa organização detém uma importância elevada, que foi possível colmatar com a facilidade das novas tecnologias. É possível, desta forma, haver linhas de comunicação direta entre a Administração e Comités e Direções, criar meios de comunicação diferenciados e assim poder monitoriza-los, como o caso da *mailbox*.

Quanto à comunicação, a auditoria interna providencia segurança que comunicações externas são precisas. De notar que, a função de auditoria interna não comunica com terceiros matérias que afetem o funcionamento do controlo interno.

5.4.5. ATIVIDADES DE MONITORIZAÇÃO

As atividades de monitorização são realizadas através de avaliações contínuas ou avaliações autónomas, podendo ser uma combinação das duas, de forma a avaliar se as componentes do modelo encontram-se presentes e a funcionar adequadamente.

O modelo COSO sempre denotou que as atividades de monitorização devem adereçar como as componentes são aplicadas e se o controlo interno funciona de forma eficaz. No modelo de 2013 existe a distinção entre uma atividade de controlo como monitorização ou como parte da revisão da gestão. Esta última questiona os erros e assigna as responsabilidades a quem de direito.

Com a aplicação de controlo interno, iBPMS¹⁵, introduzida no triénio 2006 – 2009, é possível manter os controlos monitorizados, ou seja, auxiliar na avaliação da presença e funcionamento dos controlos. (Anexo 17) A aplicação de controlo iBPMS representa o

¹⁵ iBPMS: *Intelligent Business Process Management Suites* – Suites Inteligentes de Gestão de Processos de Negócio; ferramenta de suporte aos trabalhos do SCIRF.

culminar da integração de uma grande análise de dados com os processos de uma organização. Nesta é possível fazer a integração de dados de várias fontes, processar a informação proveniente de uma máquina, por exemplo, um computador, gerando um *output* conector de todos os dados. Este *output*, por sua vez, é gerado através de filtros na própria aplicação, correlacionado eventos, permitindo obter informação atempada e fiável. Caso o processo gerado ainda não tenha tomado lugar, esta concebe um novo evento. (TIBCO; 2014)

Para que os colaboradores possam entender o funcionamento da aplicação é lhes providenciada formação específica para melhor entendimento do processo de controlo interno. (Anexo 18)

Quando identificadas controlos, estas passam a verter a sua informação na aplicação de controlo interno. Numa primeira instância procedesse à revisão e descrição do Processo. De seguida, identificam-se as principais etapas do Processo, seguida da descrição das atividades operacionais, que em conjunto com as atividades de controlo, recebe a documentação e verifica a aprovação por parte do órgão auditado. Após, processa-se a identificação e revisão dos riscos e objetivos de controlo, tal como já foi referido, é necessário ter presente os objetivos de negócio para proceder à identificação e análise dos riscos. Seguidamente, é feita a documentação e revisão dos controlos, no âmbito das atividades de controlo. Para tal estes são caracterizados segundo os seguintes parâmetros:

- Na identificação é feita a descrição e designado um código.
- Na descrição é feita a explicação da execução do controlo, em que de uma forma geral, identifica-se «quando, quem e como». Por sua vez, é caracterizada por informação de *input* e de *output*.
- A classificação dos controlos é dividida em controlo chave (*key control*) ou *standard*.
- Quanto à sua função, podem ser classificados como preventivos ou detetivos.
- Quanto à automatização podem ser automáticas, semi-automáticos, ou seja, existe a possibilidade de realizar por forma manual e por último, controlo manual.
- Identificação da frequência da execução do controlo pode ser definida a nível temporal ou de um acontecimento específico.

- A natureza do controlo é caracterizada pela forma como é identificado, nomeadamente, pela supervisão, autorização, reconciliação, comparação e acesso restrito.
- Por fim, a identificação de evento de fraude, tal como preconizo o Princípio 8.

(«Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP»)

Após, é feito o carregamento de toda esta informação para a aplicação iBPMS, conjuntamente com a nomeação do *owner* do controlo.

Com a documentação dos procedimentos de controlo interno e, respetivas evidências, consegue-se manter histórico e desta forma ser exequível planear auditorias com base nos riscos. É, por sua vez, exequível manter a informação atualizada para poder reportar à Administração e Auditores Externos, pois são quem atesta a supervisão do controlo interno.

Para além da identificação de controlos, é também necessário identificar ações detetadas pelos riscos e não mitigados pelos controlos, para assim criar as «não conformidades», comumente conhecidas como deficiências. Opção esta, também possível de carregar da aplicação iBPMS. Aqui são carregados os planos de ação para a sua resolução, com respetiva data de implementação, por forma a realizar *follow-ups* e assim obter uma completa monitorização de ações. («Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP»)

Com a automatização de controlos, valida-se a maturidade dos mesmos, com um ambiente de controlo solidificado, contribuindo para uma melhor eficiência das operações e alcance dos objetivos estabelecidos pelo Presidente. («Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP»)

É possível, através da monitorização e *follow-ups*, assegurar pontos de situação atualizados do controlo interno, bem como na sequência das auditorias. Observável nos Relatórios de Auditoria Interna, pode-se constatar que ao longo dos anos o número de controlos é variável. Para tal, é feito acompanhamento trimestral, através de avaliações autónomas, pela DAI por forma de obtenção do ponto de situação e depois remetido à Administração. (Relatório de Atividades da Direção de Auditoria Interna; 2015: 30)

Com o processo de acompanhamento estabelecido, é possível atribuir responsabilidades a os todos os níveis hierárquicos da organização, para que desta forma seja exequível atingir num

maior plano os objetivos da entidade e contribuir para a eficácia do sistema de controlo interno.

Os colaboradores da DAI responsáveis pela função de controlo interno prestam os esclarecimentos necessários aos colaboradores dos subgrupos e empresas em Portugal responsáveis pela operacionalização do SCIRF

5.5. CONCLUSÕES

Ainda que o Sistema de Controlo Interno no Grupo EDP seja direcionado para o Relato Financeiro, foi possível realizar uma abordagem com contornos gerais, sem comprometer a entidade.

Na análise feita, é possível constatar que se encontra implementado o Sistema de Controlo Interno segundo o modelo COSO, no Grupo EDP. Segundo critérios do próprio modelo, a presença de determinados princípios na organização são cruciais para que o SCI seja eficaz.

Assim, os três principais requisitos para um sistema de controlo interno eficaz passam por alcançar os objetivos de forma a cobrir, preferencialmente, todas as categorias de objetivos, cada um dos componentes e princípios relevantes devem estar presentes e a funcionar em conjunto de forma integrada. Posto isto, após análise dos dados recebidos, conclui-se que todos os componentes e princípios encontram-se presentes e a funcionar, assinalando em conjunto, com auxílio da Direção de Auditoria Interna.

Desta forma, encontram-se presentes pois subsistem no desenho e implementação do sistema de controlo interno para atingir os compromissos aos quais o Grupo se compromete. De notar que a EDP opta por ter compromissos em detrimento de objetivos gerais. Estes dirigidos para os clientes e pessoas, para com a sustentabilidade e com os resultados.

A funcionarem em conjunto de forma integrada demonstra que é possível reduzir até um nível aceitável o risco de não atingir um objetivo. Tendo em conta que, na generalidade observada, todos os componentes e respetivos princípios encontram-se presentes e a funcionar, parte-se do princípio que funcionam em conjunto de forma integrada pelo fato de que não é possível que um princípio funcione sem que outro esteja a operar.

Para um sistema de controlo interno não é apenas necessário seguir políticas e procedimentos, é também necessário usar o julgamento. Este é aplicado quando a gestão aplica as componentes de controlo interno em relação às categorias de compromissos adequados e avalia os riscos de forma a alcançar os anteriores. O julgamento é também

aplicado quando seleciona, desenvolve e implementa os controlos necessários aos princípios e avalia se os componentes e princípios estão presentes e a funcionar, bem como quando avalia a gravidade das deficiências de controlo interno.

Ao nível do ambiente de controlo, o Grupo EDP afigura deter uma posição ética, com integridade e valores. Pela existência da carta de responsabilidades constata-se que as funções e responsabilidades estão devidamente delimitadas. Está interiorizada uma cultura convenientemente estruturada, com as indispensáveis linhas de reporte. É, também observável, a importância dada ao fator recursos humanos pelo investimento feito.

No âmbito da avaliação do risco, por forma a assegurar que esta seja fiável, atempada e consistente foi atribuída à DGR a realização da sua gestão contínua. Assim, é possível à organização especificar com clareza suficiente os seus objetivos, para que facilmente sejam identificados e avaliados os riscos associados a estes. A este nível, é também considerado o risco de fraude no planeamento das atividades da DAI, inclusive as áreas geográficas fora de Portugal, bem como na avaliação do risco. De notar, que são tidos em conta todos os fatores que potenciam a fraude, a saber, a oportunidade, a pressão e a racionalização.

Na componente das atividades de controlo é devidamente feita a ligação entre a avaliação do risco e as atividades de controlo, tendo em conta os vários tipos de controlos possíveis de aplicar. A aplicação das atividades de controlo são adequadamente aplicadas aos vários níveis da entidade. Um importante fator nesta componente, é a consideração pela segregação de funções, que no Grupo EDP é aplicado através de uma aplicação. Para poder avaliar as atividades de controlo, foram instituídas políticas que estabelecem o que é esperado, bem como os procedimentos que colocam em prática tais políticas.

Ao nível da informação, esta encontra-se devidamente suportada para operar eficazmente dentro dos 5 componentes do modelo COSO. São consideradas diversas fontes de informação, podendo assim obter o maior e mais variado tipo de informação. Aquando da obtenção de informação externa, esta necessita de se encontrar nos parâmetros pré-estabelecidos. A comunicação interna é feita através do portal denominado por *intranet*, apenas acessível aos colaboradores da entidade. Quando a informação é dirigida, existem processos de comunicação reservados. De notar neste ponto, que existe uma linha direta de comunicação entre a Direção de Auditoria Interna com o Comité de Auditoria. A comunicação externa, um pouco mais que a comunicação externa, necessita de passar por um processo de aprovação formal antes de ser comunicada. São tidas em grande conta a

informação comunicada por terceiros, pois é este que detém um maior poder sobre os clientes.

Nas atividades de monitorização são tidas em grande conta supervisão do controlo interno, pelo fato de constituírem o objetivo do trabalho proposto. Foi possível concluir que, tal como emanado no princípio 16, que a avaliação do controlo interno, passa pelo exame se se encontram presentes e a funcionar todos os componentes do modelo COSO, é possível afirmar que sim pela presença de evidências que consubstanciam a afirmação.

A devida comunicação da avaliação do controlo interno é apresentado ao Conselho de Administração e Comité de Auditoria, estes por sua vez, emitem o seu parecer, para que possam ser tomadas medidas corretivas às deficiências reportadas pela Auditoria Interna. É possível, também constatar que se encontra implementado e a funcionar um processo de acompanhamento, de deficiências de controlo interno, bem como de auditorias.

Em termos conclusivos, na área de Controlo Interno dentro do Grupo EDP pode-se observar que subsiste um sistema bem suportado e evidenciado, com base em modelos aceites a nível mundial, COSO e COBIT, apresentando-se num nível de excelência.

CONCLUSÃO

Com o culminar dos tempos, a importância que o controlo interno possui numa organização tem sido cada vez maior, em grande parte devido aos escândalos financeiros. Muito devido à abrangência e ao mesmo tempo manter o enfoque em temas com elevada importância, como a gestão de riscos, o suporte na tomada de decisão para o alcance de objetivos, a manutenção da regulamentação atualizada com exigências do mercado, a qualidade, transparência e atempada informação financeira, permitindo aos clientes, fornecedores, investidores e colaboradores obterem informação materialmente relevante ao negócio.

Com a prática do uso da metodologia do controlo interno, através da implementação de um conjunto de medidas, as organizações passam a estar dotadas de um perfil máximo de *controller*, ou seja, existe uma maior atenção em estabelecer objetivos reais e atingíveis, que alcancem todos os níveis da organização no âmbito das operações, de relato e cumprimento de normas.

A metodologia com maior aceitação, em parte por estar alinhada com o normativo regulamentar, é o modelo COSO. Este é apresentado como um modelo de referência para a implementação, gestão e controlo de um adequado sistema de controlo interno, daqui resulta a possibilidade de melhorar o desempenho organizacional e reduzir o alcance das fraudes nas organizações.

Com a implementação do sistema de controlo interno é praticável a definição de normas de ética e conduta, assegura a confiança no cumprimento de objetivos, através de pareceres do funcionamento do negócio, estabelece as formas de atuação a todos os níveis da organização, com a fixação de objetivos claros e mensuráveis, concede uma segurança razoável sobre a adequada gestão dos riscos e estabelece mecanismos de monitorização para solucionar deficiências no funcionamento do sistema de controlo interno.

Para o diagnóstico das peças fulcrais no adequado funcionamento do sistema de controlo interno de uma organização, foi seguida a metodologia de investigação através de um estudo de caso. Para tal, foi realizada uma entrevista introdutória e aplicado um questionário em formato *check-list*, para conseguir obter a maior abrangência possível ao nível dos princípios.

Da análise da entrevista e com a resposta à *check-list* foi possível validar a ideia pré-concebida da existência de um bom Sistema de Controlo Interno no Grupo EDP. Ainda que

este seja direcionado para o Relato Financeiro, foi exequível diagnosticar o sistema de controlo interno de uma maneira geral, conforme requisitos segundo modelo COSO e, por sua vez, apurar que este é eficaz e eficiente, pela presença completa do mesmo.

Em forma de conclusão, pode-se afirmar que uma das melhores defesas contra a falha de um negócio, bem como um importante motor de desempenho empresarial, é ter um sistema de controlo interno eficaz, que faça a gestão do risco e permita a criação e preservação de valor. Assim, organizações bem-sucedidas são as que sabem aproveitar as oportunidades e combater as ameaças, em muitos dos casos através da aplicação de controlos eficazes e, assim, melhoram o desempenho.

LIMITAÇÕES

A maior limitação no estudo de caso foi o facto de este apenas ter sido respondido por um elemento, apresentado assim pouca representação, porém este detém uma grande importância no funcionamento do tema em estudo, com muita experiência e que permitiu partilhar informação imperativa nos vários aspetos abordados no trabalho. Deixando o caso empírico um pouco aquém do que era ambicionado, contudo foi possível validar muitos dos pontos importantes para confirmar afirmações feitas.

Não menos importante, a outra limitação foi o facto de haver muita informação para a revisão bibliográfica. Por vezes menos relevante para o estudo e haver a necessidade de delimitar a informação aos pontos de interesse.

De notar, que a adoção de metodologias que facilitem o investigador elaborar a sua pesquisa de forma mais segura, eficiente e eficaz faz com que se poupe o precioso tempo.

PROPOSTA PARA FUTURO ESTUDO

Inicialmente, o trabalho seria composto por uma avaliação à eficácia e eficiência dos componentes do modelo COSO, porém, pela impossibilidade do fator tempo, a presente dissertação teve alterações no objetivo a alcançar

Desta forma, como linha de investigação futura, preconiza-se a realização deste estudo, com interesse no setor bancário, pelo fato de se encontrar normalizado ao nível do controlo interno, nomeadamente segundo o Banco Central Europeu e pelo Banco de Portugal.

Já com alguns artigos publicados e normas emanadas, diagnosticar como impactam as atividades em *outsourcing* no sistema de controlo interno numa organização.

BIBLIOGRAFIA

- Araújo, I. P. S.; (2004) *Introdução à AUDITORIA Operacional (2º ed.)*; Rio de Janeiro: FGV Editora
- Arwinge, O; (2013) *Internal Control – A Study of Concept and Themes*; . Berlim: Physica – Verlag HD
- Baptista da Costa, C. (2014); *Auditoria Financeira : Teórica & Prática (10º ed.)*; Lisboa: Rei dos Livros.
- Basu, S. K.; (2007) *Auditing Principles & Techniques (2º ed.)*; India: Dorling Kindersley Pvt. Ltd.
- Carrilho Ramos, S. T., Naranjo, E. S.; (2014) *Metodologia da Investigação Científica*; Escolar Editora: Angola.
- Committee of Sponsoring Organizations of the Treadway Commission; (1994) *Internal Control – Integrated Framework*. New Jersey.
- Cohen, L., Manion, L., Morrison, K. (2007); *Research methods in education (6º ed.)*, Londres: Routledge.
- Coutinho, C. P.; (2014) *Metodologias de Investigação em Ciências Sociais e Humanas*; Lisboa: Almedina.
- DRA (Directriz de Revisão e Auditoria) 400. *Avaliação do Risco de Revisão/Auditoria*. Emitida em maio de 2000, pela Ordem dos Revisores Oficiais de Contas.
- DRA (Directriz de Revisão e Auditoria) 410. *Controlo Interno*. Emitida em maio de 2000, pela Ordem dos Revisores Oficiais de Contas.
- Gomes, E; (2014) *A Importância do Controlo Interno no Planeamento de Auditoria*; Lisboa: OROC - Revista 64
- Guerra, I. C.; (2006) *Pesquisa Qualitativa e Análise de Conteúdo – Sentidos e formas de uso*; Estoril: Principal Editora, Lda.
- Government Accountability Office (US); (2014); *Standards for Internal Control in the Federal Government*; Estados Unidos da América: GAO. Disponível em: <https://books.google.pt/books?id=Gf4oOFhIpNEC&pg=PA9&dq=objectives+internal+control&hl=pt->

PT&sa=X&ved=0ahUKEwj9usnus4nNAhXB2xoKHd9GCg0Q6AEIPTAE#v=onepage&q=objectives%20internal%20control&f=false

Inácio, H. C.; (2014) *Controlo Interno – Enquadramento teórico e aplicação prática*. Lisboa: Escolar Editora.

Lapan, S. D.; Quartaroli, M. T.; Riemer, F. J.; (2011) *Qualitative Research: an introduction to methods and designs*; Estados Unidos da América: John Wiley & Sons, Inc.

Leedy, P. D., Ormrod, J. E.; (1993) *Practical Research – Planning and Design (5º ed.)*; Edimburgo: Pearson Education Limited.

Lisboa, I.; Auditoria interna passa por valorização no cenário atual; São Paulo: Folha de São Paulo.

Marques, F.L., Marçal, N.; (2011) *Manual de Auditoria e Controlo Interno no Sector Público*. Lisboa: Edições Sílabo

Morais. G.; Martins., I.; (2013) *Auditoria Interna Função e Processo (4º ed.)*; Lisboa: Áreas Editora.

Neves, J. F.; (2008, Junho). A importância de um Sistema de Controlo Interno. Lisboa: TOC 99. Disponível em: http://www.otoc.pt/downloads/files/1213983276_60e61_gestao.pdf

Oliveira, E. R; Ferreira, P.; (2014) *Métodos de Investigação: da interrogação à descoberta científica*; Porto: Grupo Editorial Vida Económica.

Pereira, N. P.; A importância do controle interno para a gestão das empresas. Rio de Janeiro: Pensar Contábil.

Pfister, J. A., (2009) *Managing Organizational Culture for Effective Internal Control – From Practice to Theory*. Berlim: Physica – Verlag HD.

Pickett, K. H. S.; (2003) *The Internal Auditing Handbook (2º ed.)*; Inglaterra: Wiley.

Pinheiro, J. L. (2010); *Auditoria Interna – Auditoria Operacional – Manual Prático para Auditores Internos (2.ª ed.)*. Lisboa: Rei dos Livros.

Prodanov, C. C.; Freitas, E. C.; (2013) *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico (2º ed)*; Brasil: Editora Feevale

Roldán, M.; Chavarría, J.; (2010) *AUDITORÍA FORENSE*; Madrid: EUNED

Sawyer, L. B.; Dittenhofer, M. A.; Scheiner, J. H.; (2003) *The Practice of Modern Internal Auditing*; Florida: IIA.

Silva, E. L.; Menezes, E. M.; (2005) *Metodologia da pesquisa e elaboração de dissertação* – 4. ed. rev. atual.; Florianópolis: Universidade Federal de Santa Carrina - UFSC.

Swinkels, W. H. A.; (2012) *Exploration of a theory of internal audit: a study on the theoretical foundations of internal audit in relation to the nature and the control systems of Dutch public listed firms*; Amesterdão: Amsterdam Business School Research Institute.

Trenerry, A; (1999) *Principles of Internal Control*; Sydney: UNSW – University of New South Wales Press Ltd

Zhang, X.; (2014) *Enterprise Management Control Systems in China*; Berlim: Springer – Verlag Berlin Heidelberg

Sites consultados

<http://accounting-simplified.com/audit/introduction/types-of-audits.html>

<http://www.portaldeauditoria.com.br/artigos/testesemauditoria.htm>

<http://www.oroc.pt/gca/?id=279>

http://www.theiia.org/chapters/pubdocs/336/IIA_Newsletter___JAN_08.pdf

<http://accounting-simplified.com/audit/introduction/types-of-audits.html>

<http://www.globaliia.org>

http://www.theiia.org/chapters/pubdocs/336/IIA_Newsletter___JAN_08.pdf

<http://cadbury.cjbs.archios.info/report>

<http://www.infocontab.com.pt/download/dra/dra400.pdf>

http://www.ebizq.net/blogs/chief_risk_officer/2013/10/a_quick_guide_to_coso_internal.php

https://www.edp.pt/pt/aedp/governosocietario/etica/EDP%20Documents/CodigoEticaFev2014_PT.pdf

<https://www.edpessoa.internet.edp.pt/CEZANNECV/RecruitmentWeb/CznWfResearch.asp?FUNID=7004517&LANGID=2070>

<http://www.edp.pt/pt/aedp/governosocietario/gestaodorisco/Pages/RiskManagement.aspx>

<https://www.edpannualreport.edp.pt/2011/pt/sustentabilidade/modelo-organizativo-do-grupo/sistemas-de-controlo-gestao-risco>

<http://www.tibco.com/>

ANEXOS

Anexo 1 – Formas de registo do controlo interno

1. Questionário padronizado

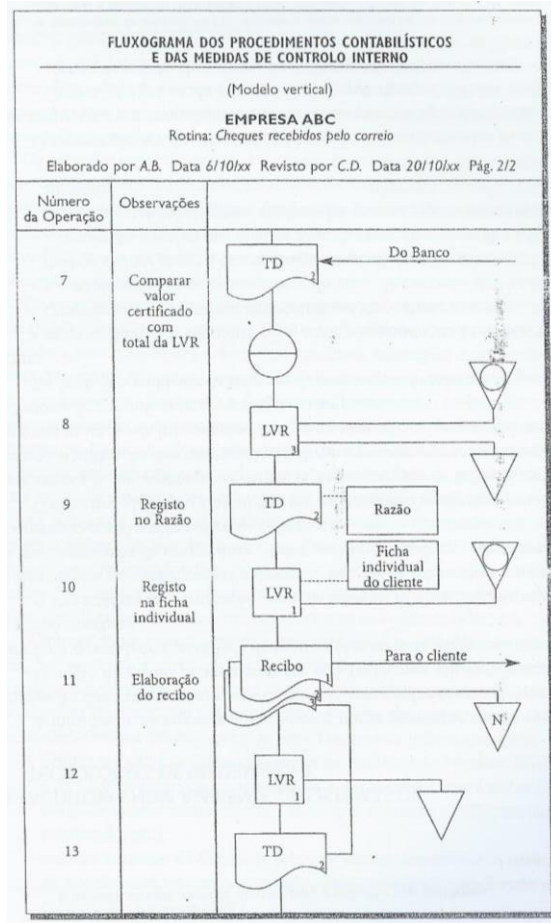
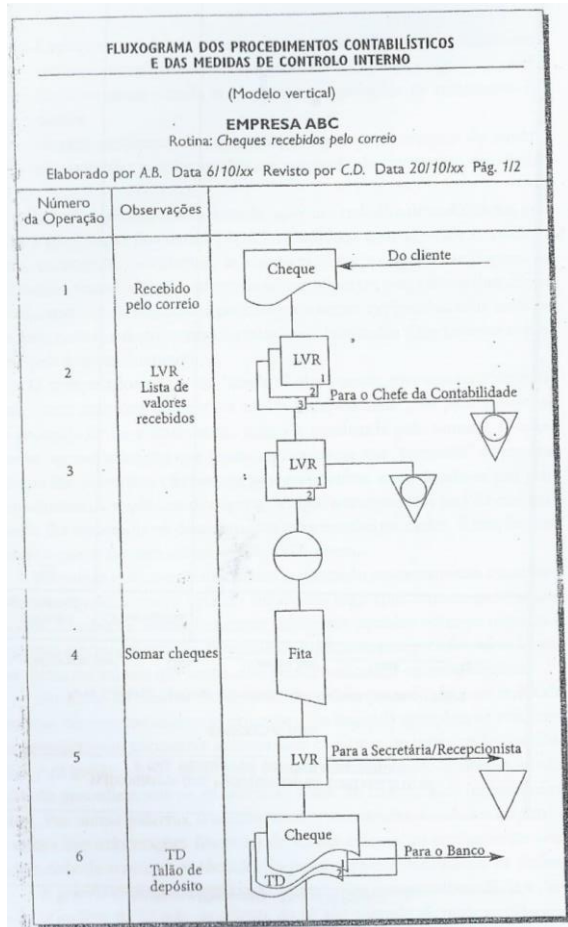
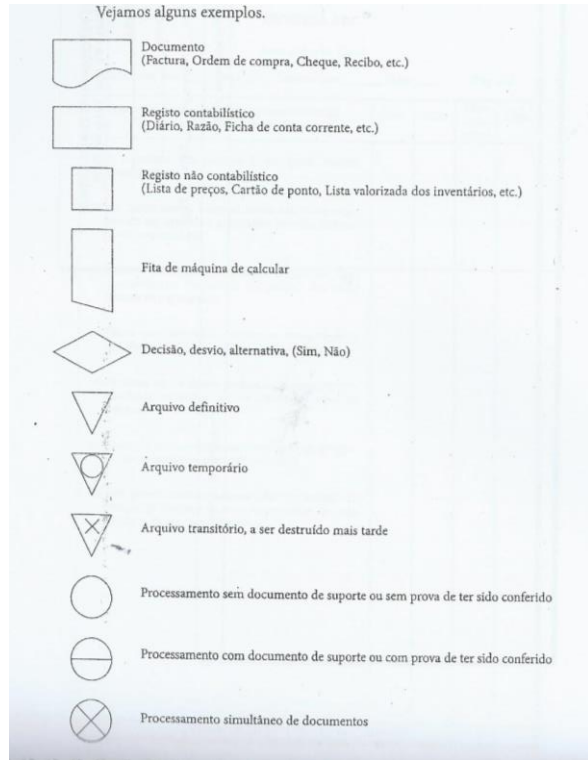
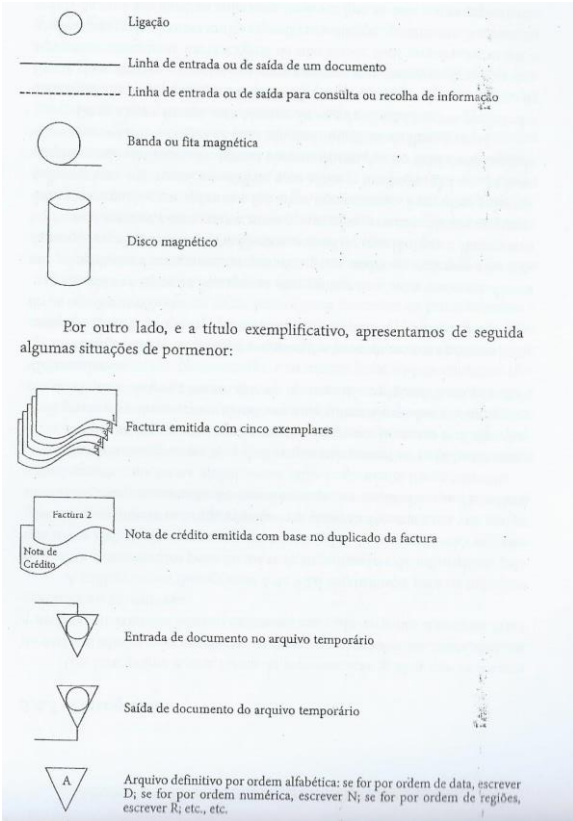
QUESTIONÁRIO SOBRE PROCEDIMENTOS CONTABILÍSTICOS E MEDIDAS DE CONTROLO INTERNO				
EMPRESA ABC				
Área coberta: <i>Geral</i>				
Elaborado por _____ Data _____		Revisto por _____ Data _____		Pág. 1/2
Descrição do procedimento contabilístico e/ou da medida de controlo interno	Sim	Não	Não aplicável	Obs.
1. A empresa possui um organigrama? Em caso afirmativo obter uma cópia.				
2. A empresa possui um manual de controlo interno? Em caso afirmativo obter uma cópia.				
3. A empresa possui um manual de contabilidade? Em caso afirmativo obter uma cópia.				
4. Em caso negativo, existe um plano de contas (lista de contas)? Em caso afirmativo obter uma cópia.				
5. Faz-se orçamentos anuais e procede-se ao seu controlo?				
6. Fazem parte dos quadros da empresa: - Director Financeiro? - Chefe da Contabilidade? - Auditor Interno? - Técnico Oficial de Contas?				
7. A secção de Contabilidade está separada das secções de: - Tesouraria? - Vendas? - Compras? - Produção?				
8. Todos os empregados gozam anualmente férias sendo as suas funções, durante o período de ausência, desempenhadas por outros empregados?				

QUESTIONÁRIO SOBRE PROCEDIMENTOS CONTABILÍSTICOS E MEDIDAS DE CONTROLO INTERNO				
EMPRESA ABC				
Área coberta: <i>Geral</i>				
Elaborado por _____ Data _____		Revisto por _____ Data _____		Pág. 2/2
Descrição do procedimento contabilístico e/ou da medida de controlo interno	Sim	Não	Não aplicável	Obs.
9. A cobertura dos seguros é, em geral, revista anualmente?				
10. Os lançamentos contabilísticos são adequadamente suportados e aprovados por um empregado responsável?				
11. Elabora-se mensalmente informações de tipo contabilístico, financeiro, de gestão? Em caso afirmativo, quais são?				
12. Existe um calendário relativo ao cumprimento das obrigações fiscais, para-fiscais e outras?				
13. No caso de existirem sucursais, delegações ou similares, exerce-se algum controlo sobre as mesmas?				
14. Todos os documentos em circulação na empresa são numerados tipograficamente?				
15. Está genericamente estabelecido o princípio da rotação de funções entre os empregados de cada secção e de secções diferentes?				

2. Narrativa

NARRATIVA DOS PROCEDIMENTOS CONTABILÍSTICOS E DAS MEDIDAS DE CONTROLO INTERNO	
EMPRESA _____	
Área coberta: _____	
Elaborado por _____ Data _____ Revisto por _____ Data _____ Pág. _____	
Procedimento inicial	Procedimento actual

3. Fluxogramas



Fonte: Auditoria Financeira – Teoria e Prática (2014)

Anexo 2 – Áreas de Foco

Control environment	
Principles	Points of focus
1. The organization demonstrates a commitment to integrity and ethical values.	<ul style="list-style-type: none"> • Sets the tone at the top • Establishes standards of conduct • Evaluates adherence to standards of conduct • Addresses deviations in a timely manner
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<ul style="list-style-type: none"> • Establishes oversight responsibilities • Applies relevant expertise • Operates independently • Provides oversight for the system of internal control
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<ul style="list-style-type: none"> • Considers all structures of the entity • Establishes reporting lines • Defines, assigns, and limits authorities and responsibilities
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<ul style="list-style-type: none"> • Establishes policies and practices • Evaluates competence and addresses shortcomings • Attracts, develops, and retains individuals • Plans and prepares for succession
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	<ul style="list-style-type: none"> • Enforces accountability through structures, authorities, and responsibilities • Establishes performance measures, incentives, and rewards • Evaluates performance measures, incentives, and rewards for ongoing relevance • Considers excessive pressures • Evaluates performance and rewards or disciplines individuals

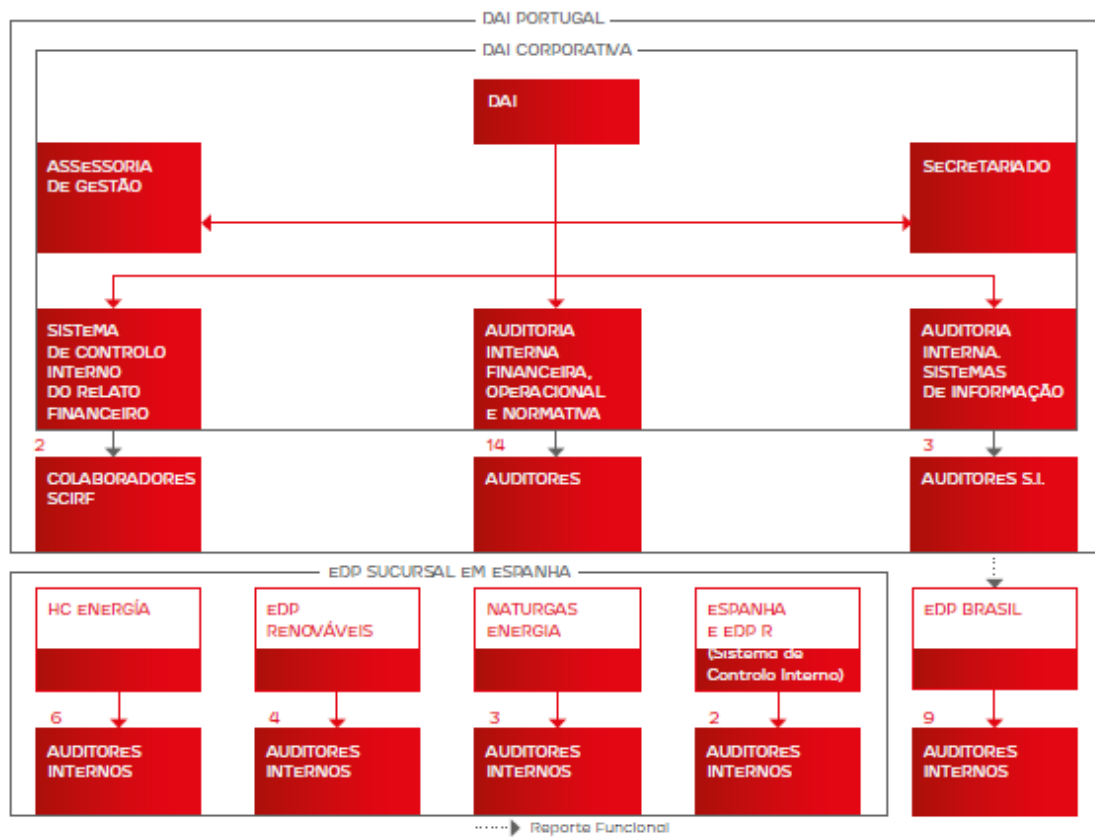
Risk assessment		
Principles	Objectives	Points of focus
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Operations Objectives	<ul style="list-style-type: none"> • Reflects management's choices • Considers tolerances for risk • Includes operations and financial performance goals • Forms a basis for committing of resources
	External Financial Reporting Objectives	<ul style="list-style-type: none"> • Complies with applicable accounting standards • Considers materiality • Reflects entity activities
	External Non-Financial Reporting Objectives	<ul style="list-style-type: none"> • Complies with externally established standards and frameworks • Considers the required level of precision • Reflects entity activities
	Internal Reporting Objectives	<ul style="list-style-type: none"> • Reflects management's choices • Considers the required level of precision • Reflects entity activities
	Compliance Objectives	<ul style="list-style-type: none"> • Reflects external laws and regulations • Considers tolerances for risk
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		<ul style="list-style-type: none"> • Includes entity, subsidiary, division, operating unit, and functional levels • Analyzes internal and external factors • Involves appropriate levels of management • Estimates significance of risks identified • Determines how to respond to risks
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.		<ul style="list-style-type: none"> • Considers various types of fraud • Assesses incentive and pressures • Assesses opportunities • Assesses attitudes and rationalizations
9. The organization identifies and assesses changes that could significantly impact the system of internal control.		<ul style="list-style-type: none"> • Assesses changes in the external environment • Assesses changes in the business model • Assesses changes in leadership

Control activities	
Principles	Points of focus
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	<ul style="list-style-type: none"> • Integrates with risk assessment • Considers entity-specific factors • Determines relevant business processes • Evaluates a mix of control activity types • Considers at what level activities are applied • Addresses segregation of duties
11. The organization selects and develops general control activities over technology to support the achievement of objectives.	<ul style="list-style-type: none"> • Determines dependency between the use of technology in business process and technology general controls • Establishes relevant technology infrastructure control activities • Establishes relevant security management process control activities • Establishes relevant technology acquisition, development, and maintenance process control activities
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	<ul style="list-style-type: none"> • Establishes policies and procedures to support deployment of management's directives • Establishes responsibility and accountability for executing policies and procedures • Performs in a timely manner • Takes corrective action • Performs using competent personnel • Reassesses policies and procedures

Information and communication	
Principles	Points of focus
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.	<ul style="list-style-type: none"> Identifies information requirements Captures internal and external sources of data Processes relevant data into information Maintains quality throughout processing Considers costs and benefits
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	<ul style="list-style-type: none"> Communicates internal control information Communicates with the board of directors Provides separate communication lines Selects relevant method of communication
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.	<ul style="list-style-type: none"> Communicates to external parties Enables Inbound Communications Communicates with the board of directors Provides separate communication lines Selects relevant method of communication
Monitoring activities	
Principles	Points of focus
16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	<ul style="list-style-type: none"> Considers a mix of ongoing and separate evaluations Considers rate of change Establishes baseline understanding Uses knowledgeable personnel Integrates with business processes Adjusts scope and frequency Objectively evaluates
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	<ul style="list-style-type: none"> Assesses results Communicates deficiencies Monitors corrective actions

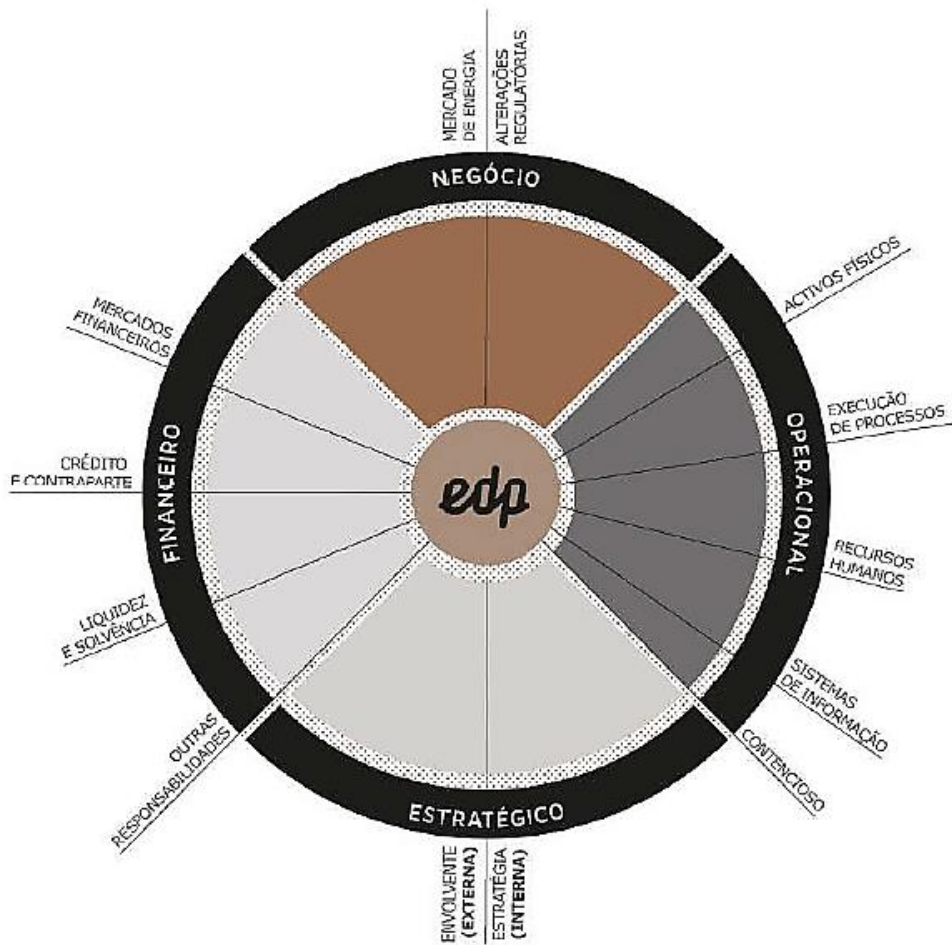
Fonte: Placemat Deloitte (2014)

Anexo 3 – Organograma DAI



Fonte: Relatório Auditoria Interna (2011; 11)

Anexo 4 – Taxonomia dos riscos do Grupo EDP



Fonte: Relatório & Contas (2015: 200)

Estratégico	Negócio	Financeiro	Operacional
1.1 Ambiente (Externo) <ul style="list-style-type: none"> Grave crise macro (saída Euro) Crise social e política (expropriação de ativos) Disrupção tecnológica Alterações climáticas Alteração do paradigma competitivo 	2.1 Mercados energéticos <ul style="list-style-type: none"> Preço da pool e commodities Consumo energético Volumes de renováveis Margem das vendas 	3.1 Mercado financeiro <ul style="list-style-type: none"> Taxa de câmbio Taxa de juro Inflação Valor de ativos financeiros 	4.1 Ativos físicos <ul style="list-style-type: none"> Ativos em desenvolvimento Danos a ativos em operação Perdas técnicas/ não técnicas
1.2 Estratégia (Interno) <ul style="list-style-type: none"> M&A Relação com stakeholders Governance Planeamento corporativo 	2.2 Regulação <ul style="list-style-type: none"> Pacotes sectoriais Modelo regulatório Impostos sectoriais e taxas Normas contabilísticas Normas ambientais Concessões 	3.2 Crédito <ul style="list-style-type: none"> Clientes Contrapartes 	4.2 Processos <ul style="list-style-type: none"> Processos comerciais Fornecedores e outsourcing Faturação, custeio e pagamentos Controlo de gestão e execução orçamental Modelo de execução de processos Outros
		3.3 Liquidez <ul style="list-style-type: none"> Tesouraria Acesso a/ custo de capital Downgrade de rating 	4.3 RH <ul style="list-style-type: none"> Saúde e segurança Conduta não ética e fraude Relações laborais e sindicatos
		3.4 Outras responsabil. <ul style="list-style-type: none"> Fundo de pensões Outras responsabilidades (e.g., médicas) 	4.4 SI (sistemas infor.) <ul style="list-style-type: none"> Disponibilidade Segurança e integridade
			4.5 Legal <ul style="list-style-type: none"> Administrativo Civil Fiscal Laboral Outros

Fonte: Programa Anual de Desenvolvimento para Administradores não Executivos - Um modelo global e integrado de gestão do risco (2015)

Anexo 5 – Check-list de Controlo Interno

Questionário de Avaliação do Ambiente de Controlo

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
1. Integridade e Valores Éticos				
1.1. A integridade figura-se presente na empresa?	sim			
1.2. O compromisso da Administração para com a Integridade e os Valores Éticos são comunicados às várias Direções?	sim			
1.3. Existe um Código de Ética na empresa, que providencie <i>standards</i> de forma a guiar os comportamentos, atividades e decisões da organização?	sim			
1.4. A empresa detém um processo de comunicar os <i>standards</i> de comportamentos a toda a organização, incluindo prestadores de serviços?	sim			
1.5. A empresa possui um processo de avaliação do cumprimento dos <i>standards</i> ? Por ex.: Procedimentos contínuos e periódicos de <i>compliance</i> ; investigação de alegados não- <i>compliance</i> com os <i>standards</i> , entre outros.	sim			
1.6. A empresa dispõem de níveis de tolerância para desvios aos <i>standards</i> ?	sim			
1.7. Se sim, os desvios são avaliados e medidas são tomadas de forma atempada?	sim			
2. Independência e Supervisão do Conselho de Administração				
2.1. Os antecedentes e experiência do Conselho de Administração são os adequados, em virtude da natureza do negócio da empresa?	sim			
2.2. O Conselho de Administração participa em formações, de forma a manter os seus conhecimentos atuais e relevantes?	sim			
2.3. O Comité de Auditoria tem uma carta que delimite as funções e responsabilidades? E recursos e autoridade adequados para se absolver das responsabilidades?	sim			
2.4. O Conselho de Administração e o Comité de Auditoria mantém-se informados, atentos e supervisionam de forma eficaz o processo de reporte financeiro e o controlo interno da organização, de modo a que cubra as 5 componentes do controlo interno?	sim			
2.5. O Conselho de Administração e o Comité de Auditoria mantém-se atuais quanto às práticas do controlo interno, bem como da indústria e, respetivos regulamentos que afetem o Sistema de Controlo Interno da organização?	sim			
2.6. Existe uma linha de comunicação direta entre o Conselho de Administração ou do Comité de Auditoria com entidades externas ou auditores internos?	sim			
3. Estrutura Organizacional e Linhas de reporte				
3.1. A organização está estruturada dada a sua dimensão e complexidade?	sim			
3.2. As linhas de reporte funcionam de maneira a que dentro da estrutura organizacional seja passível de planejar, executar, controlar e avaliar as atividades da organização?	sim			
3.3. Existem políticas e procedimentos ou uma matriz de autorização e aprovação adequada nos diferentes níveis da Direção?	sim			
3.4. As funções e respetivas responsabilidades estão alinhadas com os objetivos?	sim			
3.5. Os contratos de <i>outsourcing</i> são claros e concisos quanto aos objetivos, expetativas de conduta e <i>performance</i> , níveis de competência e fluxo de informação e comunicação?	sim			
3.6. A definição das funções da Direção de Auditoria Interna estão em conformidade com as normas e regulamentos?	sim			

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
4. Recursos Humanos				
4.1. Existem procedimentos uniformizados na contratação, formação, motivação, avaliação, promoção, compensação, transferência e término de emprego, aplicável a todas as áreas funcionais da empresa?	sim			
4.2. A descrição das funções encontra-se referenciado num manual ou num formato escrito e comunicado aos trabalhadores?	sim			
4.3. É feita avaliação formal periódica das competências, por forma a determinar lacunas ligados à falta de formação, comportamentos que indiquem incompetência, bem como motivação dos colaboradores?	sim			
4.5. Aquando da avaliação de competências, as lacunas identificadas são colmatadas?	sim			
4.6. As Direções mostram-se envolvidas no processo de contratação e formação, de maneira a manterem-se alinhadas com o crescimento e complexidade do negócio?	sim			
4.7. Existe conexão entre os padrões de conhecimento e as expetativas de desempenho dos colaboradores?	sim			
5. Recursos Humanos e Responsabilidades sobre o Controlo Interno				
5.1. A estrutura da organização está estabelecida de forma a instituir e impor responsabilização individual no desempenho de responsabilidades de controlo interno?	sim			
5.2. Existe um mecanismo que regularmente instrua e comunique à Direção e respetivos colaboradores a importância do controlo interno, para que possa haver melhor entendimento dos controlos?	sim			
5.4. A organização tem medidas, incentivos ou recompensas de <i>performance</i> alinhadas com os valores éticos e responsabilidades sob o controlo interno?	sim			
5.5. As Direções ou Conselho de Administração avalia as responsabilidades de controlo interno, incluindo a adesão aos <i>standards</i> de conduta e níveis de competência?	sim			
5.6. Os riscos a que a empresa está sujeita, resultando em requisitos estabelecidos do sistema de controlo interno, são compreendidos de forma a que seja possível alcançar os objetivos?	sim			

Questionário de Avaliação do Risco

Descrição do procedimento de controlo interno		Sim	Não	Não Aplicável	Observações
6. Identificar objetivos para identificar e avaliar os riscos					
6.1.	Os objetivos para relato financeiro externo são consistentes com a estrutura de relatório financeiro e apropriados às circunstâncias?	sim			
6.2.	A Direção estabelece um limite de materialidade para efeitos de identificação de rubricas contabilísticas e divulgações significativas?	sim			
6.3.	São tidos em conta os riscos em todas as localizações geográficas onde a empresa opera?	sim			
6.4.	As políticas, procedimentos e processos da empresa facilitam a elaboração das Demonstrações Financeiras, refletindo os eventos que geram o movimento contabilístico? Ou seja, são eventos relevantes, de representação fidedigna, comparáveis, verificáveis, atempados e compreensíveis.	sim			
6.5.	Os requisitos da Estrutura Conceptual relativos ao relato financeiro são revistos periodicamente e devidamente atualizados?	sim			
6.6.	A organização possui um processo para avaliar conjuntos de atividades, de maneira a verificar se todas as que se destacam como materialmente relevantes, estão refletidas adequadamente nas demonstrações financeiras?	sim			
7. Identificação de riscos para atingir os objetivos					
7.1.	Na avaliação dos riscos é feito o detalhe da sua identificação, análise e resposta?	sim			
7.2.	A organização identifica os riscos para a concretização dos objetivos de reporte financeiro a todos os níveis (unidades operacionais, níveis funcionais, empresas do grupo, entre outros)?	sim			
7.3.	O processo de identificação dos riscos para alcançar os objetivos financeiros, tem em consideração os fatores de risco interno e externo, para cada demonstração financeira?	sim			
7.4.	No processo de avaliação de cada risco é tido em conta o impacto e probabilidade de ocorrência do risco?	sim			
7.5.	A avaliação do risco é revisto com intervalo de tempo apropriado?	sim			Anual
7.6.	Na tolerância do risco e respetiva gestão, é considerada a sua prevenção, redução, partilha e aceitação?	sim			
8. Fraude na avaliação de riscos					
8.1.	Quando é feito o plano de atividades de auditoria é considerado o risco de fraude?	sim			
8.2.	A empresa realiza avaliações de risco relacionadas com relato financeiro fraudulento, <i>management override</i> , perda potencial de ativos e corrupção?	sim			
8.4.	A organização tem estabelecidos procedimentos para reconciliar periodicamente os ativos em relação ao que se encontra registado?	sim			
8.5.	As áreas geográficas com maior risco de fraude onde a empresa opera são tidas em conta na avaliação de riscos?	sim			
8.6.	Na avaliação do risco de fraude associado ao relato financeiro são consideradas as escolhas dos princípios e estimativas contabilísticas?	sim			
8.7.	Na avaliação do risco de fraude são tidos em conta os incentivos, pressões, oportunidades, atitudes e racionalização?	sim			
8.8.	Na avaliação do risco de fraude são consideradas as várias formas de como podem ocorrer o risco de fraude no relato financeiro? Por ex.: - Orientações da Direção; - Incentivos que podem motivar comportamentos fraudulentos; - Natureza das TI e a capacidade da Direção de manipular informação; - Possíveis esquemas para contornar as atividades de controlo.	sim			

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações	
9. Modificações no ambiente de Controlo Interno					
9.1.	Existem grupos de trabalho responsáveis por antecipar mudanças externas com possíveis efeitos na organização (ex.: a nível regulamentar ou da economia)?	sim			
9.2.	Se sim, existe algum processo de informar as Direções dos possíveis efeitos na organização?	sim			Reuniões periódicas do Centro Corporativo com os Gestores Locais do Controlo Interno
9.3.	A organização considera o impacto para o sistema de controlo interno de novas linhas de negócio, grandes alterações às já existentes, ao rápido crescimento, mudanças a nível geográfico, a novas tecnologias, entrada de novos administradores?	sim			
9.4.	São tidos em conta os impactos de mudanças no ambiente de controlo interno na avaliação do risco?	sim			
9.5.	A organização tem um processo para considerar mudanças na Direção e a respetiva atitude e filosofia perante o sistema de controlo interno?	sim			

Questionário de Avaliação das Atividades de Controlo

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
10. Atividades de Controlo perante os Riscos e Objetivos				
10.1. Os colaboradores envolvidos no processo de construção e implementação de controlos são adequados (ex.. Auditores internos, recursos humanos da área financeira, entre outros)?	sim			
10.2. Os controlos incluem os vários tipos de controlo: manuais e automáticos, preventivos e detetivos?	sim			
10.3. Os controlos identificados abordam a integridade, precisão e validação das transações processadas?	sim			
10.4. Os controlos encontram-se mapeados de forma a abordar cada risco relacionado com os princípios das demonstrações financeiras?	sim			
10.5. É tida em conta a precisão (1) dos controlos quando avaliada a extensão que cada um destes aborda os riscos? Por ex.: - Se o nível de precisão é objetiva ou subjetiva; - A natureza de erros identificados por controlos; - Existência de evidência de forma a confirmar se o controlo atua corretamente; - Se existência de <i>follow-up</i> é adequado às discrepâncias ou erros identificados.	sim			
10.6. Os controlos existem a todos os níveis da organização, desde a nível operacional, direções e funções?	sim			
10.7. A segregação de funções funciona de forma eficaz e eficiente?	sim			Existe um programa informático
10.8. Existe um mecanismo automático ou outra ferramenta que assegure uma adequada segregação de funções?	sim			
11. Atividades de Controlo perante IT e Objetivos				
11.1. Existe um processo para selecionar, desenvolver, utilizar e fazer manutenção a nível de IT?	sim			
11.2. Se sim, os processos são suficientes, na sua completude, tendo em conta a sua natureza e extensão de uso?	sim			
11.3. Os controlos de IT identificados consideram as infraestruturas tecnológicas em uso? Ex.: <i>backups</i> de aplicações, bases de dados e sistemas operativos são efetuados com intervalos de tempo adequados e periodicamente testados.	sim			
11.4. A empresa tem identificados controlos apropriados para abordar os riscos quando o uso das aplicações é feita por terceiros?	sim			Exige uma auditoria independente
11.5. Os controlos gerais encontram-se muito dependentes do uso de tecnologias?	sim			Usa-se o Cobit
11.6. Existem controlos no processo de gestão da segurança, aquisição, desenvolvimento e manutenção tecnológica?	sim			
11.7. Os colaboradores de IT têm perfis que incompatibilizem a realização de operações como <i>end-user</i> ?	sim			
11.8. Os perfis dos colaboradores são revistos de forma periódica às diferentes aplicações e bases de dados de forma a determinar se os privilégios de acesso encontram-se apropriados?	sim			

(1) Precisão, isto é, grau a que os controlos, se operarem de forma eficaz, evitam ou detectam erros materialmente relevantes nas demonstrações financeiras .

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
12. Políticas e Procedimentos de Atividades de Controlo				
12.1.	Todas as políticas e procedimentos encontram-se devidamente documentadas e suportadas pelo conhecimento do pelouro?	sim		
12.2.	As políticas e procedimentos são documentados e implementados assim que surge a necessidade, de forma a suprir acontecimentos idênticos?	sim		
12.3.	A empresa revê políticas e procedimentos para determinar se faz sentido a sua permanência ou se carecem atualização de forma atempada?	sim		
12.3.	Existe um função centralizada de controlo interno na organização?	sim		

Questionário de Avaliação da Informação e Comunicação

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
13. Informação de suporte ao Controlo Interno				
13.1. A empresa tem estabelecidos requisitos de informação para suportar operações eficazes de controlo dentro das 5 componentes?	sim			
13.2. Se sim, os requisitos estão a níveis relevantes e com formato específico de forma a suportar a identificação de fontes de informação relevantes e fiáveis?	sim			
13.3. A empresa considera como fontes de informação interna e externa quando identifica informação relevante para utilizar no exercício do controlo interno?	sim			
13.4. A qualidade da informação é revista periodicamente, de forma a avaliar a fiabilidade e atualidade?	sim			Testes
13.5. Em relação à informação obtida de forma externa, existem controlos que assegurem: - Que as fontes externas são apropriadas; - Que a informação detenha evidências que suportem a fonte; - A informação é de qualidade suficiente para suportar o funcionamento eficaz do controlo interno.	sim			
13.6. A informação obtida e produzida encontra-se armazenada num repositório, como por exemplo um <i>data warehouse</i> ou uma pasta partilhada sem acesso externo?	sim			
13.7. Os sistemas de informação geram informação de qualidade suficiente de forma a suportar um eficiente controlo interno? Como exemplo, a Direção que detém o pelouro do IT tem desenvolvido e implementado controlos relacionados com: - Dados completos e precisos; - Proteção de dados sensíveis; - Fornecimento de informação quando necessário; - Recolha de dados com frequência necessária.	sim			
13.8. A Administração legítima a importância da comunicação para o sucesso da organização?	sim			
13.9. As linhas de comunicação são suficientes para atender a necessidades de quem emite e recebe as comunicações?	sim			
14. Comunicação Interna de suporte ao Controlo Interno				
14.1. Os novos colaboradores recebem formação quando iniciam funções ou quando se procede à transferência de Direção, para debater sobre a natureza, âmbito e responsabilidades?	sim			
14.2. Esta formação inclui orientações específicas de controlo interno e respetivas responsabilidades?	sim			
14.3. A empresa tem implementadas políticas e procedimentos que facilitem a comunicação sobre controlo interno, quer sejam individualizadas ou a toda a empresa?	sim			Manuais
14.4. Existe um processo para facilmente divulgar informação crítica a toda a empresa quando necessário?	sim			Intranet
14.5. Quando há um reforço de comunicação aos colaboradores das suas responsabilidades perante o controlo interno, estas são tomadas de forma séria e rigorosa?	sim			
14.6. A Direção de Auditoria Interna tem uma linha direta de comunicação com o Comité de Auditoria?	sim			
14.7. Existe um processo para os colaboradores comunicarem má conduta e atividades ilegais, por exemplo, o <i>whistleblowing</i> ? E este processo permite o anonimato?	sim			
14.8. No caso de existência deste processo, foram tidas em conta as referências geográficas, culturais, étnicas, por forma a determinar o método de comunicação mais adequado?	sim			
14.9. Existe um processo de avaliação da eficácia das comunicações para assegurar que os métodos encontram-se em pleno funcionamento?	sim			

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
15. Comunicação Externa de suporte ao Controlo Interno				
15.1. A empresa detém um processo para comunicar informação relevante e oportuna às partes externas, incluindo acionistas, reguladores, clientes, fornecedores, analistas financeiros ou outras partes?	sim			
15.2. A empresa possui um processo de aprovação formal anterior à comunicação ao exterior?	sim			
15.3. Existe um processo de monitorização das comunicações dos clientes, fornecedores, reguladores ou outras partes e, fazer com que sejam partilhadas?	sim			
15.4. A informação procedente de entidades externas relacionada com atividades de controlo interno avaliadas pela gestão é, quando apropriado, comunicado à Administração ou Comité de Auditoria?	sim			
15.5. Existem meios de comunicação separados fora da via normal disponível a clientes, fornecedores e prestadores de serviços, de forma a permitir a comunicação direta com a Direção? Como por exemplo nos casos de whistleblowing.	sim			

Questionário de Avaliação de Atividades de Monitorização

Descrição do procedimento de controlo interno	Sim	Não	Não Aplicável	Observações
16. Avaliação das Componentes do Controlo Interno				
16.1. A empresa tem processo para avaliar se os controlos estão presentes e a funcionar tal como pretendido?	sim			
16.2. A Administração reconhece que as atividades de controlo são ferramentas que auxiliam a identificar, prevenir e reduzir riscos?	sim			
16.3. A monitorização contínua inclui avaliações baseadas em processos de comunicação de negócios/financeiros e executados em avaliações separadas?	sim			
16.4. Os planos de monitorização incluem um combinado entre monitorização contínua e avaliações separadas e da frequência da monitorização de atividades, tendo em conta: - O âmbito e a natureza das operações da empresa; - Os grau de risco ao longo da empresa; - A frequência e importância de mudanças nas operações.	sim			
16.5. Nas atividades de controlo são utilizados os controlos preventivos e detetivos?	sim			
16.6. A monitorização de atividades providencia compreensão do ponto de situação do controlo interno, como exemplo, realização de <i>follow-ups</i> ?	sim			
16.7. Os resultados da monitorização de atividades considerados como base para determinar futuras atividades de monitorização?	sim			
16.8. Os colaboradores que realizam a monitorização possuem formação especializada adequada?	sim			
16.9. A função de Auditoria Interna é empregue como parte das atividades de monitorização da empresa?	sim			
16.10. Se sim: - É independente? - Os auditores internos comunicam diretamente ao Conselho de Administração e Comité de Auditoria? - O âmbito das atividades da Auditoria apropriadas dada a natureza, dimensão e estrutura da organização?	sim			
16.11. Existem funções similares à auditoria que reportam ao Conselho de Administração e que afetam o ambiente de controlo em geral? Como, por exemplo, nos casos em que a Direção do risco ou gabinete de compliance identifica deficiências.	sim			
16.12. As atividades de monitorização incluem a observação, indagação e avaliação de evidências?	sim			
16.13. Existem procedimentos para monitorizar quando os controlos são sobrepostos? Se sim, é possível determinar se apropriado?	sim			
16.14. As atividades em <i>outsourcing</i> carecem de atividades de monitorização pela organização?	sim			
17. Comunicação deficiências Controlo Interno				
17.1. Existe um processo para aglomerar e avaliar as questões identificadas por atividades de monitorização?	sim			
17.2. As deficiências e recomendações de partes externas, como reguladores, clientes, fornecedores e auditores externo é tido em conta?	sim			
17.3. As deficiências identificadas por terceiros são devidamente comunicadas, à Direção, Conselho de Administração ou Comité de Auditoria?	sim			
17.4. Os resultados das atividades de Auditoria Interna são reportados, quando apropriados, à Direção, Conselho de Administração e Auditoria Externa?	sim			
17.5. Existem políticas e procedimentos para assegurar que as deficiências são comunicadas externamente?	sim			
17.6. A Direção toma adota medidas adequadas e de forma atempada para corrigir as deficiências reportadas pela Auditoria Interna e/ou outra atividade de	sim			
17.7. A Direção responde de forma atempada e apropriada às deficiências e recomendações dos auditores independentes sobre o controlo interno e políticas e procedimentos da empresa?	sim			
17.8. Existe um processo para acompanhar as deficiências de controlo e um protocolo elevá-las a níveis superiores, se necessário?	sim			Reportes

(2) Monitorização contínua: encontra-se, tipicamente, perto das operações de controlo; encontra-se na primeira linha para identificar fraquezas.

(3) Avaliações separadas: geralmente é mais objetiva; os resultados validam a monitorização contínua; realizada pela auditoria interna e/ou compliance; com base no risco.

Anexo 6 – Código de Conduta (capa) – Grupo EDP



Fonte:

https://www.edp.pt/pt/aedp/governosocietario/etica/EDP%20Documents/CodigoEticaFev2014_PT.pdf

Anexo 8 – Modelo de Responsabilidades do Sistema de Controlo Interno e do Relato Financeiro (capa) – Grupo EDP



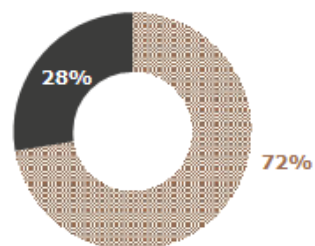
Fonte: PPTX “Formação – Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP” - e Intranet SOUEDP

Anexo 9 – Formação dos colaboradores da DAI – Grupo EDP

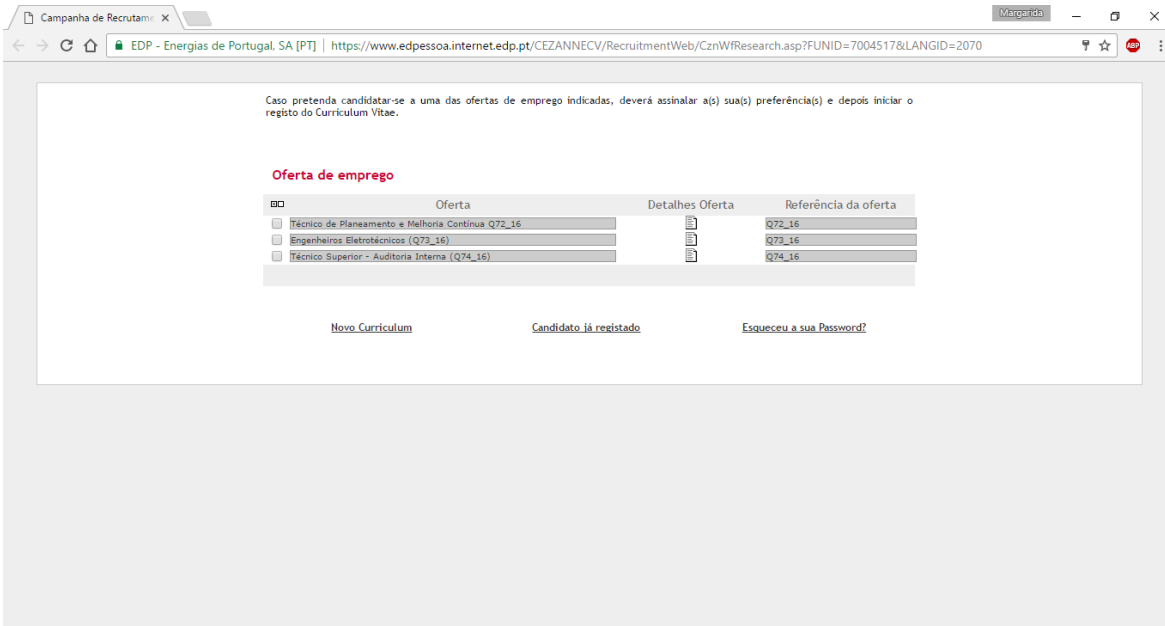
DOMÍNIO	Nº Horas	%
Área Formativa		
COMPORAMENTAL	188	7
Relações Interpessoais e Comunicação	70	
Liderança	44	
Ética	34	
Produtividade Pessoal	16	
Criatividade Aplicada	24	
GESTÃO	149	6
Finanças	16	
Gestão	40	
MBA/Mestrado/Pós-Graduação	68	
Gestão de Tempo	16	
Legal/Regulação	9	
ORGANIZACIONAL	496	19
<i>Executive Development Program</i>	84	
<i>Energizing Development Program</i>	184	
Cliente EDP 365	8	
Empresa Familiarmente Responsável	74	
<i>Amplify</i>	69	
Sessões de Acolhimento	39	
Relações interpessoais e comunicação	27	
Um encontro com...	6	
Ética	3	
Ambiente	2	
TÉCNICA	1.731	68
Negócio de Energia	555	
Línguas	287	
Auditoria Interna	182	
Legal / Regulação	178	
IPAI / IIA	106	
<i>SAP Viewer</i>	87	
Sistemas de informação	59	
Office 365	46	
SIM-PT	30	
CIA	27	
Técnicas de negócio	20	
Prevenção e Segurança	19	
Técnicas de Apresentação	16	
Amostragem em Auditoria	15	
Compliance	9	
Gestão de Risco	8	
Outras	88	
TOTAL	2.563	100

72% Formação Interna

28% Formação Externa



Anexo 10 – Plataforma de recrutamento – Grupo EDP



Caso pretenda candidatar-se a uma das ofertas de emprego indicadas, deverá assinalar a(s) sua(s) preferência(s) e depois iniciar o registo do Curriculum Vitae.

Oferta de emprego

BID	Oferta	Detalhes Oferta	Referência da oferta
<input type="checkbox"/>	Técnico de Planeamento e Melhoria Contínua (Q72_16)		Q72_16
<input type="checkbox"/>	Engenheiros Eletrotécnicos (Q73_16)		Q73_16
<input type="checkbox"/>	Técnico Superior - Auditoria Interna (Q74_16)		Q74_16

[Novo Curriculum](#) [Candidato já registado](#) [Esqueceu a sua Password?](#)

Fonte:

<https://www.edpessoa.internet.edp.pt/CEZANNECV/RecruitmentWeb/CznWfResearch.asp?FUNID=7004517&LANGID=2070>

Anexo 11 – Manual do Sistema de Controlo Interno e do Relato Financeiro (capa)



Fonte: PPTX “Formação – Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP” e Intranet SOUEDP

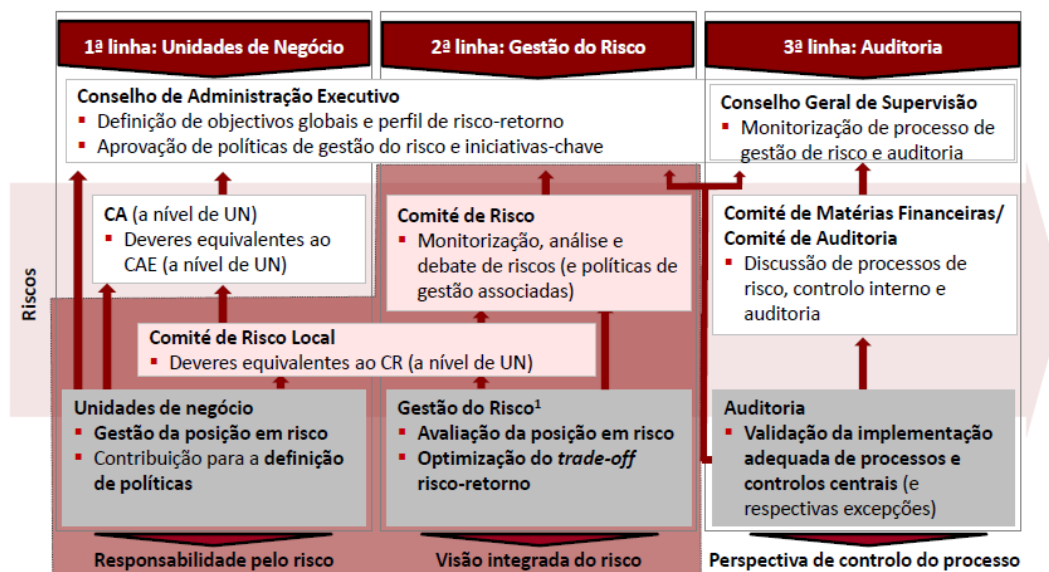
Anexo 12 – SCI no Universo do Grupo EDP



Fonte: EDP - 2015 Relatório de Atividades de Direção de Auditoria Interna (pág. 30)

Anexo 13 – Modelo das linhas de defesa – Grupo EDP

Modelo das três linhas de defesa – detalhe para o Grupo EDP



Fonte: Programa Anual de Desenvolvimento para Administradores não Executivos - Um modelo global e integrado de gestão do risco (2015)

Anexo 14 – Intranet «edpon»

The screenshot displays the edpon intranet interface. At the top, there is a navigation bar with the edpon logo and tabs for 'Geral', 'Colaboradores', 'Grupos', and 'Documentos'. A search bar is located to the right of these tabs. Below the navigation bar, there are several main sections:

- destaques**: A featured article titled 'Novo Posto Médico SÁVIDA no Porto' with a photo of a woman in a white lab coat.
- Os meus Grupos**: A list of groups including 'CONCILIAR' (504 membros) and 'Escuteiros EDP' (39 membros).
- notícias**: A section for news, including 'Leading Across Cultures' and 'Universidade EDP promove seminário'.
- as minhas notícias**: A section for personal news, stating 'Não tem notícias internas subscritas'.
- edpon meios**: A section for edpon media, featuring 'edpon tv', 'edpon rádio', and 'edpon revista'.
- biblioteca edp group**: A section for the edp group library, featuring 'Certificado de Aprovação do SGSC' and 'Síntese das Revisões do SGSC_2016'.
- atalhos**: A section for shortcuts, including 'Site EDP no Brasil', 'Site EDP Renováveis', and 'Site Grupo EDP'.
- contactos**: A section for contacts.

At the bottom of the page, there is a financial data section showing stock prices for EDP, EDPR, and EDPBR, along with a weather widget for Lisboa showing a high of 29°C and a low of 18°C.

Fonte: <http://intranet.edpon.pt>

Anexo 15 – Formação SCIRF – Grupo EDP




Formação

Sistema de Controlo Interno sobre o Relato Financeiro

Grupo EDP


XX de Setembro de 201x

Direção de Auditoria Interna



Agenda

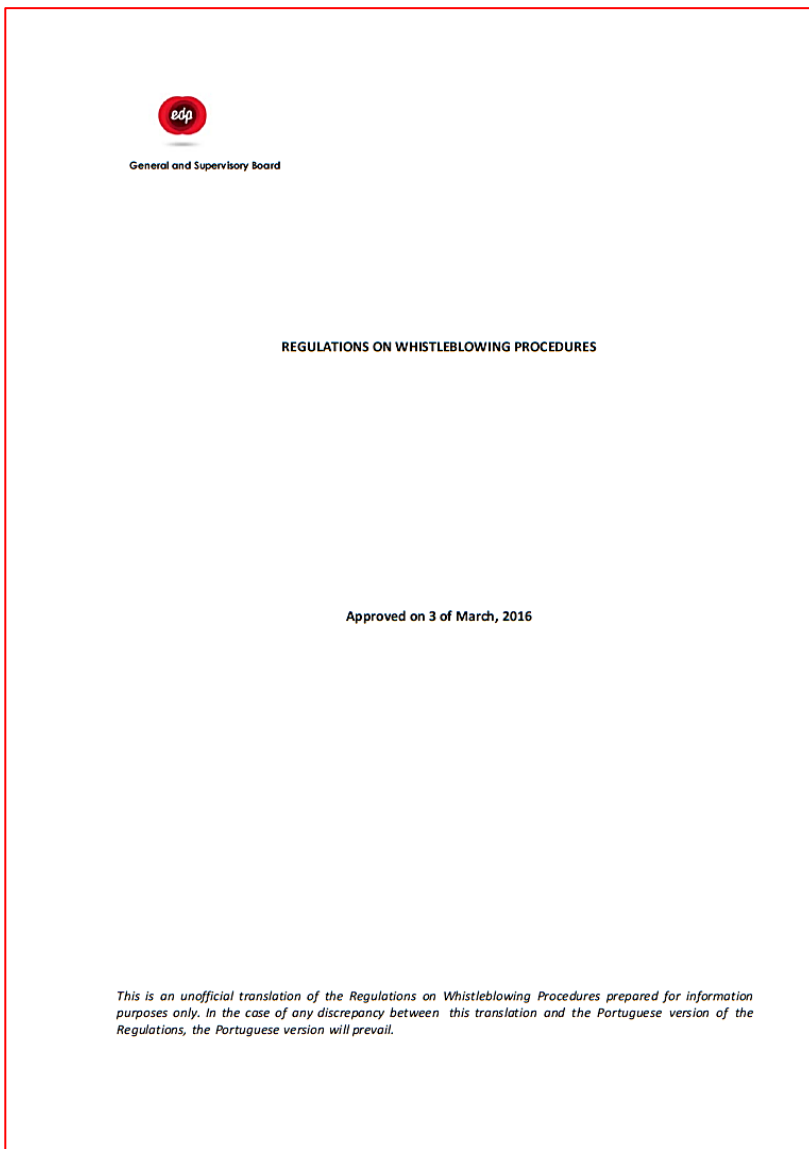
Introdução	3
Capítulo 1 – Princípios gerais do controlo interno	
• O que é o controlo interno ?	7
• Objetivos de um sistema de controlo interno	10
• Identificação de riscos e objetivos de controlo	12
• Instrumentos do SCIRF no Grupo EDP	14
Capítulo 2 – Principais componentes do SCIRF	
• Frameworks de referência	18
Capítulo 3 – Ciclo SCIRF – operacionalização	
• Fase 1 – Âmbito	25
• Fase 2 – Documentação e não conformidades	
• Fase 3 – Avaliações	86
• Fase 4 – Relatório final e certificações	95
Capítulo 4 – Modelo organizativo e de responsabilidades do SCIRF	101



2

Fonte: PPTX “Formação – Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP”

Anexo 16– *Regulations on Whistleblowing Procedures* – Grupo EDP



Fonte:

<https://www.edp.pt/en/aedp/governosocietario/comunicacaodeirregularidades/Whistle%20Blowing/Regulations%20on%20Whistleblowing%20Procedures.pdf>

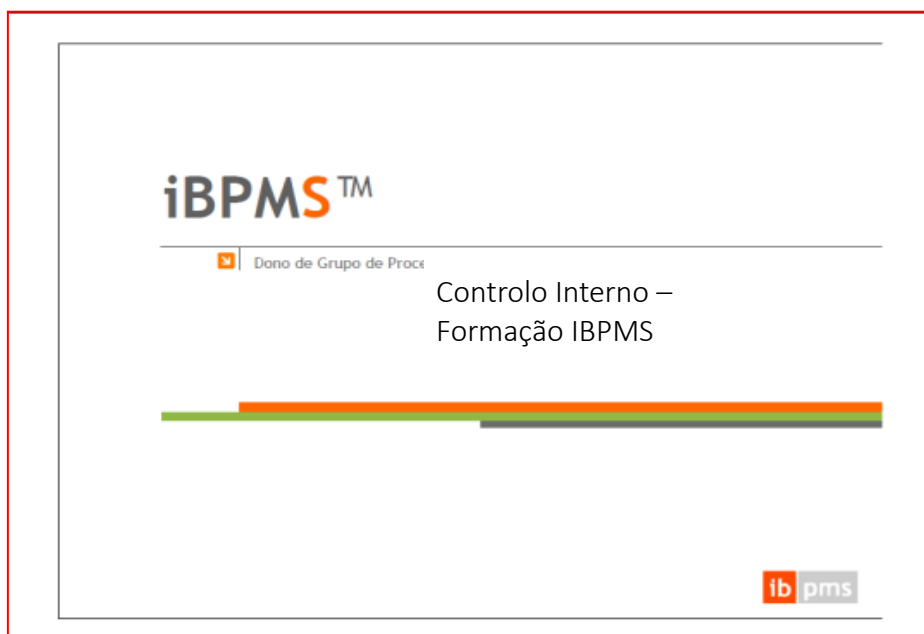
Anexo 17 – Aplicação de Controlo Interno – Grupo EDP

The screenshot displays the 'Controlo Interno' application interface. The top navigation bar includes 'Home', 'Actividades', 'Processos & Controlos', 'UDAS', 'Avaliação', 'Não Conformidades', 'Oportunidades de Melhoria', 'Acções', 'Auto-certificação', 'Sign-Off', 'Biblioteca', 'Cockpit', and 'Info'. The main menu on the left is titled 'Controlos' and is divided into three sections: 'Controlos por estado' (with sub-items: Alocados (35), Documentação/Revisão (2), Validação (0), Execução (33), Inactivo (0)), 'Controlos por estado de avaliação' (with sub-items: Avaliação de Desenho: Adequado (15), Não adequado (1), Sem ocorrências (0), Aguarda avaliação (0), Sem avaliação (20); and Avaliação de Eficácia: Avaliados (32), Efectivo (31), Não efectivo (0), Sem ocorrências (1), Aguarda avaliação (0), Sem avaliação (3)).

The main content area is titled 'Registrar Apicacional (MIC_InternalControlMgr@) - Metastorm e-Work - Windows Internet Explorer'. It shows a 'Controlo Apicacional' form with two numbered steps: 1. Identificar Unidade Empresarial / Processo / Objectivo de Controlo / Riscos, and 2. Dados Gerais do Controlo. Below the steps, there are three sections: 'Unidade Empresarial' with a table for selecting a unit (ID, Nome) and buttons for 'Associar Unid. Emp.', 'Associar Unid. Org.', 'Consultar', and 'Remover'; 'Processos' with a message 'Escolha uma Unidade Empresarial'; and 'Objectivos de Controlo' with a message 'Escolha um Processo'.

Fonte: PPTX “Formação – Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP”

Anexo 18 – Formação iBPMS – Grupo EDP



Fonte: PPTX “Formação – Sistema de Controlo Interno sobre o Relato Financeiro – Grupo EDP”