Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Data Warehouse: Modelo de Auditoria e Controlo Interno

Rui Almeida Santos

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Sistemas Integrados de Apoio à Decisão (Business Intelligence)

Orientador:
Doutor Alberto Carneiro,
Professor na UAL

Co-orientador:
Doutor Henrique O'Neill,
Professor no ISCTE

Outubro, 2009

ISCTE IUL
Instituto Universitário de Lisboa

Data Warehouse: Modelo de Auditoria e Controlo Interno

Rui Almeida Santos

Dezembro 2009

ÍNDICE

RESUMO

O objectivo central desta investigação consiste em apresentar um modelo que permita avaliar eficazmente o sistema de controlo interno e auditoria de um Data Warehouse (DW).
Para que seja facilmente aceite por auditores e auditados, propõe-se que a construção deste modelo tenha como referência os principais standards de controlo interno especialmente concebidos para avaliar tecnologias de informação (TI), nomeadamente as metodologias do CobiT® 4.1, do ITIL® V3 e do ISO/IEC 27002.

Assim, a presente investigação assentará em três pilares:

I. O Estado da Arte de:
    a. Data Warehouse – Os componentes desta arquitectura são o principal objecto de avaliação;
    b. Controlo Interno e Auditoria Interna – Meios para conseguir optimizar a prestação do DW;
    c. Modelo de governação das tecnologias de informação (IT-Governance) – Resumo das melhores e mais recentes práticas internacionais de controlo e gestão de tecnologias e sistemas de informação.
II. Desenvolvimento de um modelo de análise e avaliação do controlo interno das componentes e fases do Data Warehouse
III. Validação do modelo através de um estudo de caso constituído por uma acção de auditoria ao Data Warehouse de uma Instituição financeira.

As conclusões da investigação incidirão sobre as vantagens que as organizações poderão obter se utilizarem um modelo específico para avaliar e controlar a gestão do Data Warehouse.

ABSTRACT

The main purpose of this research is to present a model to effectively assess the internal control of Data Warehouse.
For this template to be easily accepted by auditors and audited, we propose the use of a reference set of control standards and methodologies specially conceived to assess information technology environments, such as, CobiT® 4.1, ITIL® V3 and ISO/IEC 27002.

Therefore, this research will be based on three pillars:

I. The State of the Art:
    a. Data Warehouse – The components of this architecture are the primary object of evaluation;
    b. Internal Control and Audit – Means to achieve optimum performance of a DW;
    c. IT Governance – Summary of the most recent and international accepted best practices to control and manage IT environment
II. Development of a framework to assess the DW internal control, all its components and stages
III. Model validation through a case study comprising an internal auditory action to a Financial Institution Data Warehouse environment

The research findings will focus on the advantages that organizations may obtain from using a specific template to assess and control the Data Warehouse management.

PALAVRAS-CHAVE

⇒ Modelo de Controlo e Auditoria Interna
⇒ Ambiente de Controlo
⇒ Auditoria de Sistemas de Informação (ASI)
⇒ Auditoria Interna
⇒ Fluxo de dados
⇒ Business Intelligence (BI)
⇒ Control Objectives for Information and related Technology (COBIT® 4.1)
⇒ Data Mart
⇒ Data Mining
⇒ Data Warehouse (DW)
⇒ Extract Transform and Load (ETL)
⇒ Gestão de riscos
⇒ Information Technology Infrastructure Library (ITIL® V3)
⇒ International Organization for Standardization (ISO)
⇒ Modelo de governação de tecnologias de informação (IT Governance)
⇒ Objectivos de Controlo
⇒ Requisitos de DW
⇒ Sistema de Controlo Interno
⇒ Tecnologia de Informação (TI)
⇒ Comité de Tecnologias de Informação (TI)

1. INTRODUÇÃO

"No início dos anos 40 surgiram nas organizações os primeiros sistemas de informação automatizados que se baseavam em computadores. Na altura eram sistemas simples e de operação limitada, no entanto, rapidamente cresceram em número e em complexidade. Progressivamente surgiram tecnologias como a gestão de bases de dados, o processamento em tempo real, as redes e as aplicações online.
À medida que o tempo passava e as empresas cresciam ou se fundiam, novas aplicações foram sendo desenvolvidas ou compradas e as aplicações mais antigas tornaram-se obsoletas. Antes que os gestores se apercebessem do problema, já existiam múltiplas aplicações informáticas nas organizações, cada uma delas tratando de forma separada uma parte do negócio.
Foi neste contexto de grande crescimento dos sistemas de informação que surgiu o dilema da necessidade de informação de gestão.
Os gestores sabiam que a informação existia, no entanto, devido à multiplicidade de sistemas, tecnologias, filosofias e arquitecturas de funcionamento, não era possível recolher a informação necessária, de uma forma expedita e concordante, com a qualidade suficiente para suportar o processo de tomada de decisão." (Inmon, 2001)

1.1 – Motivação, Problema e Espaço de Solução

1.1.1 – O Data Warehouse (DW)

"O DW é um sistema de informação que assegura a extracção, a limpeza, a conformidade, e a entrega dos dados da organização em bases de dados dimensionais, dando igualmente suporte ao processo de consulta e análise para efeitos do processo de tomada de decisão" (Kimball & Caserta, 2004)

Tradicionalmente um sistema de informação operacional visa satisfazer os requisitos de uma determinada unidade da empresa, no entanto, no caso do DW o foco é servir de base à satisfação da necessidade de informação de toda a organização, no que diz respeito ao processo de tomada de decisão, quer esta seja de nível estratégico, táctico ou operacional. O Data Warehouse é um activo da empresa e existe para benefício corporativo, não apenas para benefício de uma pessoa ou unidade da organização.

1.1.2 – Motivos para melhorar a gestão e o controlo do DW

Os projectos de Data Warehouse são normalmente dispendiosos. Os dados gerados pelas várias áreas do negócio têm de ser extraídos de sistemas díspares e integrados num repositório único de dados.
As iniciativas de suporte à decisão suportadas por um DW podem proporcionar vantagens competitivas, mas também exigem recursos adicionais para a organização, como por exemplo, novas tecnologias, tarefas específicas, especialidades profissionais e novas responsabilidades.
Assim, o insucesso dos projectos DW deve-se essencialmente a factores como: o planeamento inadequado, tarefas mal implementadas, incumprimento de prazos, gestão de projecto deficiente, incumprimento de requisitos de negócio ou falta de qualidade da informação final (Rodero et al, 1999).
Por outro lado, apesar de o nível de informação contida no DW facultar aos utilizadores uma visão mais intuitiva do negócio, o desenvolvimento e operação do DW pode ser alvo de constrangimentos que podem condicionar o seu sucesso.
Segundo um estudo apresentado por Emily Kay, os principais desafios do DW são, por ordem de importância, os seguintes (Kay, 1997):

- *Gestão da qualidade dos dados; Modelação dos dados de negócio; Especificações dos utilizadores; Transformação de dados legados; Análise das regras de negócio; Gestão das expectativas; Performance das bases de dados.*

Deste modo, a má gestão e controlo destes problemas pode acarretar riscos de impacto elevado para a organização, especialmente pela possibilidade de sucederem erros durante os complexos processos de extracção, transformação e carregamento nos DW, dos dados que são extraídos dos sistemas operacionais da organização[1].
Adicionalmente, a natureza e o tipo de informação residente no DW é determinante para todo o processo de gestão do negócio, ou seja, o impacto de um erro a este nível será muito elevado pois grande parte das decisões importantes para o futuro da organização são tomadas com base em informações proporcionadas pelo Data Warehouse.
Pelas razões referidas acima, a informação armazenada no Data Warehouse representa um activo de valor quase inestimável para a organização, o que faz aumentar a necessidade de gerir e controlar eficazmente as tecnologias de informação que suportam esta arquitectura, nomeadamente através da sistematização de um processo de controlo que seja eficaz, abrangente e aceite por todos os 'stakeholders' com interesse no DW.

1.1.3 – O Problema

O problema que a presente investigação se propõe solucionar reside na dificuldade que as organizações têm em assegurar a governação eficaz e o controlo das suas tecnologias de suporte à decisão, criando mecanismos eficazes para avaliar se a informação proporcionada pelo DW está alinhada com os objectivos de negócio da organização e se os gestores estão a retirar o máximo benefício da informação e conhecimento proporcionado, ou seja, se o valor gerado para a organização corresponde ao previsto no plano de projecto do DW, se os recursos afectos estão a ser utilizados de forma eficaz e responsável e se os riscos estão a ser geridos de forma apropriada.

1.1.4 – Proposta de solução

A forma indicada para optimizar qualquer processo de gestão reside em melhorar o seu sistema de controlo interno, nomeadamente através da implementação de melhorias nas grandes componentes de controlo que constituem esse mesmo sistema.
Assim, podemos definir controlo interno como:

"O Controlo Interno é um sistema concebido para assegurar, com um elevado grau de confiança, que os objectivos definidos, aos vários níveis da gestão de uma organização, estão a ser devidamente atingidos." (COSO, 1992)

1.2 – Estrutura e Objectivos

1.2.1 – Objectivos da Dissertação

Os objectivos desta dissertação são:

- Explicitar os pressupostos que justificam a implementação de um sistema de controlo interno do Data Warehouse, perceber todas as dimensões de conhecimento associadas a uma arquitectura BI de suporte à decisão e identificar o 'estado da arte' nesta área de conhecimento;

[1] Este processo é vulgarmente conhecido por ETL – Extract, Transform and Load ou por Data Integration.

- Propor um modelo ou uma base de trabalho que se aplique de forma simples e expedita aos Data Warehouses das organizações, que possibilite a implementação de um sistema de controlo interno facilmente auditável, que garanta uma boa governação das tecnologias de informação abrangidas e que assegure a identificação dos riscos associados, bem como dos respectivos planos de mitigação;

- Realizar um estudo de caso que permita avaliar se a aplicação do modelo num Data Warehouse real trará uma melhoria significativa do sistema de controlo interno e da respectiva gestão.

1.2.2 – Metodologia de Investigação

O primeiro passo desta investigação consiste em justificar o porquê da necessidade de construir um modelo de controlo interno que optimize o processo de gestão do DW, com especial enfoque na satisfação dos objectivos para os quais foi criado **(Passo 1)**.
O passo seguinte reside na análise e sistematização dos componentes fundamentais deste tipo de ferramentas de suporte à decisão, sendo primordial conseguir abranger todas as fases e vertentes que constituem o processo de Data Warehousing **(Passo 2)**.

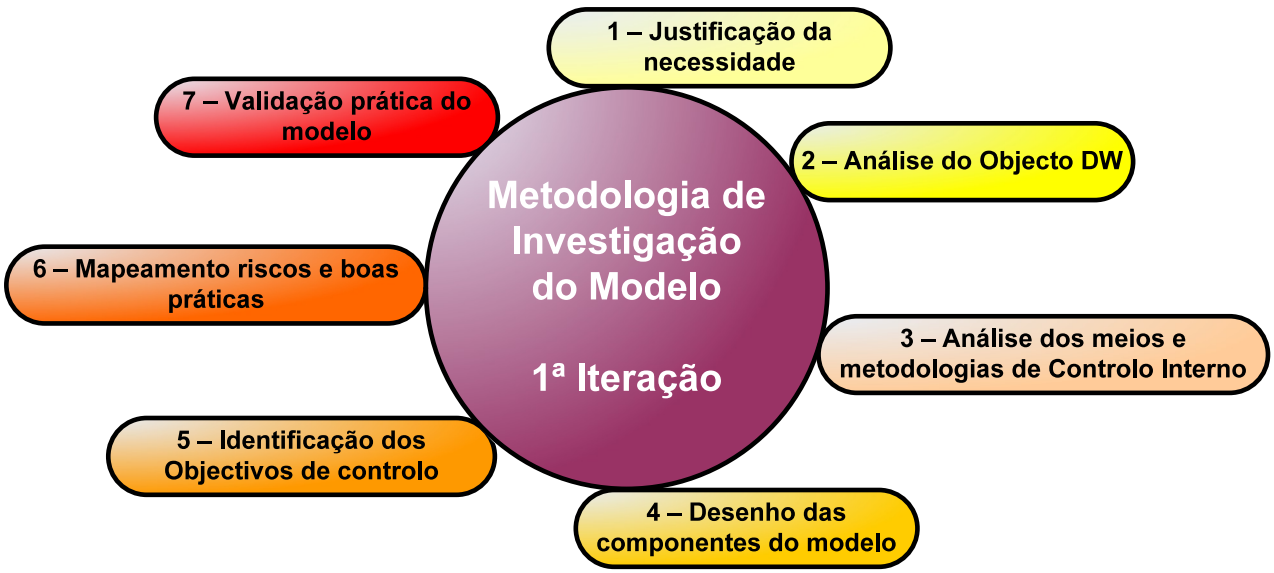

Ilustração 1 – Método utilizado para investigar e construir o modelo de avaliação do controlo interno de um DW

Outro aspecto muito importante a analisar é o conjunto de meios mais utilizados para construir um adequado sistema de controlo interno do DW, bem como identificar quais os métodos e standards mais utilizados para avaliar os controlos implementados **(Passo 3)**.
Os passos seguintes deste método são: Desenhar um modelo que sistematize todos os componentes do DW **(Passo 4)**, e enumerar os objectivos de controlo, as principais actividades, funções e responsabilidades de cada uma das componentes do modelo **(Passo 5)**.
Uma vez identificados os componentes de controlo do modelo, é determinante efectuar um mapeamento **(Passo 6)** dos riscos associados a cada componente, bem como identificar os processos e boas práticas de controlo mais adequadas, que se encontram definidas no âmbito dos Standards de avaliação de tecnologias de informação, como sejam o CobiT® 4.1, o ITIL® V3 e o ISO/IEC 27002, aplicando-se assim métodos de avaliação e controlo reconhecidos e amplamente aceites. Deste modo, será estabelecida uma relação entre as melhores práticas de avaliação dos controlos de

SI/TI e os principais componentes da arquitectura do Data Warehouse, seus subsistemas, funções e objectivos de controlo.
Após a conclusão da construção do modelo, este será testado num estudo de caso **(Passo 7),** que incluirá uma acção de auditoria ao DW de uma Instituição Financeira, bem como um conjunto de entrevistas aos responsáveis pela gestão do DW e aos responsáveis pela área de auditoria a sistemas de informação dessa mesma Instituição Financeira.

Por fim, devido às características cíclicas do método de investigação, as conclusões, criticas e sugestões de melhoria poderão ser reutilizadas como elementos de input para uma nova iteração da metodologia de investigação. Esta característica evolutiva não retira valor ao modelo apresentado, pelo contrário, esta metodologia acrescenta versatilidade a futuras revisões do modelo, facilitando a realização de novos ciclos de investigação, desenvolvimento e validação das novas versões.
Algo semelhante se passa com os métodos de investigação do CobiT® 4.1 e do ITIL® V3, também eles circulares e que actualmente já se encontram respectivamente na versão 4.1 e 3.0.

1.2.3 – Estrutura da Dissertação

Com vista a sistematizar o processo de governação de um Data Warehouse e definir o modelo que permitirá avaliar a eficácia do controlo interno, esta dissertação divide-se em três grandes partes: O Estado da Arte; O Modelo; O Estudo de Caso.

a) O Estado da Arte que define as áreas de conhecimento que envolvem o tema da investigação e identifica as principais componentes de análise, nomeadamente:

- Os fundamentos e conceitos associados a uma arquitectura de Data Warehouse: O que é um Data Warehouse, para que serve, quais as principais componentes, quais os passos para assegurar a sua operacionalidade, que requisitos possui um sistema desta natureza, quais as fases do desenvolvimento de projectos de DW, entre outros;
- O Controlo Interno das organizações e os componentes ou meios fundamentais, como a gestão de riscos, a auditoria interna e a monitorização, o sistema de informação de gestão das organizações, bem como outras partes constituintes do processo de DW;
- Os pressupostos gerais para assegurar a boa governação das Tecnologias de Informação (TI) de uma organização, bem como os Standards e metodologias mais amplamente reconhecidos em matéria de avaliação do controlo interno das TI, casos do CobiT® 4.1, ITIL® V3 e ISO/IEC 27002[2].

b) Construção de um modelo que permita avaliar e optimizar o sistema de controlo interno de uma arquitectura de DW.
Partindo de uma metodologia de controlo interno alinhada com os principais standards de avaliação e controlo de tecnologias de informação, como sejam o CobiT® 4.1, o ITIL® V3 e o ISO/IEC 27002, o modelo proposto visa sistematizar um método de avaliação dos principais riscos e objectivos de controlo para cada uma das componentes da arquitectura DW, resultando desse mapeamento um modelo que permitirá optimizar o sistema de controlo interno e a gestão daquela ferramenta de suporte à decisão.
O propósito central deste capítulo é o de apresentar um instrumento de notação – template – que possa ser utilizado por todos os gestores do DW, possibilitando deste modo avaliar e identificar oportunidades de melhoria no sistema de controlo interno daquela ferramenta e deste modo assegurar:

[2] Cobit (Control Objectives for Information and Related Technologies); ITIL (Information Technology Infrastructure Library); ISO (International Organization for Standardization) ver ponto 2.3.1

- Um modelo de governação das TI em geral e do processo BI em particular
- Que os objectivos de negócio suportados no DW estão a ser plenamente atingidos;
- Que os riscos associados ao DW estão devidamente identificados e que existe um plano actualizado da severidade e formas de mitigação de todos os riscos associados às várias componentes do DW
- Que existe um conjunto sistematizado de controlos, quantificáveis e de implementação exequível, quer quanto à sua eficácia na avaliação do risco, quer quanto ao acompanhamento de avaliações efectuadas anteriormente
- Que o sistema de controlo interno é facilmente auditável

c) Por fim, com o objectivo de avaliar a aplicabilidade do modelo proposto, será apresentado um estudo de caso que descreverá uma auditoria a um ambiente de Data Warehouse real, a realizar numa instituição financeira, onde os pressupostos do modelo serão considerados, bem como uma entrevista aos responsáveis do DW estudado sobre a pertinência do modelo para a melhoria do controlo interno.

2 – O ESTADO DA ARTE

No presente capítulo procuraremos identificar e sistematizar todas as componentes do DW, quer da fase de desenvolvimento, quer da fase de produção, as suas dimensões e perspectivas, de forma a permitir efectuar uma análise da performance e identificar os principais riscos e os objectivos de controlo.

2.1 – O Objecto DW

Este ponto aborda os conceitos e os aspectos fundamentais de um sistema de data warehouse, nomeadamente, o enquadramento no processo BI de suporte à decisão da organização, as origens desta arquitectura, os principais autores, o tipo de requisitos que visa satisfazer e os passos que compõem o processo de importação, transformação e carregamento de dados oriundos dos sistemas de informação operacional da organização.

2.1.1 – O Business Intelligence (BI)

Embora não faça parte do âmbito desta investigação analisar detalhadamente o conceito de Business Intelligence (BI), considera-se importante definir do conceito porque nele se enquadra a arquitectura do Data Warehouse.
Num artigo de 1958, o investigador Hans Peter Luhn da IBM utilizou o termo Business Intelligence. Definiu o termo do seguinte modo: *"the ability to apprehend the interrelationships of presented facts in such a way as to guide action towards a desired goal."* (Luhn, 1958)
O BI refere-se habitualmente ao processo de recolha de informação, ou seja, ao conjunto de tecnologias que permitem obter visualizações históricas, correntes ou previsões das operações de negócio.
As tecnologias de suporte à decisão mais utilizadas são o reporting, as consultas OLAP, data mining, benchmarks, text mining e análise preditiva, podendo todas elas ser suportadas por uma arquitectura de Data Warehouse (DW).

2.1.2 – O Data Warehouse

a) Dados históricos

"Em 1977, Jimmy Carter era o presidente dos Estados Unidos, o filme do momento era o Star Wars e a Apple Computer introduziu no mercado o primeiro computador pessoal. Quatro anos mais tarde era Ronald Reagan o presidente, o Príncipe Carlos e Lady Diana casavam-se e a IBM começava a comercializar o seu IBM PC.
Desde essa altura os computadores começaram a evoluir das arquitecturas de mainframe para o desktop, começando pouco depois a jornada das folhas de cálculo e dos processadores de texto, substituindo as calculadoras e as máquinas de escrever.
Em 1985 Mikhail Gorbachev era o líder da União Soviética e a Coca-cola estava no auge e os dados informáticos começaram a espalhar-se. Mesmo nos mainframes, os dados encontravam a sua própria casa. Supervisores, gestores e executivos já não conseguiam olhar para um único quadro e perceber como estava a correr o negócio. Os dados entrincheiravam-se em aplicações, nichos e saberes que nunca mais veriam a luz do dia. Este foi talvez o factor mais determinante para a emergência dos Sistemas de Suporte à Decisão nas organizações." (Silvers, 2008)

Nos anos noventa, Ralph Kimball e Bill Inmon criaram e documentaram os conceitos e princípios dos sistemas de Data Warehouse que constituem, hoje em dia, os pressupostos fundamentais de todos os DW. O conjunto de razões e intenções apresentados por estes dois autores é conhecido por filosofia dos DW.

Abaixo descrevem-se as características fundamentais do DW (Inmon, 2001):

- **Orientado por assuntos:** Um DW armazena os dados importantes sobre temas específicos da organização e conforme o interesse dos seus utilizadores;
- **Integrado:** Um DW integra dados provenientes de fontes distintas atribuindo-lhe uma representação única e universal;
- **Temporal:** Os dados de um DW são dependentes do tempo e deste modo representam as alterações ocorridas numa base de dados operacional;
- **Volatilidade:** Os dados inseridos no DW não são passíveis de serem alterados ou excluídos. Sempre que existirem actualizações, um novo item é adicionado ao DW.

b) Definições de Data Warehouse

"Se colocarmos 100 consultores experientes em Data Warehousing numa sala e lhes pedirmos que definam Data Warehouse em 20 palavras, pelo menos 95 deles, com enfoque na tecnologia, irão referir aspectos como: Orientado por assunto, com variação temporal e apenas de leitura. Os restantes 5 consultores referirão aspectos mais relacionados com o negócio como por exemplo: - Melhorar a capacidade de tomar decisões, melhoria do acesso a informação, etc." (Hammergren & Simon, 2009)

O processo de construção, consulta e manutenção de um Data Warehouse (DW) tem como objectivo integrar e gerir dados extraídos de diversas fontes, com o propósito de obter uma visão integrada e orientada ao negócio de uma parte ou de toda a organização.
Um DW é uma ferramenta cuja função é proporcionar aos seus utilizadores uma fonte única de informação, respeitante a diferentes vertentes ou negócios da organização, sendo neste sentido uma componente importante de apoio ao processo de extracção do conhecimento e tomada de decisões. Um DW tem igualmente um papel importante como unidade de armazenamento de dados de uma organização, considerando-se neste caso, um grande repositório de dados obtidos de várias fontes e com diferenças fundamentais relativamente a bases de dados convencionais.

"A missão de um DW é a de publicar os activos de informação da organização para, da forma mais eficaz, suportar o processo de tomada de decisão" (Kimball & Caserta, 2004).

c) Avaliação de custos e benefícios do Data Warehouse

O Data Warehousing é uma importante área de prática e de investigação da organização, no entanto existem poucos estudos que avaliem o impacto dessas práticas, em geral, e os factores críticos de sucesso, em particular.

"Os custos do DW são relativamente fáceis de estimar. Tal como a maioria dos projectos de TI, eles têm componentes de Hardware, Software e custos de pessoal." (Watson et al, 2004)

A tabela seguinte mostra uma lista com categorias e custos típicos do DW (Watson et al, 2004):

Hardware	Software	Pessoal
• Unidades de arquivo • Processadores • Dispositivos de Rede	• Software ETL • Software de gestão de bases de dados • Software de metadados • Ferramentas de utilização e visualização de dados	• Pessoal de TI (Exemplos: Gestores de bases de dados, modeladores de dados, técnicos de ETL, etc) • Pessoal de negócio e utilizadores • Consultores

Existem vários benefícios possíveis resultantes do DW, tais como os referidos na tabela seguinte (Watson et al, 2004):

Consolidação de Data Mart	**Poupança de tempo**	**Mais e melhor informação**	**Poupança de pessoal**	**Optimização da tomada de decisão**	**Melhorias nos processos de negócio**	**Suporte para objectivos estratégicos de negócio**
• Redução de múltiplas plataformas de decisão • Poupanças em custos de hardware e software • Eficiência operacional	• Poupanças em pessoal de TI na extracção de dados para os utilizadores • Menos tempo gasto pelo pessoal TI para escrever 'queries' • Menos tempo gasto a encontrar dados • Menos tempo gasto pelos analistas a responder a pedidos de informação	• Possuir informação inexistente antes do DW • Possibilidades dos utilizadores analisarem dados de novas maneiras • Possibilidades para visualizar e pensar o negócio em novas maneiras	• Disposição mais eficiente do pessoal de TI • Crescimento organizacional mais rápido e sem aumentos de pessoal • Reposicionamento do pessoal operacional de acordo com as actividades produtivas de valor mais elevado	• Decisões baseadas em factos em vez de intuições dos gestores • Tomada de decisão mais rápida • Possibilidade de analisar mais e melhores alternativas • Possibilidade de identificar e agir melhor perante os problemas	• Redesenho das tarefas • Poupanças na pesquisa e contratação de produtos e serviços • Ciclos de negócio mais curtos • Possibilidade de identificar e corrigir problemas em processos de negócio	• Resposta mais rápida a alterações nas condições do mercado • Aumento da fatia de mercado • Melhorias na colocação de novos produtos no mercado

Neste âmbito, Hwang & Xu (2008) definiram um modelo com o objectivo de melhor compreender os factores críticos de sucesso e os seus efeitos para o sucesso de toda a arquitectura DW na organização.
Assim, o quadro seguinte resume as variáveis e as métricas que, segundo os autores, permitem avaliar o nível de sucesso dos Data Warehouses nas organizações.

Variável	**Métrica 1**	**Métrica 2**	**Métrica 3**	**Métrica 4**
Factor Operacional	Nível de definição das necessidades de negócio e benefícios	Nível de suporte da gestão executiva	Nível de participação e envolvimento	
Factor Técnico	Nível de qualidade dos dados fonte	Nível da tecnologia de desenvolvimento	Nível de conhecimento do staff de sistemas de informação e consultoria	Nível da gestão do projecto
Factor Temporal	Grau de cumprimento da calendarização da implementação	Nível de planeamento e grau de detalhe do âmbito do projecto		
Factor Económico	Adequação orçamental do projecto	Grau de definição dos benefícios de negócio		
Qualidade do Sistema	Facilidade de utilização	Velocidade de resposta a pesquisa de informação		
Qualidade de Informação	Nível de qualidade da informação	Nível de produtividade		
Benefícios Individuais	Nível de produtividade			
Benefícios Organizacionais	Nível de melhorias nos processos de negócio	Nível de melhoria no posicionamento competitivo		

Tabela 1 – Variáveis e métricas de avaliação do sucesso do DW (Hwang & Xu, 2008)

d) Modelação Dimensional

"A modelação dimensional é uma técnica aplicada a bases de dados destinadas a suportar consultas do utilizador orientadas para a compreensão dos dados" (Kimball & Caserta, 2004)

A modelação dimensional é uma técnica de desenho lógico vocacionada para a visualização dos dados, de forma intuitiva e com altos índices de performance na extracção dos mesmos (elevado desempenho analítico). Proporciona uma representação consistente da base de dados com a forma como o utilizador visualiza e navega pelo Data Warehouse (DW), combinando tabelas de dados históricos em segmentos temporais, cujo significado é descrito através de tabelas de dimensões.
A modelação dimensional tem sido amplamente aceite como a técnica dominante para a apresentação de um Data Warehouse. A sua simplicidade é a chave fundamental que possibilita aos utilizadores entenderem facilmente os dados apresentados, bem como a navegação pelas aplicações associadas. A modelação dimensional permita a utilização de dimensões e factos conformes, o que proporciona um modelo de pesquisa prático e intuitivo para o tratamento de dados complexos.
Os modelos dimensionais são construídos com base em processos de medição. Uma medição corresponde a uma observação do mundo real traduzido num valor anteriormente desconhecido. Repetindo a mesma medição ao longo do tempo cria-se uma série temporal.

O valor da medição reflecte-se na tabela de factos de um modelo dimensional. Associada a uma medição existe um determinado contexto que se repete com ela. De modo a evitar repetições no DW normalizam-se as variáveis contextuais em dimensões. Deste modo, existem tantas dimensões quanto os tipos de atributos contextuais de uma medição. Resumindo:

- **Facto:** Um facto pode ser definido como uma realidade, uma verdade, um acontecimento, uma ocorrência. É registado na tabela de factos;
- **Dimensão:** Uma dimensão pode ser definida como uma categoria de informação. Para cada dimensão existe uma tabela específica (Exemplo: Clientes, Fornecedores, Tempo, etc);
- **Atributo:** Um nível único com uma dimensão. Por exemplo, mês é um atributo da dimensão tempo;
- **Hierarquia:** É a especificação de níveis que representa as relações entre diferente atributos e as dimensões. Um exemplo disso é uma possível hierarquia que pode ser na dimensão tempo, ou seja: ANO; SEMESTRE; TRIMESTRE; MÊS; DIA.

2.1.3 – Ambiente de Produção DW

a) Tipos de Arquitecturas DW

De um modo geral, a arquitectura do Data Warehouse passa por um processo de extracção de informação especializada, partindo de bases de dados operacionais, proporcionando ao utilizador uma visualização multidimensional dos dados de negócio, o que facilita e potencia as possibilidades de análise.
Existem, no entanto, algumas particularidades e variantes que distinguem estas arquitecturas entre si.

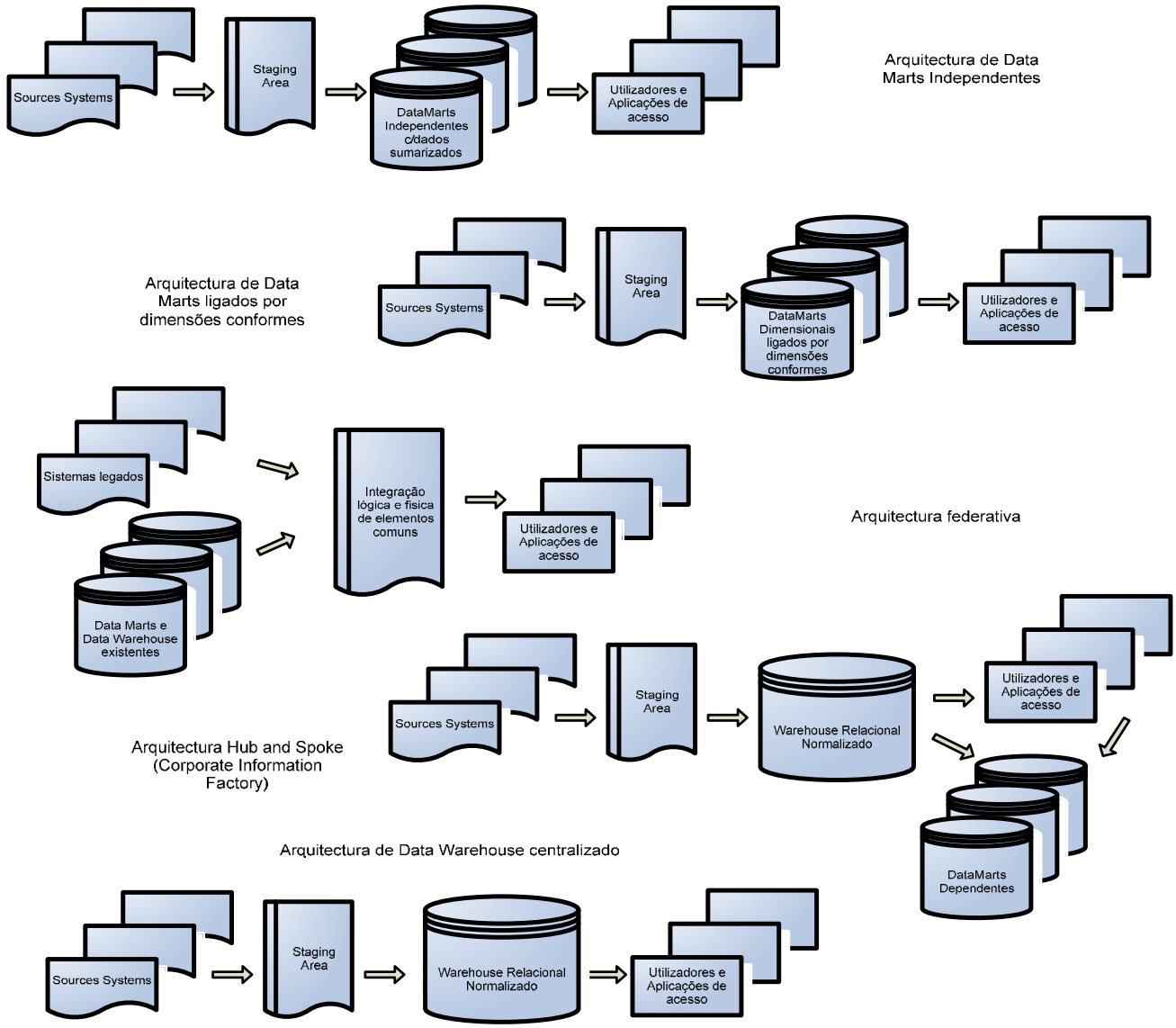

Ilustração 2 – Tipos de arquitecturas de Data Warehouse (Ariyachandra & Watson, 2008)

Um estudo efectuado em 2006 por Ariyachandra & Watson, que abrangeu cerca de 450 Data Warehouses, tipificou as arquitecturas identificadas em cinco grupos, conforme se mostra na figura seguinte.
Deste modo, em geral o fluxo de dados inicia-se com a sua extracção em bases de dados transaccionais, passando os dados por um processo de transformação e limpeza, conhecido por integração de dados ou ETL – Extract, Transform and Load. Após este primeiro processo, dependendo da arquitectura, os dados podem ser transferidos da área de trabalho (Staging Área) para os Data Marts ou outras estruturas de dados preparadas para a consulta e análise.

b) Área de Aquisição de dados ou Back Room

No Back Room tem lugar a preparação dos dados (Data Management) que envolve a aquisição e transformação. Não podem ser efectuadas consultas no Back Room, sendo o acesso aos dados restrito aos técnicos especializados em integração de dados.
O processo de 'Staging' tratado no Back Room é composto por quatro passos:

- **Extracção:** Dos dados oriundos de bases de dados operacionais (IMS) ou conjunto de dados (XML) sendo colocados na Staging Área em ficheiros de texto ou tabelas relacionais;

- **Limpeza:** Ajusta a qualidade dos dados aos requisitos do DW, envolvendo passos como a validação dos dados, remoção de duplicações, verificando as regras de negócio;
- **Conformidade:** Sempre que existem mais do que uma fonte operacional de dados, estes devem fundir-se no DW de acordo com regras bem definidas, por uma entidade próxima da gestão executiva, considerando a estandardização vigente sobre domínios e métricas;
- **Entrega:** O objectivo de todo o Back Room é o de providenciar dados prontos para consulta. Trata-se de um passo importantíssimo que consiste em estruturar os dados em esquemas dimensionais apropriados. Os esquemas são a base para as consultas OLAP – Online Analitical Process.

A missão da equipa de integração de dados é a de construir o Back room do Data Warehouse (Kimball & Caserta, 2004), ou seja:

- Entregar os dados adequados para os utilizadores;
- Adicionar valor nos processos de limpeza e conformidade;
- Proteger e documentar os dados.

c) Área de acessos ou Front Room

O principal propósito do Front Room é o de disponibilizar os dados no seu formato dimensional e orientado a objectos de negócio, de forma que possa ser facilmente acedido pelos utilizadores, directamente ou através de ferramentas de consulta especializadas.
Os Data Marts são componentes importantes do Front Room, sendo constituídos por um conjunto de tabelas dimensionais que dão suporte a um tema do negócio. Os Data Marts acrescentam desempenho às consultas específicas, pois os dados estão ordenados de forma menos rígida (menor numero de junções de tabelas) o que acrescenta eficiência às consultas.
Uma das principais características dos Data Marts reside na arquitectura associada aos dados. Os Data Marts são também designados por sistemas dimensionais ou OLAP (Online Analitical Process), cujo principal objectivo é o de possibilitar uma visão conceptual multidimensional dos dados armazenados. Esta arquitectura multidimensional permite obter uma maior performance na pesquisa dos dados bem como uma maior utilidade para os analistas, do que a arquitectura tabular tradicional utilizada nos sistemas de processamento transaccional.

"Online Analytical Processing (OLAP) é uma aproximação para responder tempestivamente a consultas multidimensionais" (Marakas & O'Brien, 2008)

"A fim de permitir uma visualização e manipulação multidimensional dos dados, as ferramentas OLAP oferecem diferentes funções" (Inmon, 2001):

- **Pivot:** Muda a orientação dimensional de uma pesquisa. Pode consistir numa troca de linhas e colunas ou mover uma das dimensões da coluna para a linha;
- **Roll-Up:** As bases de dados multidimensionais têm geralmente hierarquias e relações de dados baseadas em fórmulas dentro de cada dimensão. O Roll-Up (rodar o cubo) constitui-se na computação de todas essas relações de forma a poderem ser visualizadas de acordo com o planeado.
- **Drill Down / Up:** Consiste em efectuar uma exploração em diferentes níveis de detalhe das informações, como por exemplo, analisar uma informação por continente, país ou cidade, partindo da mesma Base de dados

Para além dos modelos dimensionais que permitem uma pesquisa orientada a objectos de negócio, existem outras áreas ou clientes do DW que pesquisam os dados de uma forma menos direccionada ou estruturada. Essa forma de pesquisa é conhecida por DataMining.

"O DataMining é o processo de explorar e analisar, através de meios automáticos ou semi-automáticos, grandes quantidades de dados, tendo em vista a descoberta de padrões e regras que façam sentido no contexto da análise que se pretende efectuar" (Berry & Linoff, 1997)

O processo de Data Mining procura pesquisar padrões com interesse para a obtenção de vantagens e apuramento do conhecimento específico, nomeadamente sobre redução de custos e dos recursos humanos envolvidos. Este tipo de processo exige normalmente uma estrutura de ficheiros completamente desnormalizada.

d) Os Metadados

Metadata significa *'Dados sobre os dados'*, de qualquer origem e meio. Um item dos metadados pode descrever um dado individual ou um conjunto de dados, incluindo itens de vários conteúdos e níveis hierárquicos.

"Para além dos dados propriamente ditos, é muito importante manter um repositório com informação sobre eles. Os metadados são normalmente definidos como dados sobre os dados ou uma abstracção dos dados, ou até, dados de mais alto nível, pois descrevem os dados de níveis inferiores, bem como todas as regras que lhe estão associados." (Sherman, 1997).

Outra classificação (Kimball & Caserta, 2004) refere-se ao teor da informação fornecida pelos metadados. Assim temos:

- Metadados de negócio – Descrevem os dados no sentido do negócio
- Metadados Técnicos – Representam os aspectos técnicos dos dados, os atributos, tipos, dimensões, etc
- Metadados de execução de processos – Apresentam informação estatística sobre os resultados dos processos de ETL, número de linhas carregadas, tempo, linhas rejeitadas, etc

A disponibilização dos metadados traz vantagens para a organização, como por exemplo:

- Asseguram a individualidade do DW face a alterações ocorridas nos sistemas operacionais
- Contribuem para a visão única e centralizada do DW
- Servem de núcleo para registar todas as transformações que afectem a informação

2.1.4 – Os Requisitos

O desenho do DW e do processo ETL deve ser iniciado pela definição dos requisitos, realidades e constrangimentos que afectam o sistema. Os requisitos são aspectos da organização com os quais o sistema tem de existir e adaptar-se. O levantamento de requisitos é uma tarefa importantíssima para o desenvolvimento do DW (Kimball and Caserta, 2004).
Muitos dos requisitos aqui abordados devem também constituir requisitos de todos os sistemas de informação da organização. Assim, os requisitos de segurança, de qualidade dos dados, de acessos e até os próprios metadados são exemplos de componentes transversais a todos os sistemas de informação da organização e portanto deverão ser alvo de políticas comuns devidamente integradas.

a) Negócio

A definição dos requisitos de negócio é provavelmente um dos aspectos mais importantes para o sucesso do DW na organização. Os requisitos de informação associados ao negócio em geral ou á parte que cada um dos utilizadores do Data Warehouse controlo ou gere, visam satisfazer as respectivas necessidades de suporte às decisões que é necessário tomar.

"Acima de tudo é preciso compreender como o negócio executa a sua cadeia de valor, desde a despesa até ao retorno/lucro. Deste modo é possível determinar onde os activos de informação são gerados e onde são consumidos." (Hammergreen & Simon, 2009)

O processo de definição dos requisitos de negócio traduz-se acima de tudo na identificação dos dados fonte que a equipa de ETL deve introduzir no Data Warehouse, bem como a periodicidade das extracções e o nível de detalhe dos mesmos. Deste modo, verifica-se que a avaliação e definição adequada dos requisitos de negócio é uma actividade nuclear da equipa ETL.
O apuramento dos requisitos faz-se através de um conjunto de entrevistas aos utilizadores com questões como:

- Qual a informação necessária para exercer a sua função?
- De quem recebe a informação? De que forma e qual a periodicidade?
- Que informação fornece a terceiros?
- Para quem a envia? De que forma e qual a periodicidade?

Após percebida a informação que é requerida pelo negócio é necessário avaliar e perceber qual é o seu valor e custo. Este processo de avaliação da informação efectua-se através da realização de vários eventos (Hammergreen & Simon, 2009):

- Entrevistas aos utilizadores com o fim de avaliar a importância, a facilidade de acesso, as dificuldades, a qualidade e o impacto da informação no negócio
- Matrizes BCG de avaliação da dificuldade em obter e com impacto da informação no negócio
- Classificação de objectos chave para o negócio
- Construção de modelos de dados de negócio com definição das relações entre os objectos de negócio e as métricas para a sua documentação
- Realização de protótipos e interacção com utilizadores

b) Conformidade

Todas as organizações estão obrigadas a cumprir e respeitar um conjunto de regulamentos e normas. A conformidade com as normas é outra das preocupações da equipa de desenvolvimento do DW. Por exemplo, deve-se assegurar que todos os elementos de prova dos resultados apresentados pelo DW são preservados, garantindo os necessários elementos de prova em caso de necessidade. Nomeadamente no caso dos relatórios financeiros, são mais evidentes os requisitos de conformidade que normalmente obrigam a operações do género:

- Cópias das fontes de dados e processos de staging;
- Prova dos fluxos transaccionais que transformaram os dados;
- Algoritmos documentados.

c) Data Profiling

O Data Profiling aplica-se aos sistemas operacionais que irão ser alvo de recolha de dados para o DW.

"Trata-se de aplicar metodologias de análise a um conjunto de dados com o propósito de compreender se os seus conteúdos, estrutura e qualidade são os adequados para satisfazer os requisitos de negócio. Um bom sistema de Data Profiling pode percorrer grandes quantidades de dados e, com o auxílio de um bom analista, permite identificar fragilidades nos dados fonte bem como optimizar o processo de extracção para o DW" (Olson, 2003).

Esta perspectiva é muito relevante para a equipa de ETL poder analisar os dados das fontes de forma sistemática quanto à qualidade, âmbito e contexto, e deste modo poder planear o sistema ETL a construir.

d) Segurança

Apesar das melhorias que os sistemas têm vindo a incorporar em matéria de segurança, este tema continua a ser uma das preocupações importantes a considerar por uma equipa de Data Warehouse, em particular, e por toda a gestão de tecnologias de informação na organização em geral.
O processo de Data Warehouse destina-se a publicar dados para que os gestores possam tomar decisões fundamentadas e com conhecimento efectivo do negócio da organização, em geral, e da respectiva área em particular. Porém, no interesse da segurança, o acesso aos dados do DW deve ser restringidos apenas aos utilizadores que têm necessidade de conhecer a informação.
Segundo os autores Raymond & LeClerc (2005), a segurança e a privacidade da informação do DW deve ser considerada como uma preocupação primária e critica. Assim, as organizações devem estabelecer um conjunto de procedimentos que, apesar de flexíveis, cumpram com os vários requisitos de privacidade.
Deste modo, os processos de segurança devem estar focados em quatro áreas (Raymond & LeClerc, 2005):

- Estabelecimento de politicas e procedimentos efectivos
- Implementar procedimentos de segurança lógica, como por exemplo: Autenticação de utilizadores, Controlos de acessos e tecnologias de encriptação de dados
- Limitar o acesso físico aos centros de dados
- Estabelecer um processo de revisão do controlo interno com ênfase especial na segurança e privacidade

Numa perspectiva mais operacional, os procedimentos de protecção da informação residentes nos sistemas de informação devem considerar os seguintes passos:

- Implementação de esquemas de classificação dos dados
- Controlos de identificação, autenticação e restrição dos utilizadores
- Desenho dos perímetros de segurança, 'firewalls' e detecção de intrusões
- Sistemas de encriptação de dados
- Ataques com software malicioso, vírus, troianos, etc
- Testes de segurança, ferramentas de monitorização e avaliação
- Métodos de protecção e segurança física
- Armazenamento, recuperação, transporte e apresentação de informação confidencial
- Controlos e riscos de utilização de dispositivos portáteis

e) Integração de Dados

O tema da integração dos dados é de importância capital para toda as TI da organização e, especialmente, para o Data Warehouse. A preocupação em implementar uma política de integração dos dados deve iniciar-se pelo nível dos sistemas transaccionais que tratam as operações da organização. No entanto, nem sempre isto acontece, pelo menos em organizações que nunca implementaram um sistema ERP – Enterprise Resourse Planing[3]. De qualquer modo, mesmo em organizações com ERP, a integração dos dados pode não estar completa, pois outros sistemas poderão coexistir fora do ERP e, portanto, sem regras definidas centralmente para aplicar aos seus dados.

[3] ERP são sistemas de informação que integram todos os dados e processos de uma organização num único sistema de informação (Laudon, 2004).

No Data Warehouse, a integração dos dados processa-se através das dimensões e factos conformes, o que significa acordar entre os gestores de todas as bases de dados sobre quais as métricas de performance e respectivas formulações matemáticas.

f) Qualidade dos Dados

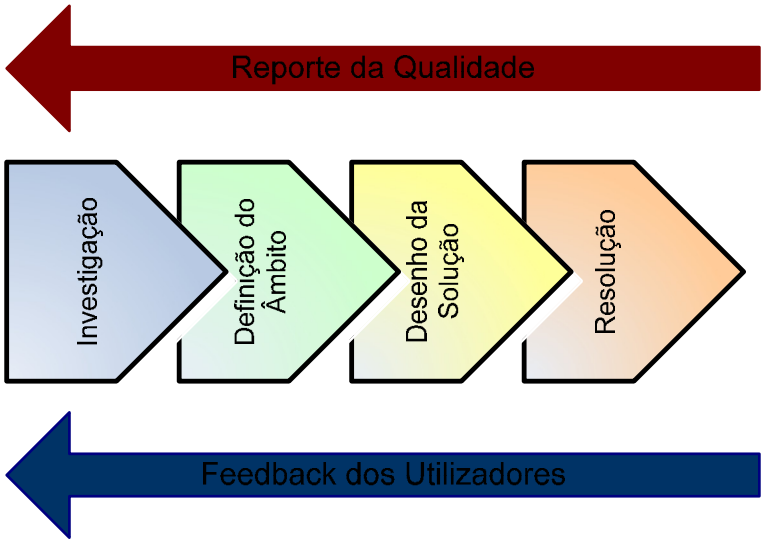

Ilustração 3 – Metodologia de Qualidade dos Dados

Outro dos processos que interessam transversalmente a todas as TI mas em especial ao DW é o processo da qualidade dos dados. Monitorizar a exactidão, abrangência e confiança dos dados de um Data Warehouse, deve ser um esforço contínuo. Apenas os ingénuos assumem que o negócio e o DW vivem num mundo perfeito onde nada de errado acontece. Monitorizar com diligência os dados antes de entrarem no DW, sendo o objectivo entregar os dados e a informação que pode derivar o negócio, com confiança. Uma definição simples de qualidade dos dados é:

"O nível no qual os dados são percebidos como verdadeiros e precisos" (Dijcks, 2004)

O âmbito da qualidade de dados inclui todos os elementos que intervêm na entrega de informação aos utilizadores finais, incluindo os dados factuais e os metadados.
O tema da qualidade evidencia-se no contexto do DW pois trata-se de uma área em que os problemas de qualidade dos dados produzem um impacto maior. De salientar que os problemas de qualidade de dados não são causados pelo DW, apenas são evidenciados por esta ferramenta.
Jean Pierre Djicks, em artigo publicado no Business Intelligence Journal em 2004, propõe uma metodologia para ajudar a assegurar a qualidade dos dados no DW. A metodologia é composta por quatro fases de análise mais duas correntes de informação iterativa (ver figura seguinte).

- **Investigação**

Inicia-se com o projecto do próprio DW pois é muito importante definir correctamente os princípios de qualidade expectáveis. Caso não tenha sido efectuada previamente ao projecto, a investigação da qualidade deve ser incluída no plano de projecto do DW para assegurar uma avaliação da qualidade dos dados antes de se iniciar o desenho. Inclui:

  - Investigação da importância dos metadados
  - Investigação do impacto tecnológico do processo de qualidade dos dados
  - Investigação dos sistemas-fonte
  - Investigação dos utilizadores-chave dos sistemas fonte
  - Investigar as políticas, regulamentos e standards sobre qualidade de dados

- **Definição do âmbito**

Depois de avaliada a organização e a qualidade dos dados, é necessário definir o âmbito do projecto de qualidade dos dados dentro do projecto de DW.

- Definir a base para a qualidade de dados – com o nível de qualidade actual e os objectivos que se pretendem atingir
- Definir o trabalho necessário
- Definir a ferramenta de apoio

- **Desenho da solução**
  - Desenhar e integrar no ETL o processo de qualidade de dados, especialmente no 'Transform'
  - Integrar com a ferramenta de apoio
  - Avaliar a performance e a escalabilidade do novo processo

- **Resolução**
  - Estabelecer os pontos de controlo do projecto
  - Apresentar os resultados aos utilizadores
  - Identificar problemas com a qualidade de dados
  - Realizar testes de processamento e carga

g) Latência, Arquivo e Recuperação

A latência significa a periodicidade e frequência com que os dados devem ser entregues aos utilizadores. Esta política, bem como as políticas de backup e registos da origem dos dados, têm um grande impacto na definição da arquitectura e na implementação de um DW.
O arquivo é o local onde se guardam registos, documentos ou outros materiais de interesse histórico. Para a informática o arquivo é o local físico ou lógico, onde se guardam as cópias de ficheiros sem utilização activa ou com o fim de repor os dados dos sistemas em caso de falha naquele repositório.
A recuperação é o processo correctivo para repor a base de dados num estado utilizável após a ocorrência de uma erro. O processo de recuperação consiste nos seguintes passos (Senft & Gallegos, 2009):

- Identificação do estado de erro ou dano da base de dados
- Suspender o normal processamento
- Determinar a origem e extensão do dano
- Tomar medidas correctivas como:
  - Repor os recursos do sistema num estado utilizável
  - Corrigir o erro e remover os dados inválidos
  - Reiniciar ou continuar os processos interrompidos

h) Responsabilidades e funções TI

As especializações mais comuns na gestão operacional das TI são as seguintes (DeLuccia, 2008):

- **Director de TI –** Tem a responsabilidade de lidar com os gestores de TI e SI, bem como de executar o plano executivo;
- **Gestores de TI –** Estão encarregados de gerir o staff técnico em matérias como o desenvolvimento de software, no Help Desk, Gestão de servidores, administração da rede e ou da segurança de informação;
- **Arquitecto de sistemas –** Revê os dados compilados pelos analistas de sistemas e determinada qual o desenho mais adequado para os novos sistemas;
- **Gestor de segurança da informação –** Especifica os standards a implementar para a segurança dos sistemas informáticos e revê os procedimentos de conformidade com as

politicas de segurança. Procede a testes e especifica os controlos a implementar pelos administradores de servidores e rede;

- **Gestor da mudança –** Pode ser exercido por uma pessoa ou um comité de gestores. Assegura-se que o pessoal técnico está a seguir os procedimentos correctos, bem como a considerar os controlos e os planos acordados;
- **Programadores –** Escrevem os programas que resolvem os problemas dos utilizadores;
- **Administrador da rede –** Trata-se do responsável técnico pela comunicação de dados entre as tecnologias ligadas à rede;
- **Administrador de servidor –** Responsável pela manutenção do hardware e software do servidor;
- **Administrador de bases de dados –** Detém a custódia dos dados bem como a manutenção dos sistemas de base de dados;
- **Operador de computadores –** Assistem os administradores de sistemas e os gestores de bases de dados;
- **Analista de sistemas –** Trabalha com os utilizadores do negócio estabelecendo os requisitos. Após definir os requisitos, trabalha os layouts dos screens e dos relatórios a produzir pelos sistemas;
- **Help Desk –** Todo o sistema de informação deve ter um help-desk que dê suporte ao hardware e software, sendo o primeiro ponto de contacto entre os utilizadores dos sistemas e o pessoal técnico.

Para além dos referidos acima, especificamente no DW e no BI de suporte à decisão, os principais papéis são os seguintes:

- **Analista BI –** É o responsável por desenvolver os planos de capacidade do hardware, middleware, base de dados e redes de dados com o fim de assegurar a necessária escalabilidade de um ambiente BI de suporte à decisão.
- **Analista de qualidade dos dados –** Assume a responsabilidade de encontrar e analisar deficiências na qualidade dos dados dos sistemas fonte. Uma vez que é impossível limpar todos os dados, devem ser estabelecidos processos de triagem e procedimentos de prioritização.
- **Administrador de metadados –** É responsável pelo repositório de metadados. Deve criar, manter e popular o repositório. Durante o projecto BI, o administrador de dados irá providenciar os metadados sobre o negócio enquanto que o administrador de bases de dados e o analista de qualidade irão providenciar metadados técnicos. Os metadados integrados devem ser guardados em repositório próprio e tornados acessíveis às comunidades de IT e de negócio.

i) Controlos de Utilizadores e Acessos

No âmbito do controlo de utilização, não só todos os acessos aos recursos computacionais devem ser controlados, como também se torna imperativa a aplicação da regra do privilégio mínimo, ou seja, nenhum utilizador individual deve possuir um nível de autoridade nos acessos maior do que aquele que a sua função exige.
Os principais tipos de acessos são o ‘User Login’; o ‘Previledged Administrator Login’ e o ‘Maintenance Login’;
Para assegurar que o acesso não autorizado é efectivamente impossível, as três formas de aceder aos dados devem ser asseguradas, ou seja, pela via do controlo de perímetro, por acesso directo aos dados ou através de Middleware. De forma a verificar que os acessos estão devidamente controlados, existem quatro tipos de controlos de protecção de dados:

1 – Controlos de conteúdo dos ficheiros de dados ou das bases de dados que passam por procedimentos de arquivamento de dados;
2 – Controlo à alteração da configuração das aplicações, que podem alterar a performance, a leitura e segurança dos ficheiros de dados acedidos por estas;
3 – Controlos de acesso lógico que deve ser forçado através da autenticação num programa de acessos de controlo;
4 – Controlo de processamento de transacções, que, sempre que envolvam ficheiros de dados, devem passar por um processo de autenticação e validação.

Os controlos de acessos visam assegurar a segurança e integridade dos acessos. Cada aplicação deve ter pelo menos três controlos de processamento internos: o controlo de inputs, que assegura que apenas a informação valida e autorizada entra nas transacções, o controlo de processamento, que assegura que os dados e as transacções são validas, e o controlo de outputs, que garantem a confidencialidade dos outputs de um sistema até que estes sejam entregues a um utilizador especifico;

j) Infra-estruturas tecnológica

Todo o levantamento de requisitos a Tecnologias de Informação, incluindo o DW, deve incluir uma avaliação das infra-estruturas tecnológicas.
Abaixo se mencionam os principais tópicos de uma infra-estrutura tecnológica que podem ser alvo de uma avaliação de controlos (Cannon et al, 2006):

- Perceber as diferenças entre as arquitecturas de computadores
- Comparar sistemas de processadores
  - Identificar os sistemas operativos
  - Comparar capacidades dos computadores
  - Perceber o processamento e o sistema de controlo
  - Lidar com o armazenamento de dados
  - Perceber os portos de acesso e de controlo
- Perceber o desenho físico da rede
- Identificar as topologias
- Os tipos de cabos
- Os dispositivos e serviços de rede

2.1.5 – Metodologia de Desenvolvimento

De acordo com os autores (Moss & Atre, 2003), a metodologia mais adequada para o desenvolvimento de um projecto de DW é designada por BI Roadmap e compõem-se por seis fases, sendo que as cinco últimas são cíclicas ou repetitivas:

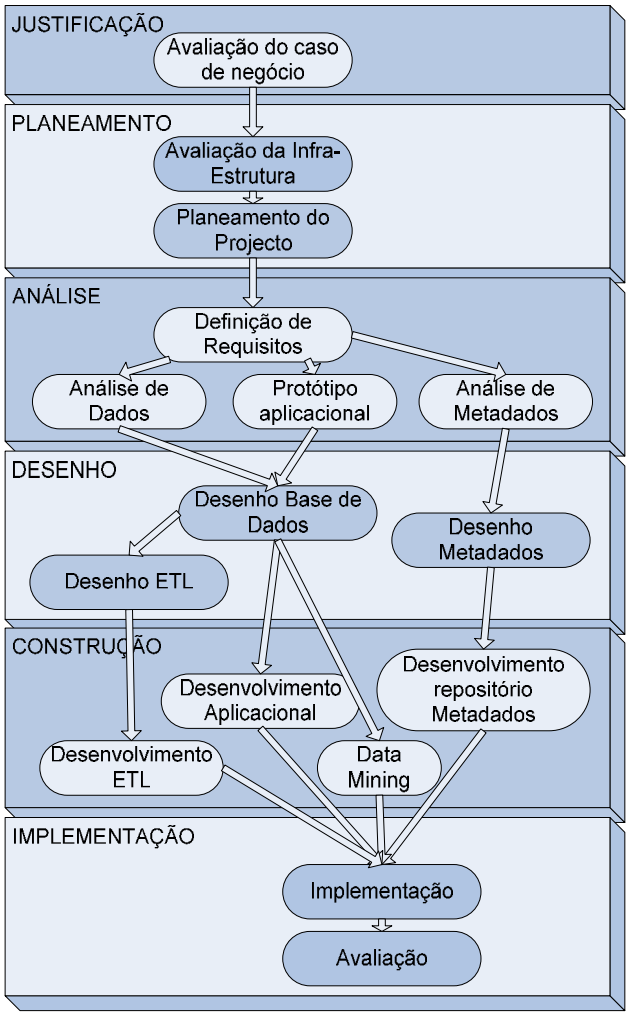

Ilustração 4 – Passos para o desenvolvimento do DW (Moss & Atre, 2003)

a) A Justificação

Não existem dúvidas que uma iniciativa de BI pode proporcionar numerosos benefícios à organização, não apenas tangíveis, como aumentar o volume de vendas, mas também intangíveis, como aumentar a reputação da organização. Muitos destes benefícios, especialmente os intangíveis, são difíceis de mensurar em termos monetários. No entanto, deve ser efectuada uma lista com os benefícios do DW, devidamente documentada e relacionada com os problemas específicos e objectivos estratégicos da organização.

Trata-se de uma avaliação de caso – Business Case Assessment – onde a oportunidade e a solução DW são propostos. Inclui análises de custo/beneficio das necessidades de negócio, avalia os actuais sistemas de suporte à decisão, as fontes e procedimentos operacionais, as opções de DW da concorrência, determina os objectivos do DW, propõe uma solução e avalia os riscos.

b) O Planeamento

Entre outros documentos, inclui:

- Avaliação das infra-estruturas da organização, quais já estão implementadas e quais desenvolver para implementar as aplicações transversais de BI
- Plano de Projecto detalhado, com revisões periódicas dado o dinamismo das aplicações de BI

c) A Análise

- Inclui os requisitos de negócio que visam indicar o âmbito. As equipas de projecto devem estar à espera que os requisitos se alterem ao longo do projecto à medida que os gestores de negócio aprendem mais sobre as possibilidades e limitações do BI
- Análise da qualidade dos dados, numa perspectiva de consolidação e reconciliação. Este passo consome bastante tempo de projecto
- Prototipagem das aplicações com uma análise de sistemas, permitindo despistar novos conceitos ou ideias e também possibilitar que os futuros utilizadores percebam as potencialidades e limites da tecnologia DW
- Análise do repositório de metadados. Os metadados técnicos devem ser mapeados com enfoque nos metadados de negócio, devendo ser guardados num repositório exclusivo para os metadados. Os requisitos para disponibilizar metadados à comunidade de utilizadores devem ser analisados neste passo.

d) O Projecto

Inclui os projectos:

- Da Base de Dados, os dados a agregar, os modelos dimensionais de acordo com os requisitos de 'Reporting'. Devem conjugar-se com os requisitos definidos pela comunidade de utilizadores.
- Do ETL, que é o processo mais complexo do DW, e as janelas de oportunidade para ser executado.
- De modelo lógico dos metadados.

e) A Construção

Desenvolvimento do processo ETL e das aplicações BI anteriormente prototipadas. Desenvolvimento das ferramentas exclusivas de DataMining e do repositório de metadados.

f) A Implementação

Uma vez realizados os testes, a equipa procede ao arranque das bases de dados e das aplicações. Dá-se então início às funções de suporte, que incluem a operação do Help Desk, a manutenção das Bases de Dados destino, programar e correr as rotinas de ETL, monitorizar a performance e optimizar e afinar as bases de dados.
A avaliação do ciclo é muito importante para futuras iterações pois existe uma ordem natural de progressão que estabelece certas dependências entre os vários ciclos de desenvolvimento.

2.1.6 – Conclusões do objecto DW

Este ponto procurou evidenciar os principais componentes e fases associados ao DW, colocando o foco no passo 2 da metodologia de investigação – O objecto DW –, nomeadamente no que diz respeito aos processos de gestão e controlo interno que lhe estão associados.
O levantamento de componentes do DW é de extrema importância para definir os princípios do modelo de avaliação do controlo interno, pois é com base nessa sistematização que se procederá ao levantamento de riscos e definição dos objectivos de controlo de cada um dos componente.
A investigação efectuada neste ponto permitiu identificar duas fases determinantes da gestão e controlo do DW, a fase de desenvolvimento e a fase de operação do DW.
De destacar que, para além dos componentes que dizem exclusivamente respeito ao DW, foram identificados componentes que são transversais a todas as tecnologias de informação da organização, não sendo portanto exclusivos do DW. Neste grupo incluem-se, por exemplo, as

componentes relacionadas com a gestão de acessos, de funções e responsabilidades, de infra-estruturas, de segurança, de qualidade dos dados, de armazenamento e arquivo, entre outras.
Abaixo se discriminam as componentes do DW identificadas neste ponto:

a) Componentes do ambiente de desenvolvimento do DW

São próprios da fase de desenvolvimento aplicacional (DW) ou temático (Datamart) possuindo objectivos de controlo específicos. A acção de auditoria deverá considerar estes componentes apenas em caso de avaliação de ambientes de desenvolvimento:

- Justificação
- Planeamento
- Análise
- Projecto
- Construção
- Implementação

b) Componentes do ambiente de produção do DW

São componentes que têm impacto directo ou decorrem da operação do DW como por exemplo o processo ETL, os outputs e o registo dos metadados.

- Sistemas-fonte
- 'Back Room' ou Aquisição
  - Extracção
  - Limpeza
  - Conformidade
  - Entrega
- 'Front Room' ou Acesso
  - Datamart
  - Fragmentação
  - Replicação
- Metadados

c) Requisitos Transversais (DW/SI/TI)

Os componentes registados neste tópico referem-se aos requisitos do DW como por exemplo, os requisitos de negócio, e outros que podem ser transversais ao DW e a outras TI. Nos casos dos requisitos transversais são normalmente instituídas políticas específicas que abrangem todos os SI/TI da organização.

- Negócio
- Conformidade
- Segurança
- Integração
- Qualidade dos dados
- Latência, Arquivo e Recuperação
- Funções e responsabilidades
- Acessos e utilizadores
- Infra-estruturas

2.2 – Os meios de Controlo e Auditoria Interna

O segundo ponto deste capítulo foca o tema do controlo interno e da auditoria interna das organizações, podendo ser integrado, portanto, no passo 3 da metodologia de investigação (ver ponto 1.2.2), ou seja, os meios para exercer o controlo do DW.
Apesar do tema não ser recente, nos últimos anos têm sido bastante questionadas os papéis da auditoria interna e do controlo interno nas organizações. Este debate surge por força dos acontecimentos que recentemente afectaram organizações que, apesar de supostamente estáveis, foram vítimas de acontecimentos que lhes causaram avultados prejuízos. A razão para tais acontecimentos não terem sido atempadamente detectados deveu-se essencialmente a falhas nos sistemas de controlo internos das organizações, especialmente na ponderação de operações financeiras, com riscos e severidades mal avaliados, resultando essa má avaliação frequentemente em situações de ruptura financeira e falência de toda a organização.

2.2.1 – O Controlo Interno

Para o Institute of Internal Auditors (IIA) a palavra "Controlo" significa *"qualquer acção tomada pela administração ou outros órgãos gestores, com vista a gerir os riscos da organização e aumentar as expectativas de cumprimento dos objectivos e das metas a atingir. O Controlo Interno gere planos, organiza e dirige um conjunto de acções suficiente para proporcionar a necessária confiança de que os objectivos e metas definidos vão ser atingidos"* (IIA, 2009)

"Em termos gerais, o sistema de controlo interno define-se como o conjunto das estratégias, sistemas, processos, políticas e procedimentos definidos pela gestão executiva com vista a garantir:

a) Objectivos de desempenho – Um desempenho eficiente e rentável da actividade que assegure: a utilização eficaz dos activos e recursos; a continuidade do negócio através de uma adequada gestão e controlo dos riscos da actividade; a prudente e adequada avaliação dos activos e responsabilidades; implementação de mecanismos de protecção contra utilizações não autorizadas, intencionais ou negligentes;

b) Objectivos de Informação – A existência de informação financeira e de gestão, completa, pertinente, fiável e tempestiva, que suporte as tomadas de decisão e processos de controlo, tanto a nível interno como externo;

c) Objectivos de conformidade ou 'compliance' – O respeito pelas disposições legais e regulamentares aplicáveis, incluindo a prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como das normas e usos profissionais e deontológicos, das regras internas e estatutárias, das regras de conduta e de relacionamento com os stakeholders. "

(Banco de Portugal, 2008)

a) Objectivos de controlo

A implementação dos controlos devem obedecer a determinados objectivos. Os objectivos de controlo.

"Declarações genéricas sobre a qualidade mínima de um bom controlo em relação aos processos de TI" (COSO 2007 – Normas de auditoria SI).

"Estes objectivos, são de natureza genérica e cobrem aspectos como a integridade da informação, a segurança das tecnologias de informação e a conformidade com as políticas, planos, regras, leis e regulamentos." (Cascarino, 2007)

Os objectivos de controlo das tecnologias de informação têm objectivos e controlos próprios que pretendem assegurar:

- Integridade dos programas e processamento
- Prevenção de mudanças indesejadas
- Assegurar o controlo do planeamento e desenvolvimento
- Assegurar os testes adequados
- Controlar a transferência de programas
- Manutenção evolutiva de sistemas
- Utilizadores
- Qualidade
- Envolvimento da auditoria interna

b) As linhas de defesa do Controlo Interno

Em 2005 o COSO definiu as quatro componentes do controlo interno das organizações (ECIIA, 2008):

- **Ambiente de Controlo –** Que se reflecte na atitude e nos actos da organização perante o controlo interno, resultando das convicções, preferências e juízos de valor manifestados, ou seja, traduz o planeamento estratégico, a estrutura e a cultura organizacional para os objectivos de controlo interno. Se em cada 'Stake Holder' da organização houver uma sensibilidade para o tema dos riscos e das actividades de controlo, muito mais fácil será a detecção e mitigação de eventos infortúnios. Uma política de ética, educação e formação são os principais dinamizadores do ambiente de controlo;
- **Gestão de Riscos e Actividades de Controlo –** Corresponde ao conjunto integrado de processos de carácter permanente que assegurem a compreensão apropriada da natureza e magnitude dos riscos subjacentes à actividade desenvolvida. A função deve estar devidamente sistematizada e organizada por tipo de riscos e dotada de recursos necessários para analisar, estabelecer e monitorizar os controlos definidos para minimizar os riscos da organização;
- **Monitorização –** Compreende todas as acções e avaliações de controlo desenvolvidas pelas organizações, incluindo a Auditoria Interna, identificando deficiências no sistema de controlo interno, quer na sua concepção, quer na sua implementação e ou utilização;
- **Informação e Comunicação –** Transversal aos restantes processos, o sistema de controlo interno deve garantir a existência de informação substantiva, actual, compreensível, consistente, tempestiva e fiável, que permita uma visão global e abrangente sobre a situação financeira, o desenvolvimento da actividade, o cumprimento da estratégia e dos objectivos definidos, o perfil de risco da instituição e o comportamento e evolução do mercado ou mercados relevantes.

Como se pode constatar na figura seguinte, o processo de controlo interno é constituído por três níveis de profundidade ou funções especializadas do Controlo Interno, as chamadas 'linhas de defesa'.
Essas linhas de defesa começam pelo ambiente de controlo, que tem de ser permanente e é a base de todo o processo, passam pela função de gestão de riscos, também ela uma função de controlo permanente e terminam na função de auditoria interna, que difere das outras pelo tipo de acções de controlo que é periódico (ECIIA, 2008).

Assim, abaixo se detalha o papel de cada uma das linhas de defesa do controlo interno:

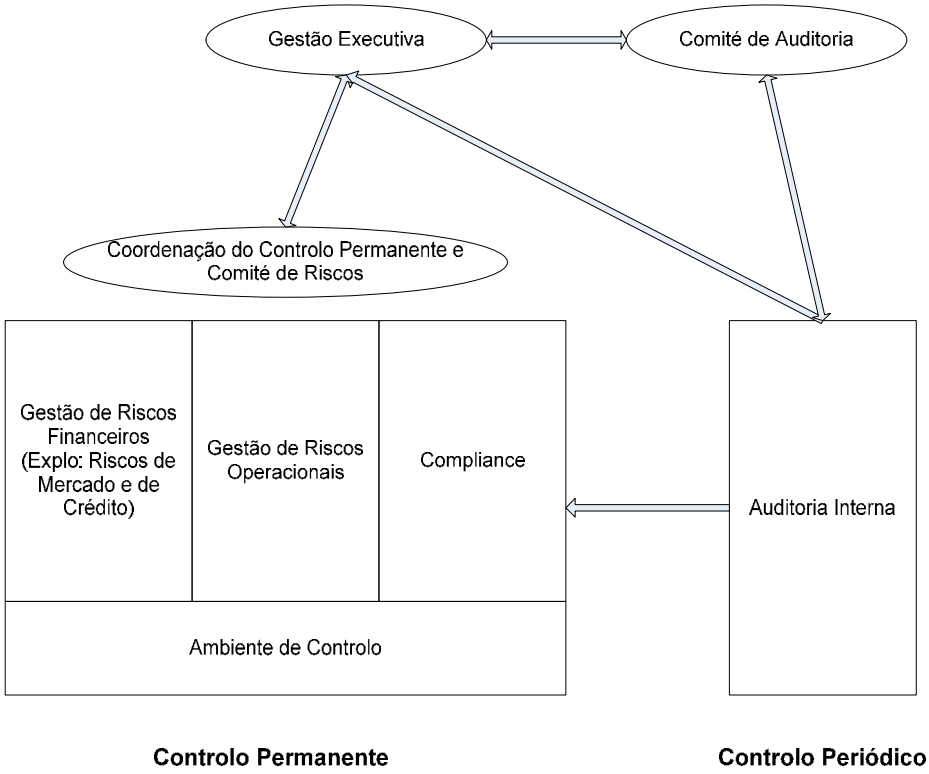

Ilustração 5 – Posicionamento da Auditoria Interna no Controlo Interno e no Modelo de Governação

A primeira linha de defesa é exercida com carácter permanente e designa-se por Ambiente de Controlo. Está relacionada com a vertente operacional e a sua execução deverá caber a todos os empregados da organização, através da aplicação às suas tarefas diárias. São exemplos de ambiente de controlo, a segregação de funções, em que nenhum indivíduo deverá exercer controlo sobre mais do que uma fase de um processo, e o princípio dos 'quatro olhos', em que todas as decisões e transacções devem ser supervisionadas por mais do que uma pessoa.

Na segunda linha de defesa do controlo interno, também ela de carácter permanente, inserem-se os actos de gestão dos riscos e supervisão dos controlos. As duas principais funções desta 2ª linha de defesa são: o 'Compliance' – que assegura a conformidade com as politicas, planos, procedimentos, leis e regulamentos – e a Gestão de Riscos – que se dedica ao controlo e redução do risco para níveis aceitáveis de acordo com o definido pela gestão executiva nesta matéria. De referir que existem muitas tipologias de riscos que poderão ser geridos em sede própria, no entanto os riscos de natureza transversal como o risco de estratégia ou o risco reputacional deverão ser geridos por um órgão próximo da Administração, como por exemplo, um Comité de Gestão de Riscos ou pelo próprio Comité de Controlo Interno.
A terceira e última linha de defesa do controlo interno é efectuada com um carácter periódico, onde o principal enfoque está em medir e avaliar a eficácia e a eficiência dos controlos executados pelas duas primeiras linhas de defesa. Esta função é executada pela auditoria interna e constitui a sua principal actividade.
O papel principal da auditoria interna é o de monitorizar se os controlos implementados são adequados e estão a ser executados convenientemente pelas primeira e segunda linhas de defesa, ou seja, a Auditoria Interna avalia, de forma quantitativa e qualitativa, se os riscos estão a ser devidamente considerados e se os controlos são eficazes para prevenir ou mitigar os riscos. Deste modo, a Auditoria Interna serve de elemento de garantia da confiança da gestão executiva no sistema de Controlo Interno da organização. Com estas três linhas de defesa do Sistema de Controlo

Interno devidamente implementadas, garantem-se que os objectivos estratégicos da organização vão ser atingidos com o máximo de eficiência e eficácia.

2.2.2 – A Auditoria Interna

A auditoria é um conceito muito mais amplo do que a simples detecção de erros e falhas (análise de conformidade). A auditoria pode ser referida como um exame crítico que tem a finalidade de avaliar a eficácia e eficiência de um departamento ou uma organização, e tem o objectivo de analisar o funcionamento parcelar ou global das organizações, de modo a avaliar as deficiências de desempenho, informar a Gestão Executiva dos impactos potenciais dos riscos e sugerir vias de correcção e melhoria.
Pode-se deste modo afirmar que "a auditoria é uma operação de análise e diagnóstico da empresa, tendo em consideração todos os aspectos da sua gestão, a fim de avaliar a coerência, a racionalização de processos e de apreciar a validade e o rigor dos resultados". (Carneiro, 2004)
De referir que a principal diferença entre a auditoria interna e a auditoria externa é, não apenas o facto de a origem dos auditores ser interna à empresa ou externa mas também as suas finalidades distintas. A auditoria externa é mais utilizada quando se pretende um relato mais distante entre auditores e auditados. Recorre-se igualmente à auditoria externa quando se pretendem auditar matérias de cariz muito técnico, ou seja, em que o conhecimento dos auditores terá de ser bastante especializado.
A auditoria interna é, como já referido, exercida por técnicos da própria organização e pretende ser um órgão de suporte e auxilio à gestão, constituindo uma função de avaliação independente que tenha por finalidade a avaliação das actividades da organização e assim apoiar a administração.
Em 1978 o Institute of Internal Auditors IIA introduziu os standards para a prática profissional da auditoria interna, proporcionando consistência internacional e uma ferramenta para avaliar a qualidade do processo de auditoria interna. Desde então, o IIA tornou-se na entidade de referência mundial da auditoria interna.
Em Janeiro de 2002 o IIA adoptou a revisão dos standards de auditoria, os quais incluíam a seguinte definição:

"A auditoria interna é uma actividade independente, com objectivo de garantir a confiança e o conhecimento especializado, e concebida para adicionar valor e melhorar a operacionalidade da organização. Contribui para que a organização atinja os seus objectivos criando uma abordagem, sistemática e disciplinada, para avaliar e melhorar a performance dos processos de gestão de riscos, de controlo interno e de governação." (IIA, 2009)

a) O Processo de Auditoria

O processo de auditoria é baseado numa série de procedimentos globalmente aceites. O papel do auditor é o de assegurar que os objectivos da auditoria são atingidos através da aplicação dos standards profissionais.
Durante uma auditoria é importante recordar que todas as decisões e opiniões precisam de um suporte de evidência e documentação. Cabe ao auditor a responsabilidade de assegurar a consistência do processo de auditoria.
Existem 10 fases a considerar quando se realiza uma auditoria (Cannon et al, 2006):

- Plano da actividade de auditoria;
- Programar a auditoria;
- Definição dos riscos e objectivos de controlo a avaliar;
- Determinar o âmbito da auditoria e a auditabilidade;
- Executar a auditoria;
- Identificar e recolher evidências;

- Realizar testes de auditoria;
- Analisar os resultados;
- Relatar as deficiências encontradas;
- Conduzir actividades de Follow-up.

b) Os Tipos de Auditoria

Para a auditoria de um sistema Data Warehouse importa realçar mais três tipos de auditoria:

- **Auditoria de gestão**, que visa monitorizar os objectivos estratégicos e tácticos de alto nível, bem como o processo de tomada de decisão, os critérios, políticas e procedimentos para a respectiva aplicação aos sistemas da organização. A finalidade deste tipo de auditoria é a de verificar em que medida os recursos limitados à disposição da gestão estão a ser aplicados, do ponto de vista da eficiência, eficácia e economia. A Auditoria de gestão emite pareceres, nomeadamente, sobre os objectivos definidos e as políticas seguidas, o processo de planeamento estratégico, a estrutura organizacional e sua adequação com os objectivos globais, a metodologia de controlo interno, os respectivos procedimentos e resultados obtidos.

- **Auditoria de Sistemas** abrange, não apenas a função informática, mas todos os Sistemas de Informação, informatizados ou não, analisando e avaliando os controlos de processamento de informação, a formulação e instalação dos sistemas, verificando os fluxos de informação, a eficiência dos recursos informáticos e o processamento e a integridade dos dados. A Auditoria de sistemas abrange os processos de planeamento, desenvolvimento, testes e aplicação dos sistemas, quer examinando a estrutura lógica, física, ambiental, de controlo, segurança e protecção dos dados. Os objectivos da Auditoria de sistemas passa por assegurar os níveis de confiança dos utilizadores, controlar os objectivos de segurança dos dados, dos componentes tecnológicos, contribuindo para a adequada governação da função informática e do compromisso de responder a metas e objectivos organizacionais, minimizar e controlar os níveis dos riscos inerentes à utilização de tecnologias de informação, e assegurar a integridade, confidencialidade e fiabilidade da informação mediante o controlo e recomendação de objectivos de segurança.

- **Auditoria Informática** é uma sub aplicação da Auditoria de sistemas, especificamente direccionada para as ferramentas informáticas e respectiva envolvente tecnológica. Sendo praticada por técnicos especializados, internos ou externos, este tipo de auditoria visa inventariar e avaliar os meios físicos e as tecnologias adequadas à recolha e processamento de dados e informação, examinar os controlos e avaliar a sua eficácia, validar a qualidade e utilidade da informação obtida e verificar a sua segurança face ao parque informático.

c) O Papel do auditor informático

A função do auditor de sistemas de informação é a de avaliar os controlos internos da organização. Os controlos internos são um requisito do processamento diário em todos os computadores.
Os tipos de controlos que se aplicam ao serviço prestado pelas TI são (Bacik, 2008)
Uma auditoria é simplesmente uma revisão do passado. Ao auditor de Sistemas de Informação é esperado que siga o já definido processo de auditoria, estabeleça os critérios, recolha as evidências significantes, e dê uma opinião independente acerca dos controlos internos.
O sucesso de um auditor está relacionado com a sua capacidade para reportar objectivamente os resultados das investigações, quer estes sejam bons ou maus, e também que esses resultados sejam verificáveis. A função do auditor é a de reportar o que as evidências apontam.

2.2.3 – A Gestão do Risco

A gestão de risco é a identificação, avaliação e prioritização dos riscos seguida da aplicação eficaz dos recursos para minimizar, monitorizar e controlar a probabilidade e o impacto dos eventos infortúnios. Os riscos podem provir de incertezas nos mercados financeiros, falhas de projectos, inconformidades legais, risco de crédito, acidentes, causas naturais e desastres ou ainda, por ataques deliberados de adversários (Hubbard, 2009).
No geral, as metodologias de gestão de riscos são constituídas pelos seguintes elementos:

1. Identificação, caracterização e avaliação dos riscos;
2. Avaliação da vulnerabilidade dos activos críticos a ameaças específicas;
3. Determinação dos riscos (incluindo as consequências de ataques a activos específicos);
4. Identificação de formas de redução dos riscos;
5. Prioritização das medidas para reduzir os riscos de acordo com a estratégia da organização.

As estratégias para reduzir o risco incluem a sua transferência para outra parte ou titular, a sua prevenção, a redução do efeito negativo e assumpção de parte ou de todas as consequências de algum risco em particular.
Os riscos ocorrem a todos os níveis da organização. Existem riscos estratégicos, riscos tácticos, riscos operacionais e outros riscos inerentes.
A gestão dos riscos deve ser permanente em todas as áreas do negócio, incluindo as tecnologias de informação.
A gestão de riscos opera a vários níveis. A gestão de riscos ao nível estratégico está focalizada na evolução de uma determinada estratégia ao longo dos anos. Ao nível dos projectos, a gestão de riscos avalia se o projecto está no caminho certo. No dia a dia, hora a hora, a gestão de riscos operacionais procura assegurar que o pessoal está a proceder de acordo com o que é esperado.
Acima de tudo, em situações de elevado risco, com potencialidades para gerar elevadas perdas, consequências ou impacto, devem aplicar-se métodos que permitam assegurar que o problema recebe a consideração adequada e o apropriado nível de esforço para prevenir a desafortunada ocorrência. É bastante comum que as equipas de TI, devido à pressão elevada, possuírem um fraco controlo de mudança, nomeadamente em interrupções, falhas, fraudes ou outros riscos.
Ao desenvolver um programa de avaliação da gestão de riscos, o auditor pretende assegurar-se de que a função de gestão de riscos foi implementada, com um propósito claramente definido, responsabilidades de gestão atribuídas e que se trata de um processo efectivamente implementado no terreno.
Após identificar a metodologia para avaliar os riscos e os controlos, o auditor deve identificar potenciais riscos para a organização. Para identificar esses riscos, o auditor precisa de saber: que activos precisam de ser protegidos, qual o seu nível de exposição, as ameaças e as fontes e outras matérias relativas à segurança.

a) Riscos de implementação de um Data Warehouse

Como foi descrito, o desenvolvimento de uma arquitectura de Data Warehouse acarreta vários tipos e níveis de riscos. Uma das formas de classificar os riscos pode ser dividindo-os em três categorias:

- Riscos de Tecnologia – A equipa que administra a DW não consegue colocar a tecnologia a funcionar correctamente devido, por exemplo a falhas nas ferramentas de importação e carregamento dos dados;

- Risco de Gestão de Projecto – A equipa, apesar do domínio da tecnologia, não consegue apresentar os projectos com a qualidade desejada ou nos prazos devidos;

- Risco Comercial – Este é o risco menos considerado no planeamento e análise dos projectos DW mas é o que normalmente causa problemas com maior frequência, sendo que, após a correcta implementação do sistema, este pura e simplesmente não é utilizado ou é subaproveitado. O grande problema deste tipo de risco é que só é detectável após a implementação do DW e portanto com o orçamento totalmente gasto.

2.2.5 – Conclusões dos meios de Controlo e Auditoria Interna

A segunda parte do 'Estado da Arte' visou acima de tudo aprofundar o tema do controlo interno e o seu papel determinante na arte de bem gerir, especialmente quando se tratam de gerir realidades complexas como por exemplo a gestão das organizações, em geral, ou a gestão de sistemas e tecnologias de informação, em particular.
Deste modo identificámos as principais actividades realizadas no âmbito do controlo interno das organizações, também designadas por linhas de defesa, ou seja:

- 1ª linha – Ambiente de Controlo
- 2ª linha – Gestão de riscos e gestão de informação e comunicação
- 3ª linha – Monitorização / Auditoria Interna

Para além de conceitos mais gerais relacionados com o controlo interno, procuraram-se também particularizar alguns processos específicos das actividades de auditoria interna, nomeadamente aquelas mais directamente relacionadas com a auditoria de sistemas de informação, bem como identificar alguns riscos específicos associados à implementação de ferramentas de 'Business Intelligence' e 'Data Warehousing'.

2.3 – Governação das Tecnologias de Informação (IT Governance)

A terceira parte do 'Estado da Arte' procura identificar as metodologias e as melhores práticas recomendadas para a governação de sistemas e tecnologias de informação.
Assim, a matéria estudada neste ponto insere-se no passo 3 da metodologia proposta para a presente investigação (Ver ponto 1.2.2).

"A forma como se processa a gestão das TI/SI numa organização revela-nos o nível de integração e controlo que essa organização tem sobre o seu investimento." (Cannon et al, 2006)

"É necessário considerar o modelo de governação das Tecnologias de Informação (TI), que se consegue através da gestão da estrutura, da atribuição de responsabilidades e definição de autoridade, e passa pela implementação de politicas e procedimentos com vista à adequada alocação dos recursos. Para a maioria dos casos, a politica é planeada para proteger a informação critica, os sistemas de informação, os detentores desses sistemas e os utilizadores, através de controlos físicos e virtuais" (Bacik, 2008)

O IT Governance pode-se definir como: *"Estabelecer os direitos de decisão e o modelo de notação contabilística de modo a encorajar um desejável ambiente na utilização das TI"* (Weill & Ross, 2004)
O IT Governance Institute expandiu a definição anterior de modo a incluir os mecanismos funcionais: *"A liderança, a estrutura organizacional e os processos que asseguram que as TI suportam as estratégias e os objectivos da organização."* (IT Governance Institute, 2008*)*
As tecnologias de informação (TI) são uma inevitabilidade dos negócios da actualidade. A função TI deve ter o seu valor intrínseco incorporado em todos os aspectos do negócio, em lugar de ser considerada como uma função distinta. O nível de integração da função TI, nomeadamente nas ferramentas de suporte à decisão, tem um efeito preponderante sobre a forma como a organização define a sua missão, os seus objectivos estratégicos e comunica a sua visão de crescimento.
Assim, de forma a obter uma visão geral sobre o que pode ser avaliado, em termos de controlo interno das TI, e quais os níveis de gestão abrangidos abaixo se caracteriza o conjunto de metodologias e boas práticas amplamente aceite, cuja implementação numa organização é fundamental para que o acto de governar das tecnologias de informação se faça da forma mais adequada, maximizando o investimento efectuado nos sistemas de informação da organização, incluindo o sistema de Data Warehouse, como repositório de informação determinante para a tomada de decisão. Referimo-nos especialmente às metodologias do Cobit, ITIL e ISO/IEC 27002.

O International Organization for Standardization (ISO) ajudou a clarificar o termo 'IT Governance' descrevendo-o como o modelo de governação utilizado pela Direcção Executiva. Por outras palavras, o modelo de governação diz respeito ao processo de gerir os recursos de tecnologias de informação, numa perspectiva sustentada de satisfação de todos os 'stakeholders', os quais esperam um retorno do seu investimento. Os directores responsáveis por este desígnio terão de assegurar a gestão da implementação dos sistemas necessários e dos controlos de TI, gerir o risco e garantir a conformidade.
Estes são os componentes essenciais para uma boa governação, sendo que o mais importe é focar na entrega de valor e na medição da performance.
Muito se fala acerca do tema do modelo de governação das TI das organizações pois trata-se de uma matéria complexa que abrange diferentes áreas de conhecimento, nomeadamente a gestão executiva, a gestão de TI, os auditores e técnicos de compliance, quase sempre detentoras de culturas e linguagens diferentes, o que não contribui para facilitar o assunto.
A utilização de práticas estandardizadas dão suporte e possibilitam:

- Uma melhor gestão das TI, o que é critico para o sucesso da organização;

- Actos de gestão de TI mais eficazes;
- Uma gestão mais eficaz das politicas, do controlo interno e da definição de funções e papéis;
- Outros benefícios como ganhos na eficiência, menor dependência de conhecimento individualizado, menos erros, parceiros mais confiantes, etc

Assim, todas as organizações que desejem adoptar as melhores práticas para a gestão de TI devem definir um modelo de trabalho eficaz, que, através de uma abordagem abrangente e consistente, permita assegurar o sucesso dos outputs da organização, quando utiliza as TI para suportar a sua estratégia (IT Governance Institute, 2008).

2.3.1 – A gestão estratégica

Para ter sucesso nos seus investimentos em TI, a gestão de topo deve definir uma estratégia de actuação e, simultaneamente, dotar o modelo de governação corporativa de um órgão de estrutura especialmente vocacionado para estas matérias, o Comité de TI/SI.

"O Modelo de Governação Corporativa – 'Corporate Governance' – é um conjunto de processos, modelos, políticas, regulamentos, estatutos que afectam a forma como a organização é gerida, administrada ou controlada. A governação corporativa abrange também o relacionamento entre os 'stakeholders' envolvidos e os objectivos pelos quais a organização é governada." (Crawford, 2007)

Uma das iniciativas organizacionais de maior sucesso para assegurar a adequada gestão estratégica das TI é efectuada com a criação de um Comité especializado, onde se incluem os representantes de várias áreas do negócio.
As áreas normalmente representadas no Comité de TI são: a gestão de topo, a gestão de TI, a gestão do marketing, das vendas, a contabilidade, o controlo de qualidade e o 'compliance'.
Desta forma é possível reunir as diferentes dimensões do negócio e as respectivas perspectivas.
A gestão executiva selecciona uma estratégia que lhe permita atingir os seus objectivos. Após uma aprovação top-down, a estratégia é formalizada em politicas e comunicada através da organização.
O propósito de especificar as politicas é o de informar as partes interessadas sobre uma solução adoptada.
Os planos estratégicos de TI são feitos para ajudar a organização a atingir os seus objectivos de curto e médio prazo. Este planeamento deve explicitar os objectivos de negócio abrangidos e a que nível as TI contribuem para a organização poder atingir esses objectivos.
O plano de TI deve ser composto por: - plano de dados, plano de gestão aplicacional, plano tecnológico e plano de infra-estruturas.

2.3.2 – Standards da governação de TI: CobiT® 4.1, ITIL® V3, ISO/IEC 27002

Todas as organizações, se quiserem seguir as práticas de maior sucesso no mercado adoptando os standards, precisam de os adaptar de modo a servir os seus requisitos específicos de tecnologias de informação (TI).
Neste campo os standards mais conhecidos e adoptados são o CobiT® 4.1 e o ISO/IEC 27002, para definir o que deve ser feito, e o ITIL® V3, para definir como devem ser geridos determinados aspectos.
A utilização das melhores práticas (Standards) possibilita e suporta:

- Uma melhor gestão das TI, o que é critico para o sucesso da estratégia da empresa
- Uma governação efectiva das actividades de TI
- Um conjunto de notações de trabalho para definir políticas, controlos e práticas necessárias para que todos saibam o que fazer

- Outros benefícios de negócio como ganhos de eficiência, menor dependência de experts, menos erros e confiança crescente dos utilizadores e outros stakeholders

Existe, no entanto, o risco da implementação destas boas práticas ser demasiado dispendiosa para a organização e não focalizada no essencial. Para ser eficaz, a adopção dos standards deve ser aplicada no contexto de negócio e focalizada nos aspectos que podem gerar maior benefício para a organização.
Os responsáveis pela gestão executiva, pelo negócio, pela auditoria, os especialistas de compliance e os gestores de TI, devem trabalhar em conjunto para assegurar que a implementação dos standards conduzirá a uma melhoria, em termos de custo benefício, de controlo das tecnologias de informação e, em especial, de gestão da arquitectura de Data Warehousing.
Os standards abaixo referidos são os mais amplamente adoptados em todo o mundo, nomeadamente:

- ITIL® V3 — Publicado pelo Governo Inglês como um modelo de referência para a gestão dos serviços de TI;
- CobiT® 4.1 — Publicado pelo ITGI, posicionando-se como um modelo de governação e controlo de alto nível;
- ISO/IEC 27002:2005 — Publicado pelo ISO (International Organization for Standardization) em conjunto com a IEC (Electrotechnical Commission).

a) ISACA/CobiT® 4.1

O ISACA (Information Systems Audit and Control Association - http://www.isaca.org/) reconheceu no início dos anos noventa que os auditores, que já tinham criado as suas listas de questões relacionadas com as tecnologias de informação, não utilizavam uma linguagem sintonizada com o s gestores de TI e com o s gestores executivos das organizações.
Em resposta a esta falha de comunicação, foi desenvolvido um modelo de trabalho que permitisse identificar os objectivos de controlo das TI de uma forma compreensível aos gestores de TI e aos gestores executivos. Nasceu assim o CobiT® 4.1 (Control Objectives for Information Tecnology).
Ao longo dos anos o CobiT® 4.1 tem sido desenvolvido como um Standard sendo actualmente o modelo de controlo mais amplamente adoptado pelas organizações para avaliar da eficácia da gestão de TI.

O CobiT® 4.1 habilita a gestão executiva a compreender melhor as TI da organização e que esperar dos fornecedores em termos de boas práticas. É um guia para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*, www.isaca.org). O CobiT® 4.1 inclui recursos tais como um sumário executivo, um modelo de trabalho – *Framework* – para o controlo de objectivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gestão de TI. As práticas de gestão do CobiT® 4.1 são recomendadas pelos peritos em gestão de TI pois permitem optimizar os investimentos efectuados, quer pelo fornecimento de métricas adequadas, quer pela avaliação dos resultados obtidos.

Top Management Issues Based on the CobiT Framework	Who Has a Primary Interest?			
	Board/ Executive	Business Management	IT Management	Audit/ Compliance
Plan and Organise				
Are IT and the business strategy in alignment?	√	√	√	
Is the enterprise achieving optimum use of its internal and external resources?	√	√	√	√
Does everyone in the enterprise understand the IT objectives?	√	√	√	√
Is IT's impact on enterprise risk understood and is the responsibility for IT risk management established?	√			
Are IT risks understood and being managed?		√	√	√
Is the quality of IT systems appropriate for business needs?		√	√	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		√	√	
Are new projects likely to deliver on time and within budget?		√	√	√
Will the new systems work properly when implemented?		√	√	√
Will changes be made without upsetting the current business operation?		√	√	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities?		√	√	
Are IT costs optimised?		√	√	√
Is the workforce able to use the IT systems productively and safely?		√	√	
Are adequate confidentiality, integrity and availability in place?		√	√	√
Monitor and Evaluate				
Can IT's performance be measured and can problems be detected before it is too late?	√	√	√	
Are internal controls operating effectively?	√			√
Is the enterprise in compliance with regulatory requirements?	√	√	√	√
Is IT governance effective?	√	√	√	√

Ilustração 6 – Mapeamento dos tópicos de gestão do CobiT® 4.1 com as Áreas de interesse (CobiT® 4.1)

Trata-se de um modelo de gestão das TI baseado em standards da indústria e nas melhores práticas. Uma vez implementado, o CobiT® 4.1 assegura que as TI estão devidamente alinhadas com os objectivos do negócio e que a prestação está optimizada para retirar vantagem acrescida da sua utilização.
O CobiT® 4.1 permite criar um interface de entendimento comum entre executivos e profissionais de TI, facilitando a comunicação de objectivos, de metas e de resultados aos auditores e aos profissionais de TI, assegurando, deste modo, as melhores práticas para monitorizar e gerir as actividades de TI.
Uma vez identificados e implementados os princípios chave que, de acordo com o CobiT® 4.1, são mais relevantes para a organização, os executivos conseguem gerar a confiança de que a gestão dos TI é eficaz, podendo esperar-se os seguintes resultados:

- Maior capacidade de trabalho conjunto entre os executivos e os profissionais de TI e melhor conhecimento da relação das TI com o negócio;
- Maior capacidade de gestão de custos e dos ciclos de vida das TI;
- Maior qualidade e tempestividade da informação produzida;
- Maior qualidade dos serviços e sucesso dos projectos de TI;
- Maior clareza nos requisitos de segurança, privacidade da informação;
- Melhor eficácia na gestão dos riscos relacionados com o TI;
- Maior eficiência e sucesso das acções de auditoria;
- Optimização da conformidade das TI com os requisitos regulamentares.

O modelo do CobiT® 4.1 – Framework do CobiT® 4.1 – explica como se organiza o modelo de governação, a gestão e os objectivos de controlo das TI e quais as melhores práticas para criar os domínios e processos das TI, bem como, ligá-los com os requisitos de negócio.

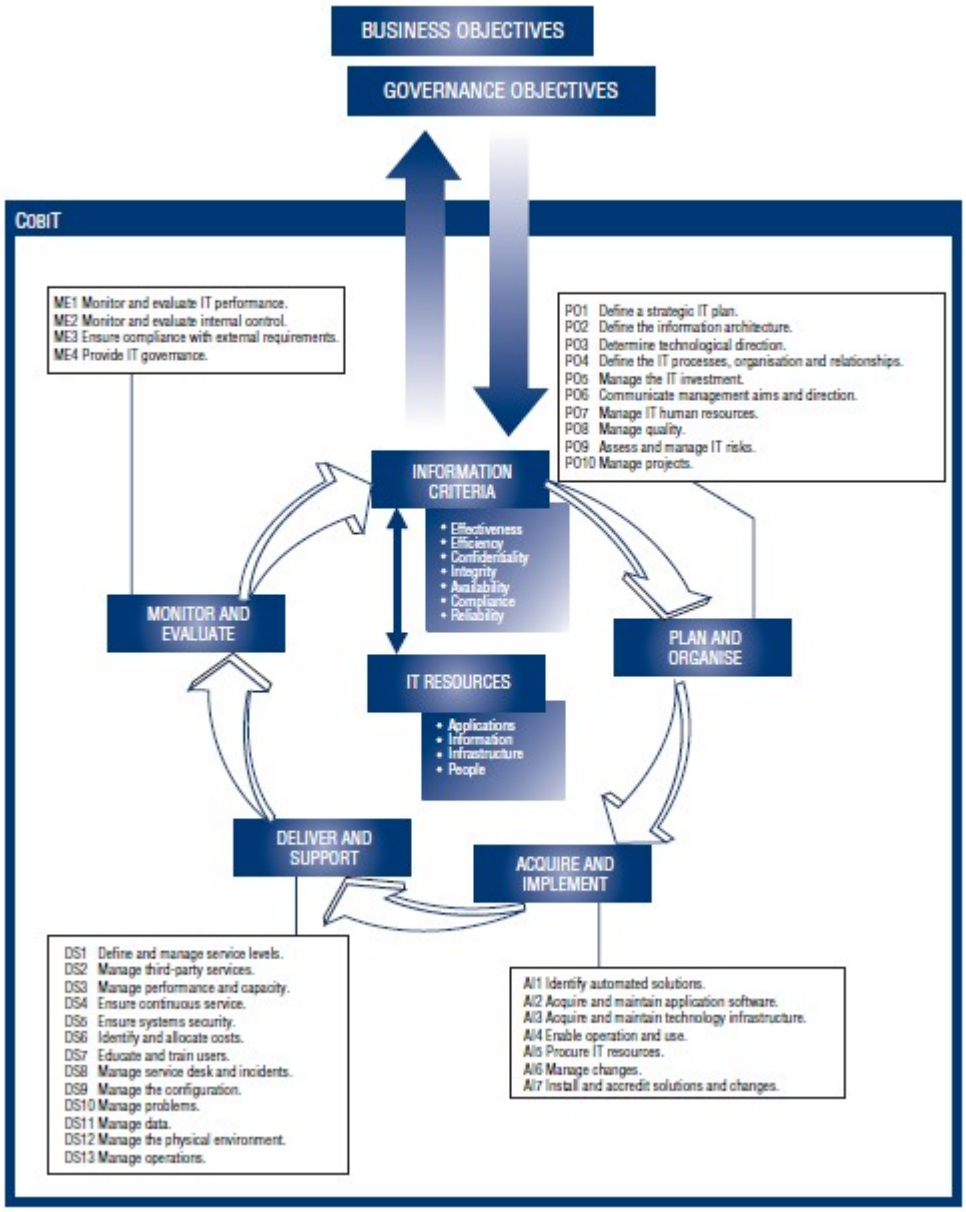

Ilustração 7 – Os processos de controlo do CobiT® 4.1 e os domínios de enfoque (In CobiT® 4.1)

O Framework do CobiT® 4.1 contém um conjunto de 34 processos de controlo de alto nível que se agrupam em 4 domínios:

"Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME)."

O CobiT® 4.1 define, para cada um dos 34 processos, um nível mais alto de objectivos de controlo e de 3 a 30 objectivos de controlo mais detalhados.
Os objectivos de controlo contêm declarações dos resultados desejados ou metas a serem alcançadas na implementação de procedimentos de controlo específicos dentro de uma actividade de TI e fornecem uma política clara para o controle de TI na empresa.
Os 34 processos de controlo do CobiT® 4.1 abrangem uma a descrição detalhada de:

- Processos, cobrindo áreas de responsabilidade de TI e de negócio;
- Objectivos de controlo genérico da gestão dos processos de TI;
- Linhas mestras e ferramentas para atribuir responsabilidades e medir a performance;
- Nível de maturidade dos processos, descrevendo perfis e descrevendo estados presentes e futuros.

A figura seguinte ilustra a estrutura do CobiT® 4.1, com os seus quatro domínios de actuação, em que fica claro uma ligação entre os processos TI e os processos de negócio da organização. Os mapas fornecidos pelo CobiT® 4.1 auxiliam os auditores e gestores a manter o adequado controlo para garantir o acompanhamento das iniciativas de TI e recomendar a implementação de novas práticas, se necessário.
Cada domínio cobre um conjunto de processos para garantir a completa gestão de TI, somando 34 processos:

(1) Planeamento e Organização (PO)

- PO1 – Define o plano estratégico de TI
- PO2 – Define a arquitectura da informação
- PO3 – Determina a direcção tecnológica
- PO4 – Define os processos de TI, a organização e os seus relacionamentos
- PO5 – Gere os investimentos em TI
- PO6 – Gere o plano de comunicação e de direcção das TI
- PO7 – Gere os recursos humanos de TI
- PO8 – Gere a qualidade
- PO9 – Gere e avalia os riscos
- PO10 – Gere os projectos

(2) Aquisição e implementação (AI)

- AI1 – Identifica as soluções de automatização
- AI2 – Adquire e mantém o software aplicacional
- AI3 – Adquire e mantém a infra-estrutura tecnológica
- AI4 – Desenvolve e mantém os procedimentos operacionais
- AI5 – Instala e certifica softwares
- AI6 – Gere a mudança

(3) Entrega e suporte (DS)

- DS1 – Define e mantém os acordos de níveis de serviços (SLA)
- DS2 – Gere os serviços de terceiros
- DS3 – Gere a performance e capacidade dos recursos TI
- DS4 – Assegura a continuidade dos serviços
- DS5 – Assegura a segurança dos sistemas
- DS6 – Identifica e aloca custos
- DS7 – Formação dos utilizadores
- DS8 – Gere o serviço de help desk e incidentes
- DS9 – Manutenção das configurações
- DS10 – Gere problemas
- DS11 – Gere os dados
- DS12 – Gere as infra-estruturas
- DS13 – Gere as operações

(4) Monitorização e Avaliação (ME)

- ME1 – Monitoriza e avalia a performance de TI
- ME2 – Monitoriza e avalia os controlos internos
- ME3 – Assegura a conformidade com os regulamentos
- ME4 – Garante o processo de governação de TI

b) ITIL® V3

As organizações da actualidade dependem das tecnologias de informação (TI) para satisfazer os objectivos da organização em satisfazer as necessidades de negócio e gerar valor para os consumidores.
Para que isto suceda de forma persistente e controlável, a organização deve assegurar que os serviços de IT são de elevada qualidade, alinhados com os requisitos de negócio, conformes com a regulamentação, eficazes na recolha e entrega e continuamente revistos e melhorados.
O Information Technology Infrastructure Library (ITIL® V3) é uma biblioteca de boas práticas (do inglês best practices) nos serviços de tecnologia da informação (TI), desenvolvida no final dos anos 80 pela CCTA (Central Computer and Telecomunications Agency) e actualmente sob custódia da OGC (Office for Government Commerce) da Inglaterra. O ITIL® V3 procura promover a gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação (TI). O ITIL® V3 endereça estruturas de processos para a gestão de uma organização de TI apresentando um conjunto abrangente de processos e procedimentos de gestão, organizados em disciplinas, com os quais uma organização pode fazer sua gestão táctica e operacional com vista a alcançar o alinhamento estratégico com os negócios (ITSMF, 2006).
O ITIL® V3 proporciona um método de trabalho compreensivo, consistente e coerente para a gestão de TI e seus processos relacionados, promovendo uma abordagem de elevada qualidade para garantir a eficiência e eficácia da gestão de TI.

"A missão do ITIL® V3 é a de descrever aproximações, funções, papéis e processos, que as organizações devem seguir como base das suas práticas." (Steinberg, 2006)

"O ITIL® V3 reúne vários conceitos e modelos num único documento, de modo a proporcionar um guia vocacionado para melhorar a qualidade dos serviços prestados pelas tecnologias de informação (TI), garantir o alinhamento entre as TI e o negócio, aumentar a eficiência das TI e reduzir os seus custos" (Marquis, 2006)

De acordo com este autor, o ITIL® V3 força as tecnologias de informação a cumprir os requisitos de negócio. Assim, algumas vezes as TI são ineficientes e dispendiosas, e outras vezes requerem mais investimento. O ITIL® V3 permite identificar estes desajustamentos não pelo valor do custo mas pela avaliação do serviço prestado pelas TI e valor entregue aos seus clientes.
Independentemente de toda a publicidade, não é possível aplicar, estar conforme, adoptar, implementar ou praticar o ITIL® V3 de forma directa. No entanto, o ITIL® V3 permite o seguinte:

- Servir de guia como princípio de base para uma filosofia de foco nos clientes, e de orientação dos processos de IT para o negócio;
- Servir de guia apenas nas partes mais necessárias à organização
- Servir de elemento de adaptação para uma situação específica

O **itSMF** é um fórum destinado a profissionais especializados em ITIL® V3 totalmente independente e reconhecido mundialmente. Em Portugal o endereço é o seguinte: http://www.itsmf.pt/.

As bibliotecas do ITIL® V3 dão suporte específico às seguintes áreas:

- **Incident Management (Gestão de incidentes)** – reduzir o tempo de indisponibilidade (downtime) dos serviços;
- **Problem Management (Gestão de problemas)** – minimizar o impacto no negócio dos incidentes e problemas causados pelos erros na infra-estrutura de TI e prevenir incidentes recorrentes desses mesmos erros;
- **Configuration Management (Gestão de configurações)** – identificar e controlar os activos de TI e os itens de configuração existentes na organização, estabelecendo o relacionamento dos mesmos aos serviços prestados;
- **Change Management (Gestão de mudança)** – minimizar o impacto da mudança requerida para resolução do incidente ou problema, mantendo a qualidade dos serviços, bem como melhorar a operacionalização da infra-estrutura;
- **Release Management (Gestão de novas versões)** – prevenir a indisponibilidade do serviço, garantindo que a instalação de versões de hardware e software estejam seguras, autorizadas e devidamente testadas.
- **Service Level Management/SLM (Gestão de Níveis de Serviços)** – garantir o acordo de nível de serviços (SLA) previamente estabelecido entre o fornecedor e o cliente;
- **Financial Management for IT Service (Gestão Financeira para TI)** – demonstrar ao cliente o custo real dos serviços prestados e proporcionar um nível de gestão profissional;
- **Availability Management (Gestão de Disponibilidades)** – garantir a disponibilidade e segurança dos recursos de TI, a fim de assegurar a satisfação do cliente e a reputação do negócio;
- **Capacity Management (Gestão de Capacidade)** – assegurar que a capacidade da infra-estrutura de TI está adequada às necessidades do negócio, observando sempre a gestão do custo envolvido;
- **IT Service Continuity Management/ITSCM (Gestão da Continuidade de Serviços)** – atender todo o processo de gestão da continuidade do negócio, assegurando que os recursos técnicos e sistemas de TI sejam recuperados quando requeridos, no tempo desejado.

Ao nível mais operacional das organizações é necessário que existam conhecimentos específicos dos processos para que a implementação do ITIL® V3 possa ser optimizada. Neste caso, existe uma complementaridade entre esta metodologia e, por exemplo, o standard internacional ISO/IEC 20000:2005 ou o CobiT® 4.1.

A prática do ITIL® V3 significa conduzir um processo contínuo de revisão, auditoria, análise e mudança de processos.

Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operation (SO)	Continual Service Improvement (CSI)
• Service management • Service life cycle • Service assets and value creation • Service provider types and structures • Strategy, markets and offerings • Financial management • Service portfolio management • Demand management • Organisational design, culture and development • Sourcing strategy • Service automation and interfaces • Strategy tools • Challenges and risks	• Balanced design • Requirements, drivers, activities and constraints • Service-oriented architecture • Business service management • SD models • Service catalogue management • Service level management • Capacity and availability • IT service continuity • Information security • Supplier management • Data and information management • Application management • Roles and tools • Business impact analysis • Challenges and risks • SD package • Service acceptance criteria • Documentation • Environmental issues • Process maturity framework	• Goals, principles, policies, context, roles and models • Planning and support • Change management • Service asset and configuration management • Release and deployment • Service validation and testing • Evaluation • Knowledge management • Managing communication and commitment • Stakeholder management • Configuration management system • Staged introduction • Challenges and risks • Asset types	• Balance in SO • Operational health • Communication • Documentation • Events, incidents and problems • Request fulfilment • Access management • Monitoring and control • Infrastructure and service management • Facilities and data centre management • Information and physical security • Service desk • Technical, IT operations and application management • Roles, responsibilities and organisational structures • Technology support to SO • Managing change, projects and risk • Challenges • Complementary guidance	• Goals, methods and techniques • Organisational change • Ownership • Drivers • Service level management • Service measurement • Knowledge management • Benchmarks • Models, standards and quality • CSI seven-step improvement process • Return on investment (ROI) and business issues • Roles • Authority matrix (RACI) • Support tools • Implementation • Governance • Communications • Challenges and risks • Innovation, correction and improvement • Best practices supporting CSI

Ilustração 8 – ITIL® V3 Core Topics (Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit – IT Governance Institute, 2008)

c) ISO/IEC 27002

O standard internacional foi publicado pela ISO (International Organization for Standardization) – www.iso.org/iso/home.htm e o IEC (International Electrotechnical Commission) - http://www.iec.ch que formaram um comité técnico conjunto.
O objectivo do ISO/IEC 27002:2005 é o de fornecer informação aos responsáveis pela implementação da segurança de informação da organização. Pode ser considerado como um conjunto de boas práticas para gerir o desenvolvimento e a manutenção dos standards de segurança de forma a optimizar a confiabilidade da informação.
O standard define 133 estratégias de controlo da segurança das TI, classificadas em 11 domínios, onde se destaca a importância da gestão de risco.
Os princípios orientadores do ISO/IEC 27002:2005 são os pontos para implementar uma segurança da informação. Estes pontos assentam, quer em requisitos de conformidade legal, quer em boas práticas amplamente aceites como tal.

Assim, os objectivos de conformidade incluem:

- Protecção dos dados pessoais;
- Protecção da informação interna;
- Protecção dos direitos de propriedade intelectual;

As boas práticas referidas no standard incluem:

- Política de segurança de informação;
- Atribuição de responsabilidades pela segurança de informação;
- Detecção de problemas;
- Gestão da continuidade do negócio;

Quando se implementa um sistema para a segurança da informação, os factores críticos a considerar são os seguintes:

- A política de segurança, os seus objectivos e actividades devem reflector os objectivos de negócio;
- A implementação deve considerar os aspectos culturais da organização;
- O suporte e compromisso da gestão executiva são requeridos;
- Devem existir processos de avaliação e gestão de riscos, bem como o conhecimento dos requisitos de segurança;
- Ampla implementação da segurança, incluindo os membros da gestão;
- As políticas e medidas de segurança estendidas a todo o âmbito de TI, incluindo outsourcing;
- A política de formação;
- Sistema de medição de performance compreensível, que suporte um sistema de feedback e melhoria contínua;

2.3.3 – A gestão operacional

"Uma operação é um procedimento para produzir um resultado desejado" (Weill & Ross, 2004).

O objectivo da gestão de operações é sustentar as necessidades diárias do negócio. A estratégia foi visionada e explicitada pela gestão executiva, a operacionalização técnica da estratégia foi criada pela gestão intermédia e os processos e procedimentos de trabalho são coordenados pelos gestores operacionais e pessoal de suporte. Deste modo, o trabalho produzido deve ser um suporte directo dos objectivos de alto nível do negócio.
Todas as organizações enfrentam o desafio de sustentar as operações. As áreas de interesse para a sustentação das operações associadas às TI/SI são as seguintes: - Pessoal técnico adequado; - Procedimentos devidamente explicitados; - Nível de integração do pessoal e processos.
Ou seja, é praticamente impossível sustentar operações com regularidade sem explicitar o conjunto de procedimentos apropriados, e que sejam executados por pessoal técnico especializado.

2.3.4 – Conclusões do IT Governance

A análise do IT Governance culmina a identificação dos principais pressupostos e componentes necessários para desenhar o modelo de controlo e auditoria interna do DW.
Este ponto serviu para identificar o que de melhor se faz no âmbito do controlo interno e auditoria dos sistemas e tecnologias de informação, quais os standards mais divulgados, e as práticas mais aconselhadas e amplamente aceites, para que o valor gerado por essas TI possa ser optimizado, correspondendo, no mínimo, ao previsto no plano de retorno do investimento efectuado pela organização na fase de desenvolvimento do DW.
Concretamente, da investigação efectuada, destacam-se as metodologias de controlo interno de TI/SI, difundidas como boas práticas e standards que, no modelo de avaliação proposto, serão mapeados com os componentes de controlo do DW. Deste modo, o processo de avaliação do controlo interno do DW proposto, será efectuado de acordo com as melhores práticas de avaliação de desempenho de TI reconhecidas internacionalmente, como sejam:

- CobiT® 4.1
- ITIL® V3
- ISO/IEC 27002

A implementação de um modelo de boas práticas deve ser consistente com a organização, nomeadamente com a gestão de riscos e a forma de executar o controlo interno.

3 – MODELO PARA AUDITAR O CONTROLO INTERNO DE UM DATA WAREHOUSE

Este capítulo visa propor um modelo de controlo e auditoria interna específico para Data Warehouses que identifique os principais componentes e objectivos de controlo associados a esta ferramenta de suporte à decisão. O modelo pretende servir de elemento de referência para avaliar se os processos de controlo estão a ser efectuados de acordo com as melhores práticas, ou seja, se a gestão da ferramenta está a ser efectuada de modo a que os resultados produzidos pelo DW correspondem ao previsto para aquele projecto.

Para proceder à construção do modelo de controlo e auditoria de DW foram seguidos os passos 4, 5 e 6 da metodologia de investigação proposta no ponto 1.2.2, respectivamente:

- Passo 4 – Desenho das componentes do modelo de controlo do DW
- Passo 5 – Identificação dos riscos e dos objectivos de controlo do DW
- Passo 6 – Mapeamento dos processos standard de avaliação do controlo do DW

3.1 – Desenho das componentes de controlo do Data Warehouse

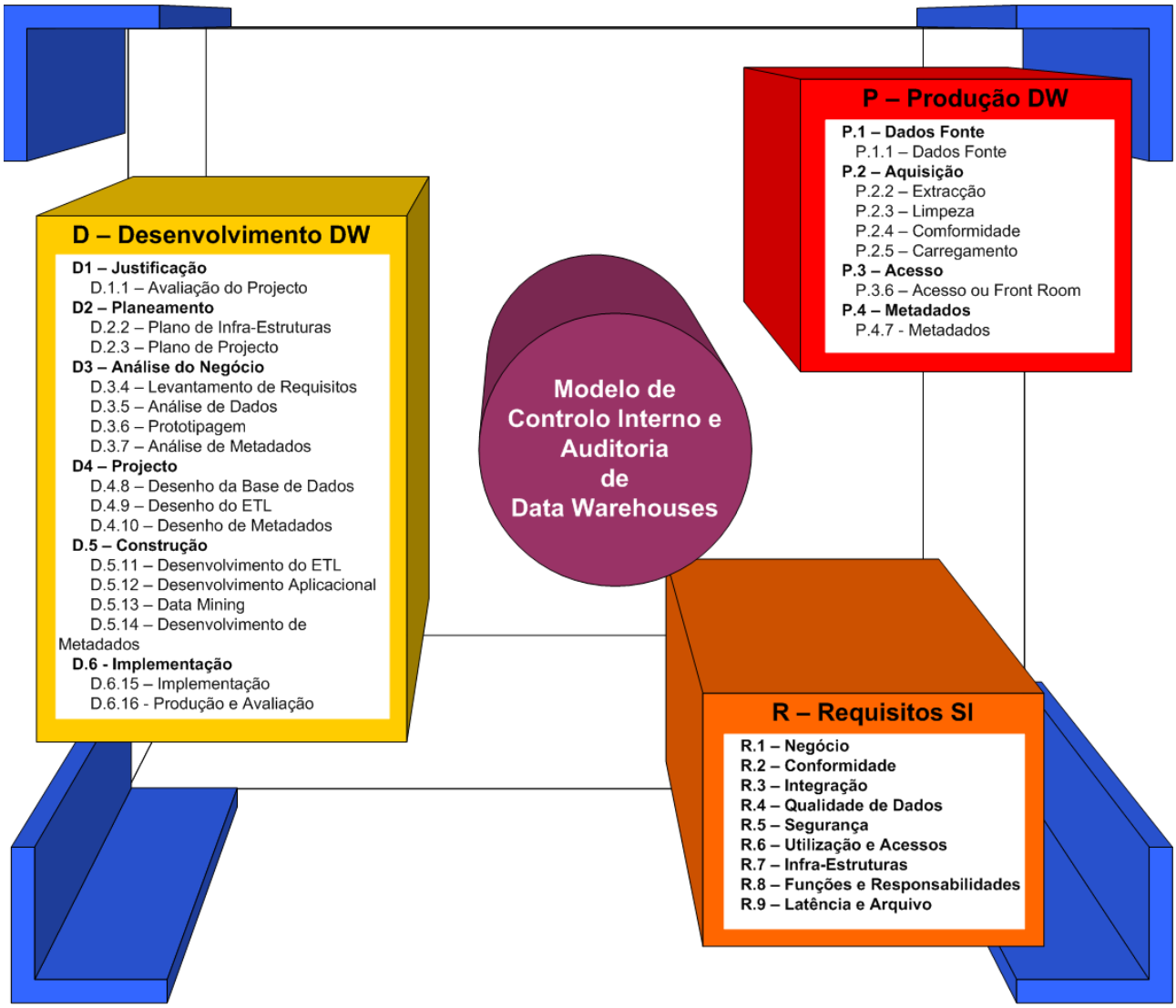

Ilustração 9 – Componentes do Controlo Interno do DW

Da análise efectuada no capítulo anterior considerámos que o modelo a propor deveria ser composto por três grupos de componentes de controlo:

- Ambiente de desenvolvimento DW
- Ambiente de produção DW
- Outros requisitos transversais

Trata-se de uma sistematização que, acima de tudo, procura ser abrangente quanto ao número de funcionalidades e fases do ciclo de vida do Data Warehouse, podendo deste modo servir de elemento de referência para as organizações, sistematizando e instituindo um conjunto de procedimentos de melhoria das necessidades de controlo dos seus DW, independentemente da fase, das particularidades de arquitectura ou da volumetria de informação tratada.

3.2 – Modelo para Controlo Interno e Auditoria de Data Warehouses

Nos pontos seguintes detalham-se as particularidades do modelo de controlo e auditoria de DW, nomeadamente pela definição dos objectivos de controlo e dos riscos de cada um dos componentes, bem como pelo mapeamento dos componentes com os processos de avaliação de controlo standardizados pelo Cobit, ITIL e ISO 27002 (Passo 5 e 6 do método de investigação - Ver ponto 1.2.2).

3.2.1 – D – Ambiente de Desenvolvimento DW

O ambiente de desenvolvimento abrange um conjunto de fases necessárias para tornar o processo DW de suporte à decisão uma realidade (Ver Ponto 2.1.6).
A principal referência considerada para identificar as fases do desenvolvimento do DW, os riscos e as necessidades de controlo, foi o manual de Moss, Larissa & Atre, Shaku (2003), *Business Intelligence Roadmap – The complete lifecycle for decision-support applications.*

Assim, neste ponto procuramos identificar os riscos das várias fases do processo de desenvolvimento de um DW ou de um Datamart, nomeadamente da Justificação, Planeamento, Análise, Projecto, Construção e Implementação.

a) D.1 – Justificação

Uma vez que é muito dispendioso criar uma arquitectura de DW, a organização necessita de ter uma estratégia de informação de suporte à decisão e uma justificação de negócio que estabeleça uma relação entre os custos envolvidos e os benefícios gerados.
A justificação deve avaliar as capacidades e performance actuais:

D.1 – Justificação				
D.1.1 – Avaliação do projecto DW				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• O acesso à informação • As variáveis de decisão chaves para o negócio • A cultura de decisão e a infra-estrutura de suporte • Os riscos • Os custos • O retorno do investimento	• Determinar a necessidade do negócio • Avaliar o actual sistema de suporte à decisão • Avaliar as fontes operacionais e os procedimentos • Avaliar as ferramentas de suporte à decisão da concorrência • Determinar os	• Um gestor de negócio (o utilizador da informação de suporte à decisão) • Um sponsor (alguém com peso institucional para fazer avançar o processo) • Um analista da	• Acabar a construir uma solução de suporte à decisão que não inclua as variáveis chave para o negócio nem dê suporte aos objectivos estratégicos para o negócio	• CobiT® 4.1: • PO1.1 IT value management • PO1.2 Business-IT alignment • PO1.3 Assessment of Current Capability and Performance • PO1.4 IT Strategic Plan • PO2.1 Enterprise information architecture model • PO4.2 IT strategy committee

	objectivos do DW • Propor a solução de DW • Elaborar uma análise de custo-benefício • Elaborar uma avaliação de risco	qualidade dos dados • Um gestor de projecto • Um especialista de negócio		• PO4.5 IT organisational structure • PO5.3 IT budgeting • PO5.4 Cost management • PO5.5 Benefit management • PO9.1 IT risk management framework • DS3.2 Current performance and capacity • DS3.4 IT resources availability • DS6.3 Cost modelling and charging

b) D.2 – Planeamento

O planeamento deve envolver duas componentes principais: o plano de infra-estrutura e o plano de projecto.

D.2 – Planeamento				
D.2.2 – Plano de Infra-estruturas				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
O **plano da infra-estrutura** deve definir os elementos da infra-estrutura física como por exemplo: 'Hardware', 'Middleware', e Sistemas de gestão de bases de dados, e os elementos não técnicos como: Os standards, as regras de negócio, os metadados e as políticas.	• O plano de infra-estrutura técnica inclui uma avaliação do actual estado, uma avaliação e selecção de novos produtos, uma avaliação da nova infra-estrutura e um plano de implementação. • O plano de infra-estrutura lógica inclui uma avaliação das políticas, procedimentos, linhas de acção e standards, definindo regras de denominação comuns a toda a organização, a optimização de tarefas e actividades, revendo os modelos e estratégias de dados e metadados, refinando a qualidade de dados, testando os standards e a reconciliação e revendo os SLA e a segurança.	Os técnicos especializados para elaborar o plano de infra-estrutura técnica são: • O arquitecto de sistemas de suporte à decisão • O administrador de bases de dados Os técnicos especializados para elaborar o plano de infra-estrutura lógica são: • O arquitecto de sistemas de suporte à decisão • O administrador de dados • O analista de qualidade de dados • O administrador de metadados	Os riscos de não realizar o plano de infra-estrutura são: • A performance técnica pode degradar-se a tal nível que a plataforma DW deixe de ser utilizável ou de a tecnologia ficar rapidamente desactualizada • A integração transversal do DW é fundamental. Não existindo políticas e regras comuns a toda a organização pode levar a soluções de DW espartilhadas, recursos mal aproveitados, arquitecturas complexas ou indecifráveis, e resultados indecifráveis ou irreconciliáveis	• PO4.1 IT process Framework • PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO2.4 Integrity management • PO3.1 Technological direction planning • PO3.2 Technology infrastructure plan • PO3.4 Technology standards • PO3.5 IT architecture board

D.2.3 – Plano de Projecto				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
O **plano de projecto** deve incluir uma análise do envolvimento da componente de negócio (Sponsor, stakeholders e níveis de comprometimento), o âmbito, os objectivos e as metas, os riscos, os constrangimentos, uma análise do custo benefício, da infra-estrutura, do pessoal e do conhecimento disponíveis. O plano de projecto deve ainda incluir um plano de actividades, entregáveis e hierarquias, do tipo 'work breakdown structure', uma estimativa de esforço nas actividades, das suas dependências e uma relação dos recursos afectos.		• O líder de desenvolvimento aplicacional • O representante da vertente de negócio • O administrador de dados • O analista da qualidade de dados • O administrador de bases de dados • O líder o desenvolvimento do ETL • O administrador de metadados • O gestor de projecto • O expert em sistemas de suporte à decisão	• Impossibilidade de construir um DW de suporte à decisão ad hoc sem um plano • Perda de controlo sobre o projecto • Não conseguir ultrapassar a complexidade do projecto de DW • Ultrapassar o orçamento previsto	• PO1.5 IT tactical plans • PO4.1 IT process Framework • PO4.6 Establishment of roles and responsibilities • PO4.7 Responsibility for IT quality assurance (QA) • PO4.8 Responsibility for risk, security and compliance • PO4.9 Data and system ownership • PO5.3 IT budgeting • PO5.4 Cost management • PO5.5 Benefit management • PO6.5 Communication of IT objectives and direction • PO7 Manage Human Resources • PO9.4 Risk assessment • PO9.5 Risk response • PO10 Manage Projects • DS5.2 IT security plan

c) D.3 – Análise do negócio

A análise do negócio inclui um levantamento dos requisitos do projecto, uma análise dos dados, uma prototipagem aplicacional e uma análise do repositório de metadados.

D.3 – Análise do negócio				
D.3.4 – Levantamento de requisitos				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Entrevistas com os responsáveis pelo negócio • Definição dos requisitos gerais do negócio • Requisitos de qualidade dos dados		• O líder de desenvolvimento aplicacional • O representante da vertente de negócio • O administrador de dados • O analista da	• Perder o sentido dos objectivos e âmbito do DW • Falhas no processo de análise • Falhas nas funcionalidade	• AI1.1 Definition and maintenance of business functional and technical requirements • PO8.2 IT standards and quality practices • AI1.2 Risk analysis report

• Requisitos específicos • Requisitos de infra-estrutura • Requisitos de reporting • Requisitos de dados fonte • Data Profiling		qualidade de dados • O administrador de metadados • O expert em sistemas de suporte à decisão	s • Aspectos da segurança ignorados	• AI1.3 Feasibility study and formulation of alternative courses of action • PO4.12 IT staffing • AI2.4 Application security and availability • AI2.9 Applications requirements management • DS11.1 Business requirements for data management

D.3.5 – Análise dos dados

Componentes a identificar	Actividades a realizar	Pessoas envolvidas	Riscos	Standards de avaliação
A **<u>análise dos dados</u>** deve abranger os dados fonte, a qualidade dos dados e as necessidades de limpeza nos dados.	• Análise das fontes externas de dados • Refinar o modelo lógico de dados • Análise da qualidade dos dados fonte • Resolução para as discrepâncias de dados • Especificações para os metadados • Especificações para a limpeza de dados	• O representante da vertente de negócio • O administrador de dados • O analista da qualidade de dados • O líder o desenvolvimento do ETL • O administrador de metadados • Os stakeholders • O expert em sistemas de suporte à decisão	• Criar datamarts não integrados ou sem valor acrescentado face aos sistemas operacionais • Tornar o DW numa gigantesca base de dados com todos os dados da organização • Não eliminar os problemas de integração de dados e criar bases de dados redundantes e inconsistentes. • Não conseguir montar uma aplicação verdadeiramente transversal a toda a organização • Retirar a utilidade do DW no seu papel de proporcionar melhor informação de suporte à decisão aos gestores da organização	• PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO4.7 Responsibility for IT quality assurance (QA) • PO4.9 Data and system ownership • DS11.6 Security requirements for data management

D.3.6 – Prototipagem

Componentes a identificar	Actividades a realizar	Pessoas envolvidas	Riscos	Standards de avaliação
• Objectivos • Âmbito e calendário • Entregáveis • Âmbito de cobertura do negócio • Ferramentas e métodos	• Analisar os requisitos de acesso • Determinar o âmbito do protótipo • Seleccionar as ferramentas para o protótipo • Preparar o propósito • Desenhar as	• O líder de desenvolvimento aplicacional • O representante da vertente de negócio • O administrador de bases de dados • Stakeholders • O expert em sistemas de suporte à decisão	• Erros de capacidade da base de dados • Erros na análise aplicacional e no desenho dos acessos • Incapacidade de as tecnologias seleccionadas não conseguirem cumprir os	• ITIL® V3: • SD4.3.5.7 Modeling and Trending

	queries e os reports • Construir o protótipo • Demonstrar	• Web master	requisitos de negócio • Custos e tempo de desenvolvimento do DW muito superiores ao previsto	
D.3.7 – Análise do repositório de metadados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• A utilização deste repositório • Os requisitos • Os requisitos de segurança • Os métodos de captura de metadados • Os meios de entrega de metadados • O staff de pessoal	• Os detentores dos dados e das aplicações • As características descritivas dos metadados • As regras e as politicas • As características físicas (exemplos: origem, localização, transformação) • Um mapa de prioridades (mandatórios, importantes ou opcionais)	• O administrador de dados • O administrador de metadados • O expert em sistemas de suporte à decisão	• Não permitir uma actualização expedita dos metadados face às mudanças • Os utilizadores/gestores de negócio não conseguem reconciliar os dados operacionais com os oriundos do DW • Dificuldades na compreensão dos dados oriundos do DW • Sentimento da comunidade gestora de que os dados do DW não são de confiança	• PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO3.1 Technological direction planning • PO4.6 Establishment of roles and responsibilities • AI1.1 Definition and maintenance of business functional and technical requirements • PO8.2 IT standards and quality practices

d) D.4 – Projecto

A fase de desenho do DW é composta pelo desenho da base de dados, o desenho do ETL e o desenho do repositório de metadados.

D.4 – Projecto				
D.4.8 – Desenho da base de dados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Considerações da arquitectura, desenho lógico e físico • Relatórios e consultas • Considerações de performance • O sistema de gestão de bases de dados • O staff de apoio	• Rever os requisitos de acesso • Determinar os requisitos de agregação e sumarização • Desenhar as bases de dados dimensionais de destino • Determinar os procedimentos de manutenção • Preparar o processo de monitorização e	• O líder de desenvolvimento aplicacional • O administrador de dados • O administrador de bases de dados • O líder o desenvolvimento do ETL	• Não aplicar as regras adequadas para as bases de dados • Má performance da aplicação • Pode ser a razão para falhar todo o projecto de informação de suporte à decisão	• PO2.3 Data classification scheme • PO2.1 Enterprise information architecture model • PO2.4 Integrity management • PO4.6 Establishment of roles and Responsibilities • PO4.9 Data and system ownership • PO10 Manage Projects

	melhoria da BD e das queries			

D.4.9 – Desenho do ETL				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• As ferramentas de suporte ao ETL • Definição da área de trabalho do ETL (Staging Área) • Determinar os fluxos do ETL • Considerações de performance • Regras de reconciliação • Métricas de qualidade dos dados	• Preparação para o processo ETL • Desenhar os programas de extracção, de transformação e carregamento • Avaliar as ferramentas de ETL • Mapear as especificações de transformação desde a fonte até ao destino	• O analista da qualidade de dados • O administrador de bases de dados • O líder o desenvolvimento do ETL • O expert em sistemas de suporte à decisão	• Trata-se de um passo fundamental do DW • Não operar as necessárias melhorias e limpeza dos dados da origem • Tratar dados sem qualidade, não integrados e não focalizados nos requisitos de negócio	• PO4.7 Responsibility for IT quality assurance (QA) • PO4.1 IT process Framework • PO3.1 Technological direction planning • PO2.2 Enterprise data dictionary and data syntax rules • PO2.4 Integrity management • PO7.3 Staffing of roles • PO8.3 Development and acquisition Standards • PO8.4 Customer focus • PO8.6 Quality measurement, monitoring and review • PO10 Manage Projects • DS5.4 User account management

D.4.10 – Desenho do repositório de metadados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Análise dos repositórios e produtos de metadados existentes • Levantamento de interfaces • Determinar o staff	• Desenhar a base de dados do repositório de metadados • Instalar e testar o repositório • Desenhar o processo de migração de metadados • Desenhar a aplicação de tratamento de metadados	• O líder de desenvolvimento aplicacional • O administrador de dados • O administrador de metadados	• Os utilizadores do DW não conseguem decifrar a origem dos dados • Impossível reconciliar com os dados fonte	• PO2.3 Data classification scheme • PO2.1 Enterprise information architecture model • PO2.4 Integrity management • PO4.6 Establishment of roles and Responsibilities • PO2.2 Enterprise data dictionary and data syntax rules • PO4.9 Data and system ownership • PO8.4 Customer focus • PO10 Manage Projects • DS5.4 User account management

e) D.5 – Construção

A fase de construção abrange o desenvolvimento do ETL, das aplicações de suporte à consulta e do repositório de metadados.

D.5 – Construção
D.5.11 – Desenvolvimento do ETL

Componentes a identificar	Actividades a realizar	Pessoas envolvidas	Riscos	Standards de avaliação
• Extracções dos dados fonte • Ferramentas de ETL • Dependências do processo ETL • Testes • Considerações técnicas	• Construir e testar os processos de ETL • Testar os processos de integração e regressão do ETL • Testar a performance, a qualidade e a aceitação do ETL	• O representante da vertente de negócio • O administrador de bases de dados • O líder o desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • O expert em sistemas de suporte à decisão • Responsáveis pelos testes	• Um processo de ETL devidamente desenvolvido e testado constitui o elemento chave do DW • Sem ETL não existe o DW	• AI2.7 Development of application Software • AI2.4 Application security and Availability • AI2.5 Configuration and implementation of acquired application software • AI2.9 Applications requirements Management • AI4.4 Knowledge transfer to operations and support staff • AI5.2 Supplier contract management • AI7.2 Test plan • AI7.5 System and data conversion
D.5.12 – Desenvolvimento aplicacional				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Resultados da prototipagem • Ferramentas de análise e acesso • Competências e formação • Âmbito e requisitos • Considerações de utilização de rede e internet • Considerações técnicas	• Determinar os requisitos finais do projecto • Desenhar os programas aplicacionais • Construir e testar os programas aplicacionais • Determinar as necessidades de treino do 'help desk', dos 'powerusers', dos analistas de negócio, etc	• O líder de desenvolvimento aplicacional • O representante da vertente de negócio • O administrador de bases de dados • O expert em sistemas de suporte à decisão • Responsáveis pelos testes	• Má qualidade dos olap de consulta • Fracas possibilidades de análises adicionais • Inexistência de visualização dos dados em gráficos e quadros • Impossibilidade de utilização em ambiente Web • Processo de suporte à tomada de decisão pouco potenciado	• AI2.7 Development of application Software • AI2.4 Application security and Availability • AI2.5 Configuration and implementation of acquired application software • AI2.9 Applications requirements Management • AI4.3 Knowledge transfer to end users • AI5.2 Supplier contract management • AI5.4 IT resources acquisition • AI7.1 Training • AI7.2 Test plan
D.5.13 – 'Data Mining'				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Considerar questões de marketing • Os dados • A ferramenta e técnicas de data Mining • O staff de apoio necessário	• Identificar o problema de negócio • Recolher os dados • Limpar e consolidar os dados • Preparar os dados • Construir o	• O representante da vertente de negócio • Expert em Data Mining • O administrador de bases de dados • O expert em sistemas de suporte à decisão	• Não conhecer os hábitos de consumo dos clientes • Não conseguir retirar conhecimento de negócio dos dados da organização • Perder a vantagem	• AI5.4 IT resources acquisition • AI7.1 Training • AI7.2 Test plan • AI2.4 Application security and Availability • AI2.5 Configuration and implementation of

	modelo analítico de dados • Interpretar os resultados do Data Mining • Validar externamente os resultados • Monitorizar o modelo analítico		competitiva de aumentar lucros, reduzir custos, inovar estratégias de produtos, expandir fatias de mercado • Perder clientes	acquired application software • AI2.9 Applications requirements Management • AI4.4 Knowledge transfer to operations and support staff
D.5.14 – Desenvolvimento do repositório de metadados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Produtos e aplicações de suporte • Customização do repositório de metadados • Pessoal e competências necessárias • Preparação para produção	• Desenvolver o repositório de metadados • Construir e testar o processo de migração de metadados • Construir e testar a aplicação de metadados • Testar os programas e funções associados ao repositório • Preparar o repositório para produção • Preparar a formação dos utilizadores do repositório	• O representante da vertente de negócio • O administrador de bases de dados • O administrador de metadados • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelos testes	• Desenvolver complexas aplicações de extracção de metadados para responder a pedidos de relatório de metadados • Utilização de ferramentas inadequadas para registar os metadados como por exemplo as ferramentas CASE	• AI4.4 Knowledge transfer to operations and support staff • AI2.5 Configuration and implementation of acquired application software • AI5.4 IT resources acquisition • AI7.1 Training • AI7.2 Test plan

f) D.6 – Implementação

A fase de implementação é composta pela implementação propriamente dita, pela entrada em produção e avaliação global dos resultados.

D.6 – Implementação				
D.6.15 – Implementação				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Preparação para a entrada em produção • Considerações sobre a segurança • Manutenção da base de dados • Formação • Suporte (help desk)	• Planear a implementação • Parametrizar o ambiente de produção • Instalar os componentes do DW • Definir o calendário de produção • Carregar as bases de dados de	• Responsáveis pelo desenvolvimento • O líder de desenvolvimento aplicacional • O expert em sistemas de suporte à decisão • Expert em Data Mining • O administrador de bases de dados • O líder o	• A implementação pode ficar instável, ser pouco robusto ou não cumprir os requisitos de segurança.	• PO10.11 Project change control • AI2.3 Application control and Auditability • AI3.4 Feasibility test environment • AI4.3 Knowledge transfer to end users • AI6.3 Emergency changes • AI7.1 Training

	produção • Preparar para dar suporte à produção	desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • O administrador de metadados • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento Web		• AI7.4 Test environment • AI7.7 Final acceptance test • DS8.1 Service desk • DS8.2 Registration of customer queries

D.6.16 – Produção e Avaliação

Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Revisão pós implementação • Métricas de desempenho • Planos da nova versão	• Preparar a revisão pós implementação • Organizar e conduzir reuniões para revisão pós implementação • Acompanhar a implementação das melhorias pós implementação	• O líder de desenvolvimento aplicacional • O responsável da vertente de negócio • Arquitecto de sistemas de suporte à decisão • O administrador de dados • Expert em Data Mining • Analista da qualidade de dados • O administrador de bases de dados • O líder o desenvolvimento do ETL • Responsáveis pelo desenvolvimento • Gestor de projectos • Stakeholders • Responsáveis pelo desenvolvimento Web	• Não recolher os conhecimentos suficientes para melhorar o projecto DW • Não detectar nem corrigir deficiências de desenvolvimento • Deixar crescer as pequenas insuficiências e deficiências a uma dimensão que se tornam irresolúveis	• PO10.13 Project performance measurement, reporting and monitoring • PO10.14 Project closure • AI2.10 Application software Maintenance • AI3.3 Infrastructure maintenance • AI6.4 Change status tracking and Reporting • AI7.8 Promotion to production • AI7.9 Post-implementation review • DS1.5 Monitoring and reporting of service level achievements • DS2.4 Supplier performance Monitoring • DS3.5 Monitoring and reporting • DS4.2 IT continuity plans • DS5.5 Security testing, surveillance and monitoring • DS5.11 Exchange of sensitive data • DS13.3 IT infrastructure monitoring • ME1.3 Monitoring method • ME1.4 Performance assessment • ME2.1 Monitoring of internal control Framework • ME2.5 Assurance of internal control • ME4.1 Establishment of an IT governance Framework • ME4.2 Strategic alignment

3.2.2 – P – Ambiente de Produção DW

Uma vez analisados os componentes do processo de desenvolvimento e implementação de um DW propomos neste ponto efectuar semelhante exercício para os componentes de controlo do processo de produção.

Assim, há que garantir que os fluxos de dados necessários para popular os modelos de dados do DW são suportados por procedimentos de extracção, transformação e entrega expeditos, consistentes e seguros e que estas funções são desempenhadas por técnicos conhecedores e preparados para lidar com situações de risco decorrentes do dia a dia do funcionamento do DW.

Para poder avaliar se os procedimentos de gestão e controlo do ambiente de produção do DW estão a ser realizados de forma adequada, procedeu-se à segmentação deste processo nos vários tópicos que o constituem, nomeadamente, os dados fonte; o 'back-room' ou aquisição; o 'front-room' ou acesso e os metadados.
Esta segmentação pretendeu incluir apenas os tópicos mais intimamente relacionados com o dia a dia da operação do DW.
Importa referir que as principais referências bibliográficas para estruturar e identificar em cada um dos tópicos os objectivos de controlo, os componentes, as actividades, as pessoas e os riscos, foram Kimball & Caserta, *The Data Warehouse ETL Toolkit*, publicado em 2004 e o artigo de Rodero & Toval & Piattini, *The audit of Data Warehouse*, publicado em 1999.

a) P.1 – Dados Fonte

Correspondem ao alimento do DW e abrangem a totalidade dos seus inputs. Os candidatos a dados fonte do DW compreendem toda a informação tratada pela organização e toda a informação tratada externamente que possa ter utilidade para o objecto de consulta dos utilizadores do DW.

- Assim, o DW deve considerar, para além da origem externa ou interna, dados fonte que podem ter origem em diferentes tipos de arquitecturas e formatos de ficheiros, por exemplo, ficheiros de Excel, de texto, oriundos de tabelas de bases de dados, entre outros. Adicionalmente, os dados fonte pode ter diferentes naturezas como sejam texto, imagem, vídeo, som, etc
- Para além disso, os dados fonte devem ser todos documentados quanto à origem e ao modelo de dados que os suporta
- Os procedimentos de segurança dos dados fonte devem ser igualmente documentados de modo a assegurar que lhes é atribuído um nível de segurança
- Assegurar a precisão e qualidade dos dados nas fontes como forma de manter a confiança do utilizador no DW (Pang, 2008)
- Ser selectivo quanto aos dados a incluir no DW (Pang, 2008)

P.1 – Dados Fonte				
P.1.1 – Dados Fonte				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Levantamento dos dados de input do DW • Tipos de fontes • Tipos de sistemas fonte e origem (interna ou externa) • Data profiling	• Documentar os dados, a sua origem, os modelos de dados • Mapear os dados fonte • Identificar e determinar os requisitos de segurança dos dados • Definir métodos de localização dos dados fonte necessários para o ETL • Examinar a qualidade, o âmbito e o contexto dos dados fonte	• Arquitecto de sistemas de suporte à decisão • O administrador de dados • Expert em Data Mining • Analista da qualidade de dados • O administrador de bases de dados • Os administradores das bases de dados operacionais	• Utilizar e trabalhar dados que não são importantes para o objecto de negócio em análise. • Utilizar dados incorrectos, sem qualidade para produzir um output de consulta consistente e fiável • Não ter um critério definido para a segurança dos dados	• PO2.1 Enterprise information architecture model • PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO2.4 Integrity management • PO4.1 IT process framework • PO4.9 Data and system ownership • PO4.14 Contracted staff policies and Procedures • PO10.5 Project scope statement • PO10.10 Project quality plan

			utilizando o mesmo procedimento para todos os níveis de informação • Não identificar as principais deficiências ao nível dos sistemas de captura de informação operacional	• DS5.11 Exchange of sensitive data • DS11.1 Business requirements for data management • DS11.6 Security requirements for data Management • ME3.1 Identification of external legal, regulatory and contractual compliance requirements

b) P.2 – Aquisição ou 'Back Room'

A aquisição constitui a primeira parte do 'back room', ou seja, o conjunto dos processos de extracção, limpeza, conformidade (sincronização e agregação) e entrega ou carregamento no 'front room'.
O 'back room' e o 'front room' do Data Warehouse estão física, lógica e administrativamente separados (ver Ilustração 4).
O processo de aquisição corresponde ao conjunto de procedimentos utilizados para extrair a informação dos sistemas originais, para efectuar as necessárias transformações e integrações, e finalmente para carregar os dados no modelo do DW definido como destino, normalmente os modelos dimensionais que compõem os Data Marts.
Assume-se assim que no 'back room' o acesso aos dados é estritamente proibido aos utilizadores, sendo o 'front room' sido criado exclusivamente para esse propósito.
Adicionalmente, é também certo que existe uma área no 'back room' destinada ao armazenamento temporário de dados (Staging área) que tem a finalidade de suportar os processos inerentes ao ETL.

- Assim, sempre que possível, o processo de aquisição de dados deve ser efectuado por ferramentas especializadas para tal
- O propósito do Staging Área deve ser o de servir o modelo final no front room, deste modo a sua arquitectura deve ser projectada de modo a que o processo de entrega seja directo e sem operações de conversão
- O processo de extracção deve ser acompanhada de informação necessária para sincronizar os dados no DW
- Devem ser implementados procedimentos de controlo das operações realizadas para adquirir os dados, como por exemplo, processos despoletados, o número de registos processados, registo de crescimento do DW, entre outros
- Os processos de limpeza devem satisfazer os requisitos mínimos de qualidade
- Na aquisição devem existir procedimentos de segurança adequados e sintonizados com as políticas de segurança dos sistemas fonte e com o plano de segurança do DW
- Deve existir uma metodologia explícita para assegurar a coerência dos dados após os procedimentos de limpeza e agregação
- Seleccionar cuidadosamente a estratégia do ETL (Pang, 2008)

P.2 – Aquisição				
P.2.2 – Extracção				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Sistemas e	• Criar um plano da	• O líder o	• Perder dados	• PO2.3 Data

arquitecturas lógica e física da fonte de dados • Hardware e protocolos de comunicação • Ferramentas e aplicações especializadas para a extracção • Tipo de dados a adquirir e modo de aquisição • Janela temporal para processar a aquisição • Políticas de segurança • Política e regras de integração dos dados • Documentação do processo	extracção • Identificar as fontes de dados • Analisar as fontes com uma ferramenta de Data Profiling • Validar cálculos e fórmulas • Segmentar o processo ETL assegurando pontos de recuperação em caso de falha • Identificar e extrair apenas os dados modificados desde a última extracção • Colocar na 'Staging Área' os dados extraídos • Extrair referências temporais dos dados (sincronização) • Assegurar os dados necessários para documentar os dados extraídos • Optimizar a performance do processo de modo a reduzir o tempo de processamento	desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • Os administradores das bases de dados operacionais • Analista da qualidade de dados • O líder de desenvolvimento aplicacional	durante a extracção • Extrair dados em duplicado ou dados já extraídos anteriormente • Dados sem referências temporais para sincronização • Dados defeituosos ou com diferentes critérios para efeitos de integração • Processo ETL demasiado pesado e intrusivo para as fontes • Falhas ou inexistência de procedimentos de segurança dos dados	classification scheme • PO4.9 Data and system ownership • PO4.10 Supervision • PO4.15 Relationships • PO6.1 IT policy and control environment • PO6.3 IT policies management • PO8.3 Development and acquisition Standards • AI3.2 Infrastructure resource protection and availability • AI6.1 Change standards and Procedures • DS2.1 Identification of all supplier Relationships • DS2.2 Supplier relationship Management • DS3.4 IT resources availability • DS5.5 Security testing, surveillance and monitoring • DS5.11 Exchange of sensitive data

P.2.3 – Limpeza

Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Regras de tratamento dos dados extraídos • Integridade referencial do sistema fonte • Objectivos de desnormalização	• Validar, substituir e corrigir dados • Transformar valores nulos, numéricos e alfanuméricos ajustando com as referências internas • Chekar a relação entre as entidades • Registar e sumarizar todos os erros ocorridos	• O líder o desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • O expert em sistemas de suporte à decisão • Analista da qualidade de dados	• Perda de coerência, abrangência, objectividade e correcção dos dados durante o processo de limpeza • Falhas no processo de filtragem dos dados extraídos	• PO2.4 Integrity management • PO4.7 Responsibility for IT quality assurance (QA) • PO8.6 Quality measurement, monitoring and review • AI2.7 Development of application Software • AI2.8 Software quality assurance

				• AI7.4 Test environment • AI7.5 System and data conversion

P.2.4 – Conformidade

Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Regras de cálculo, sincronização e agregação dos dados • Ferramentas e procedimentos de verificação dos dados • Modelo lógico dos dados no destino • 'Staging Área' • Conformidade das dimensões e dos factos	• Desnormalizar de acordo com as necessidades do modelo alvo • Sincronizar temporalmente os dados oriundos de diferentes fontes • Agregar dados de acordo com as granularidades pretendidas pelo modelo alvo • Efectuar os cálculos necessários • Dispor os dados de acordo com o modelo de destino e prontos a carregar • Validar os requisitos mínimos de qualidade dos dados	• O líder o desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • O expert em sistemas de suporte à decisão • Analista da qualidade de dados	• Cálculos mal efectuados • Dados dessincronizados • Agregações defeituosas • O formato dos dados após a conformidade não corresponder ao pretendido para o carregamento no DW • Dados não conformes com as regras de conformidade das dimensões e factos • Não ficar assegurada a qualidade mínima dos dados	• PO2.4 Integrity management • PO4.7 Responsibility for IT quality assurance (QA) • PO8.6 Quality measurement, monitoring and review • AI2.7 Development of application Software • AI2.8 Software quality assurance • AI3.4 Feasibility test environment • AI6.3 Emergency changes • AI7.4 Test environment • AI7.5 System and data conversion • ME3.5 Integrated reporting

P.2.5 – Carregamento

Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Plano de carregamento das tabelas • Modelo lógico do destino no 'front room' do DW • Ferramentas e aplicações especializadas para o carregamento • Políticas de segurança	• Assegurar a adequada entrega dos dados no formato do modelo de destino • Assegurar o cumprimento dos procedimentos de carregamento das dimensões e factos • Efectuar procedimentos de controlo da adequada entrega dos dados nos modelos • Optimizar a performance do processo de modo a reduzir o tempo de processamento • Assegurar a reposição da situação inicial em caso de falha no carregamento	• O líder do desenvolvimento do ETL • Responsáveis pelo desenvolvimento do ETL • O expert em sistemas de suporte à decisão • Analista da qualidade de dados • O líder de desenvolvimento aplicacional	• Os dados não ficam totalmente carregados nos modelos de destino • O procedimento falha e não é possível repor o estado inicial • O processo é muito pesado e demorado • O carregamento é efectuado de forma pouco segura	• PO6.1 IT policy and control environment • AI3.2 Infrastructure resource protection and availability • DS3.4 IT resources availability • ME1.4 Performance assessment • ME4.6 Performance measurement

c) P.3 – Acesso ou 'Front Room'

O acesso ao Data Warehouse processa-se exclusivamente na zona designada por 'front room' e é constituído pela colecção de processos destinados à captura e exploração da informação do DW, ou seja, é através destes processos que os utilizadores podem obter informação necessária para a tomada de decisão. O acesso é efectuado através da combinação de ferramentas standard e programas especializados.
Na realidade, a presença do DW e dos próprios Data Marts passa despercebida aos utilizadores pois estes acedem de um ponto único em que a visibilidade é apenas a que foi atribuída ao respectivo perfil de acesso.
Existem normalmente duas formas de apresentar a informação disponibilizada pelo DW:

- A forma tradicional em que a informação é disponibilizada em modelos dimensionais, em que o utilizador conhece a questão de partida e utiliza a consulta para validar essa questão, é também designada por consulta OLAP. Esta forma de estruturar os dados em modelos dimensionais visa servir os processos de consulta OLAP e as estruturas temáticas conhecidas por Data Marts, mas também podem servir outras aplicações como EIS/DSS[4], folhas de cálculo, painéis de comando (Dashboards), entre outras.
- A forma em que os dados são apresentados em ficheiros planos e completamente desnormalizados é também conhecida por consulta de Data Mining. Neste tipo de consulta a questão de partida é parcial ou completamente desconhecida, aplicando-se, neste caso, métodos estatísticos e matemáticos, como por exemplo, a regressão linear, as redes neuronais e as árvores de decisão, para encontrar clusters com padrões e regras próprios. Deste modo consegue-se extrair conhecimento acrescido dos dados, sendo normalmente o processo Data Mining efectuado com recurso à utilização de ferramentas especializadas.

Assim, os principais objectivos do controlo de acessos ao DW são os seguintes:

- Estender o universo de utilizadores do DW a todos os colaboradores especializados, não apenas aos decisores de topo (Pang, 2008)
- A construção de reports à medida não deve estar do lado do DW, ou seja, mesmo que sejam simples views dos dados a actividade de reporting deve ser orientado para os utilizadores
- Os relatórios e as ´queries' ao DW devem ser parametrizáveis e interactivas com vista a servir diversas áreas de utilização
- O utilizador apenas deve ter um ponto de acesso independentemente da estrutura física e lógica do DW
- O ambiente de acesso deve ser simples, intuitivo e completamente suportado por metadados actualizados
- A monitorização do processo de acessos deve ser permanente, especialmente nas tabelas mais consultadas, na sua dimensão, indexantes, frequência de acessos, etc. O objectivo é o de optimizar a performance, justificar o investimento e planear melhorias no sistema.
- O sistema de acessos deve cumprir todos os requisitos de segurança, especialmente no controlo de acessos, ou seja, nos processos de autenticação, autorização e 'audit trail'.

P.3 –Acesso				
P.3.6 –Acesso ou 'Front Room'				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Tipo de estrutura lógica e física dos modelos de dados do 'front room'	• Procurar integrar os diferentes tipos de acesso numa plataforma	• Responsáveis pelo desenvolvimento do ETL	• Acessos e views pouco interactivas e com poucas	• PO6.1 IT policy and control environment • PO6.5 Communication of IT

[4] EIS – Enterprise Information Systems; DSS – Decision Suport Systems

• Aplicações que acedem ao front room • Politicas de segurança	comum e única • Criar ambientes de consulta, simples, intuitivos, interactivos e suportados pelo repositório de metadados • Monitorizar os níveis e alvos de maior acesso e optimizar os respectivos processos • Implementar um sistema de controlo de acessos com todos os requisitos definidos pelas políticas de segurança	• O expert em sistemas de suporte à decisão • Analista da qualidade de dados • O líder de desenvolvimento aplicacional • Os administradores dos modelos dimensionais • Expert em Data Mining • O administrador de metadados • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento Web	possibilidades de personalizar a pesquisa • Consultas não suportadas por metadados não estando portanto definidas as características dos dados apresentados • Múltiplos sistemas de acesso • Tabelas de consulta mal parametrizadas com processos pesados e demorados • Controlo de acessos mal gerido com perfis inadequados e sem informação de auditoria	objectives and direction • PO7.2 Personnel competencies • PO8.4 Customer focus • AI2.4 Application security and Availability • AI4.2 Knowledge transfer to business Management • AI4.3 Knowledge transfer to end users • AI7.1 Training • AI7.7 Final acceptance test • DS1.3 Service level agreements • DS5.4 User account management • DS7.2 Delivery of training and education • DS8.1 Service desk • DS9.2 Identification and maintenance of configuration items • ME1.2 Definition and collection of monitoring data • ME3.2 Optimisation of response to external requirements • ME3.5 Integrated reporting

d) P.4 – Metadados

Como já foi referido no ponto 2.1.5 os metadados definem-se como ‘os dados sobre os dados’, no entanto, estes podem servir diferentes áreas e utilizadores e como tal, ter propósitos diferentes. (Kimball & Caserta, 2004) situando os metadados a dois níveis, os metadados de ‘back room’, que são direccionados aos técnicos responsáveis pelo ETL e por isso com informação mais técnica sobre a origem e os procedimentos técnicos, e os matadados de ‘front room’, mais direccionados para o utilizador final e por isso com uma componente de informação mais de negócio.

Assim, uma vez que os metadados têm uma importância central no DW, justifica-se que sejam estabelecidos objectivos de controlo adequados, como por exemplo:

- Deve existir e ser mantido actual um dicionário dos metadados da organização que inclua, pelo menos, uma definição das regras de negócio, das funções e das responsabilidades, dos elementos de consulta, dos algoritmos de agregação e do mapeamento dos dados
- Sistematizar de forma coerente os diferentes tipos de metadados como por exemplo, metadados de negócio, metadados técnicos e metadados de processos
- Os metadados devem ser geridos numa plataforma única e automatizada por uma ferramenta especializada, normalmente numa bases de dados autónoma

- Se os metadados coexistirem em diferentes ferramentas, estas devem partilhar e sincronizar-se entre si e apresentar a informação ao utilizador de uma forma conjunta
- Os metadados devem ser dinâmicos, evoluindo com os projectos e o ciclo de vida dos sistemas, sendo actualizados sempre que houver alterações que os afectem

P.4 – Metadados				
P.4.7 – Metadados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Tipos de metadados • Repositório de metadados • Definições de negócio • Definições técnicas e de processos • Fontes de dados • Modelos dimensionais	• Actualizar repositório de metadados sempre que houver alterações • Manter a gestão e manutenção dos metadados centralizado num único repositório • Permitir o acesso aos metadados nas ferramentas de acessos aos dados do DW • Assegurar a segurança e a confidencialidade dos metadados da organização	• O expert em sistemas de suporte à decisão • O administrador de metadados • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento do ETL • Responsáveis pelo desenvolvimento Web	• Não se perceber as características dos dados apresentados, como a sua origem, as regras de cálculo • Ocorrerem interpretações erradas pela inexistência ou indefinições das regras de negócio • Não existir um registo técnico dos dados e dos procedimentos realizados durante o ETL • Impossibilidade de estabelecer uma relação entre os dados do DW e os dados de fontes alvo de mudança	• PO2.3 Data classification scheme • PO4.9 Data and system ownership • PO6.5 Communication of IT objectives and direction • PO8.4 Customer focus • PO8.6 Quality measurement, monitoring and review • AI2.4 Application security and Availability • AI4.3 Knowledge transfer to end users • DS5.4 User account management • DS5.11 Exchange of sensitive data • DS7.2 Delivery of training and Education • DS9.2 Identification and maintenance of configuration items • DS11.6 Security requirements for data • DS13.4 Sensitive documents and output devices

3.2.3 – R – Requisitos transversais (DW/SI/TI)

O terceiro ponto do modelo foca-se nos objectivos de gestão e controlo de todos os componentes que se relacionam com o cumprimento de requisitos, quer estes sejam específicos do DW, como por exemplo os requisitos de negócio, quer sejam requisitos transversais a todos os Sistemas de Informação e Tecnologias de Informação, como por exemplo os requisitos de segurança.

a) R.1 – Requisitos de Negócio

Como foi referido no ponto 2.1.4, a definição dos requisitos de informação de negócio é um dos factores de sucesso mais importantes para o DW. É fundamental perceber as necessidades de informação da organização, quais os principais fluxos de dados que alimentam a cadeia de valor e proceder à sua avaliação e classificação.
Assim, a adequada definição dos requisitos de informação de negócio passa pela satisfação dos seguintes objectivos de controlo:

- Deve existir um dicionário actualizado de regras, termos e conceitos de negócio comum e transversal a toda a organização
- Deve existir uma relação entre os processos chave do negócio e as necessidades de informação de gestão
- Deve ser efectuada uma relação entre os processos de negócio e os indicadores de performance em vertentes como por exemplo a aquisição de matérias-primas, ordens de compra, transportes, inventário e contabilidade
- Os modelos devem ser orientados a processos de negócio e não a estruturas organizacionais, por exemplo, o modelo de vendas pode servir o departamento de vendas e o de marketing.
- Assegurar modelos consistentes, orientados aos processos de negócio e com o mínimo de fluxos redundantes.
- A granularidade dos modelos deve ser exactamente a que satisfaz a especificação, correspondendo o grão a uma linha da tabela de factos
- Devem ser seleccionadas as dimensões que servem os factos e apenas essas.
- Determinar factos numéricos que respondem as medições que se pretendem efectuar e que sejam coerentes com a granularidade da tabela de factos

R.1 – Requisitos de negócio				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Cadeia de valor do negócio ou da componente de negócio • Regras de negócio • Definição dos objectos chave do negócio • Modelo de negócio	• Realizar entrevistas aos utilizadores chave • Identificar a informação e as fontes de dados para satisfazer o utilizador • Avaliar a informação quanto ao valor, periodicidade, dificuldade de obtenção • Efectuar protótipos • Definir o âmbito	• O responsável pela vertente de negócio • Arquitecto de sistemas de suporte à decisão • O administrador de dados • O administrador de metadados • Os administradores das bases de dados operacionais • Os utilizadores chave	• O modelo não responder às necessidades de decisão do utilizador • O nível de detalhe do modelo (granularidade) ser insuficiente ou mais detalhada que o necessário • Criar uma infra-estrutura desfasada das necessidades de negócio • Confundir	• PO1.1 IT value management • PO1.2 Business-IT alignment • PO1.4 IT strategic plan • PO10.7 Integrated project plan • AI1.1 Definition and maintenance of business functional and technical requirements • DS1 Service level management framework

	de dados e informação de negócio		capacidades tecnológicas com necessidades de informação • Incongruências na informação por falta de definição de regras de negócio claras e transversais à organização	• DS1.6 Review of service level agreements and contracts • DS11.1 Business requirements for data management • ME4.2 Strategic alignment • ME4.3 Value delivery

b) R.2 – Requisitos de Conformidade

Por definição, estar conforme significa estar de acordo com princípios determinados, por exemplo, agir ou comportar-se de acordo com os standards aceites, normas, regulamentos e leis. (www.thefreedictionary.com).
Nos últimos anos as entidades reguladoras têm obrigado as organizações a níveis crescentes de exigência no que toca ao relato financeiro, nomeadamente na precisão e abrangência dos dados e respectivas evidências.
Neste âmbito, os requisitos de conformidade para o DW obrigam a que devam ser considerados os seguintes elementos:

- Estandardizar as definições dos dados da organização (Pang, 2008)
- Arquivo dos dados extraídos e dos dados trabalhados durante os processos de limpeza e conformidade
- Elementos de prova das transacções ocorridas durante os fluxos de dados que provocaram mudanças
- Documentação completa dos algoritmos que efectuaram o ajustamento e a revisão dos dados
- Prova de segurança das cópias de dados
- Preferencialmente, deve existir um plano de 'conformity assurance' em que se identifiquem todas as fontes regulamentares que tenham impacto no DW e os procedimentos para assegurar o seu cumprimento
- Os acessos ao DW devem ser feitos numa base somente de leitura

R.2 – Requisitos de conformidade				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Normas de segurança, privacidade e acessos • Normas de controlo do relato financeiro • Regulamentos das entidades supervisoras • Regras de sintaxe dos dados • Politicas de segurança • Informação e classificação da informação	• Registar e arquivar todas as alterações efectuadas aos dados desde a fonte até carregamento • Assegurar os procedimentos de controlo de confidencialidade, abrangência, exactidão, disponibilidade e acesso aos dados	• Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento do ETL • O expert em sistemas de suporte à decisão • Analista da qualidade de dados • O líder de	• Não conseguir demonstrar com evidências a veracidade dos resultados apresentados pelo DW • Estar em situação de incumprimento legal • Sofrer quebras de segurança por incumprimento dos requisitos de	• PO2.2 Enterprise data dictionary and data syntax rules • PO3.3 Monitor future trends and regulations • PO4.6 Establishment of roles and responsibilities • PO4.8 Responsibility for risk, security and compliance • PO4.14 Contracted staff policies and procedures • PO6.1 IT policy and control environment • PO6.4 Policy, standard and procedures Rollout • PO7.2 Personnel

• Descrição das hierarquias e responsabilidades dos intervenientes no processo DW	• Assegurar um processo de monitorização de novos regulamentos	desenvolvimento aplicacional • Os administradores das bases de dados operacionais • Responsáveis pelas consultas na vertente do negócio	segurança	competencies • PO7.6 Personnel clearance procedures • PO8.3 Development and acquisition Standards • PO9.6 Maintenance and monitoring of a risk action plan • AI5.2 Supplier Contract Management • AI6.1 Change standards and procedures • AI6.5 Change closure and documentation • DS5.2 IT security plan • ME3.1 Identification of external legal, regulatory and contractual compliance requirements

c) R.3 – Requisitos de Integração

A integração dos dados é um dos aspectos mais importantes no DW e em todo o universo TI pois, nos últimos anos, todos os sistemas têm trocar informação entre si e muitas vezes trabalhar em conjunto.
A integração dos dados deve ser pensada logo nos sistemas operacionais e portanto muito antes do DW, no entanto nem sempre isto se verifica.
No DW a integração dos dados tem lugar na parametrização e carregamento das dimensões conformes e dos factos conformes.

"Dimensões conformes significa estabelecer atributos comuns para dimensões homólogas oriundos de sistemas diferentes, para que possam integrar relatórios abrangentes e ser gerados de acordo com esses atributos.
Os factos conformes abrangem métricas transversais ao negócio com contributos de bases de dados díspares, como por exemplo os KPI (Key Performance Indicators), de modo que os resultados possam ser matematicamente comparáveis." (Kimball & Caserta, 2004)

Assim, de modo a avaliar se a integração de dados é efectuada de forma adequada, é necessário considerar os seguintes elementos:

- Para as dimensões principais, como por exemplo, cliente, produto, localização, transacção, calendário, deverá existir uma tabela mestre que faça um mapeamento actualizado dos critérios de definição utilizados em cada sistema fonte e quais os critérios que o DW assume como standard
- As tabelas de dimensões conformes devem ser comuns e utilizadas por várias tabelas de factos dentro do mesmo espaço de dados, o que significa que para cada dimensão apenas deve existir uma tabela
- Os factos conformes devem resultar da implementação das dimensões conformes e devem ser concordantes com a documentação que define as regras de negócio e as métricas associadas aos factos
- Os factos conformes devem permitir comparações entre si ou em expressões matemáticas como somatórios ou rácios

- Fornecer os dados em formato compatível com folhas de cálculo[5] (Pang, 2008)

R.3 – Requisitos de integração dos dados				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Data Profiling • Atributos das fontes • Regras de sintaxe dos dados • Informação e classificação da informação • Descrição das hierarquias e responsabilidades dos intervenientes no processo DW • Regras de negócio • Definição dos objectos chave do negócio	• Mapear em tabela mestre os atributos, as particularidades nas fontes e as regras de integração • Estabelecer atributos dimensionais comuns • Estabelecer métricas de negócio comuns • Definir um passo no ETL propositadamente para a integração dos dados • Estandardizar, corresponder e desduplicar	• Os administradores das bases de dados operacionais • Responsáveis pelas consultas na vertente do negócio • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento do ETL • O responsável pela vertente de negócio • Arquitecto de sistemas de suporte à decisão	• De existirem diferentes atributos para a mesma dimensão • Factos de negócio com nomenclaturas idênticas e significados diferentes • Erros ou impossibilidade de realizar cálculos entre atributos das tabelas de factos	• PO2.1 Enterprise information architecture model • PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO2.4 Integrity management • PO4.9 Data and system ownership • DS9.3 Configuration integrity review • DS11.1 Business requirements for data management • ME4.2 Strategic alignment

d) R.4 – Requisitos de Qualidade de Dados

Como referido no ponto 2.1.4 alínea f) uma definição de qualidade dos dados pode ser o nível em que é perceptível a veracidade e precisão dos dados, no entanto, o problema é que se trata de uma questão subjectiva pois qualidade elevada para uma pessoa pode ser considerada como pobre qualidade por outra. Isto torna a qualidade dos dados difícil de medir, mas não impossível nem desprovida de interesse.
Na realidade o esforço de analisar a qualidade dos dados e definir uma metodologia de a melhorar proporciona vantagens para a organização, devendo assegurar:

- Uma clara avaliação de quais são os principais problemas da qualidade dos dados antes do início do projecto DW
- Uma arquitectura melhorada para lidar com a qualidade dos dados
- Uma melhor avaliação das ferramentas utilizadas para tratar a qualidade dos dados
- Incluir nos processos ETL uma componente de avaliação e tratamento da qualidade dos dados
- Um repositório único para os metadados
- Um processo de envolvimento dos utilizadores na avaliação da qualidade dos dados
- Um processo de avaliação e reporte da qualidade final dos dados
- Assegurar a auditabilidade do processo de ETL (Pang, 2008)

R.4 – Requisitos de Qualidade de Dados

[5] A folha de cálculo ainda é a ferramenta de siuporte à decisão mais utilizado no mundo inteiro

Componentes a identificar	Actividades a realizar	Pessoas envolvidas	Riscos	Standards de avaliação
• Regras de negócio • Data Profiling • Regras de qualidade dos dados • Políticas de qualidade dos dados e informação • Documentação do ETL • Descrição das hierarquias e responsibilidades dos intervenientes no processo DW • Normas de controlo do relato financeiro • Informação e classificação da informação • Regras de sintaxe dos dados	• No desenvolvimento investigar os sistemas fonte e entrevistar os utilizadores chave • Assegurar que o repositório de metadados existe e é completo • As regras do ETL estão a ser devidamente documentadas e guardadas • As regras de negócio e de qualidade dos dados são aplicadas no processo ETL • As capacidades de reporte incluem os metadados • Estabelecer os níveis de qualidade de dados da organização, e quais os objectivos de qualidade a atingir no futuro • Manter o envolvimento dos utilizadores no projecto	• Sponsor do projecto DW • Utilizadores finais • Responsáveis pelo desenvolvimento do ETL • Arquitecto de sistemas de suporte à decisão • Analista da qualidade de dados • Os utilizadores chave	• Fraca qualidade dos dados faz aumentar o tempo e o esforço para a resolução dos problemas • Atrasos na entrega de relatórios • Riscos de falhas devido a inesperados problemas com a qualidade dos dados	• PO4.7 Responsibility for IT quality assurance (QA) • PO8.1 Quality management system • PO8.2 IT standards and quality practices • PO8.6 Quality measurement, monitoring and review • PO10.10 Project quality plan • AI2.8 Software quality assurance

e) R.5 – Requisitos de Segurança

A segurança e a privacidade da informação do DW devem ser considerada como uma preocupação primária e critica (Raymond & LeClerc, 2005)
De forma a assegurar a existência de procedimentos de segurança efectivos devem ser alcançados os seguintes objectivos de controlo:

- A organização deve ter uma política de segurança explicitamente suportada pela direcção executiva que defina uma orientação e suporte para todos os procedimentos de segurança
- Para ser efectiva, a política de segurança deve ser comunicada a todos os elementos com responsabilidades na organização
- A gestão de risco deve estar alinhada com a política de segurança
- De modo a restringir o acesso ao DW, devem-se controlar os acessos, autenticar os utilizadores e encriptar todos os dados classificados ou considerados sensíveis (Pang, 2008)
- O acesso ao DW deve ser efectuado numa filosofia apenas de leitura e deve ser pratica o limite de privilégio de acesso ao estritamente necessário para o exercício da função
- Os servidores e computadores do DW devem ser mantidos no centro de dados cujo acesso é restrito a indivíduos autorizados
- Devem ser estabelecidos procedimentos periódicos de revisão do controlo interno do DW
- Potenciar a auditabilidade do controlo interno do DW

R.5 – Requisitos de Segurança				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Políticas e procedimento	• Classificar e encriptar	• Arquitecto de sistemas de	• Procedimentos de não conformes	• PO2.3 Data classification scheme

s de segurança • Plano de comunicação das políticas de segurança • Gestão de Risco • Politica de acessos ao DW • Centro de dados	dados • Avaliar a protecção física e lógica do DW • Avaliar a capacidade de revisão do controlo interno do DW • Analisar as recomendaçõe s auditorias anteriores e seu cumprimento	suporte à decisão • Analista da qualidade de dados • Auditores SI • Sponsor do projecto DW • Utilizadores finais • Responsáveis pelo desenvolvime nto do ETL	com as politicas de segurança • Falta de formação sobre os procedimentos de segurança • Avaliação inadequada dos riscos • Utilização intrusiva do DW • Acesso físico ao hardware do DW não controlado • Procedimentos de controlo interno ineficientes ou desactualizados	• PO4.6 Establishment of roles and Responsibilities • PO4.8 Responsibility for risk, security and compliance • PO4.9 Data and system ownership • PO4.14 Contracted staff policies and Procedures • PO6.1 IT policy and control environment • PO6.2 Enterprise IT risk and control Framework • PO6.4 Policy, standard and procedures Rollout • PO7.4 Personnel training • PO9.4 Risk assessment • AI2.4 Application security and Availability • AI3.2 Infrastructure resource protection and availability • DS.4 Ensure Contínuos Service • DS5 Ensure Systems Security

f) R.6 – Requisitos de Utilização e Acessos

Os utilizadores do DW são analistas de negócio, gestores, etc, que pretendem melhorar a sua capacidade de decisão com base na informação que lhes é fornecida. O DW tem a finalidade de os servir, sendo os utilizadores finais os receptores dos processos, ferramentas e aplicações DW.
Entre os utilizadores existem os gestores com responsabilidade sobre toda a organização, que acedem ao DW como um todo, e os gestores que são responsáveis pela sua área restrita. Neste último caso a política de segurança restringirá o acesso deste utilizador apenas à parte do DW necessária para a sua tomada de decisão.
Assim, neste âmbito, os objectivos de controlo são os seguintes:

- Os utilizadores deverão ter um papel importante na definição dos requisitos do DW, devendo fazer parte deste projecto desde a sua concepção e aprovação até ao seu final
- Deve ser implementado um processo de controlo da utilização do DW por parte dos utilizadores que registe os níveis individuais de utilização e a sua evolução ao longo do tempo
- As necessidades de formação dos utilizadores devem ser identificadas e documentadas com base nas funcionalidades dos DW e nos conhecimentos dos utilizadores
- O âmbito de acessos deve respeitar a regra do privilégio mínimo, ou seja, nenhum utilizador individual deve ter um nível de autoridade nos acessos maior do que aquele que a sua função exige

Por outro lado, os acessos são constituídos pelos processos que se destinam a capturar e explorar o 'front room' do DW para que os utilizadores possam obter a informação que precisam para o seu processo de tomada de decisão. Esses acessos processam-se por uma combinação de ferramentas standard e programas especialmente desenhados.
Para o utilizador a percepção deve ser a de um único ponto de acesso ao DW, sendo os elementos do front-room, data marts e outros suportes de dados acedidos por esse ponto único de acesso.
Assim, no âmbito do controlo de acessos ao 'front room', colocam-se os seguintes objectivos:

- Potenciar o uso de portais Web para chegar a utilizadores distantes (Pang, 2008)
- Os reports e queries devem ser programáveis com capacidade para ser planeados, para correr de forma interactiva em função dos parâmetros, para ser distribuída para objectivos diversos, etc
- O utilizador deve perceber apenas um ponto de acesso para a informação, independentemente da sua origem e localização física
- O ambiente de acesso deve ser o mais simples e intuitivo possível e assistido completamente pelos metadados
- A monitorização dos acessos deve ser implementada, especialmente das queries e tabelas mais utilizadas, o tamanho das tabelas e indexantes, frequência de acessos, etc
- A monitorização de acessos deve alimentar os processos de melhoria contínua do sistema de acessos, nomeadamente da sua performance, de justificação do investimento e de planeamento futuro
- Os acessos devem cumprir todos os requisitos de segurança, em especial os processos de autenticação e autorização
- Os acessos devem garantir a confidencialidade dos outputs até que estes sejam entregues a um utilizador específico

R.6 – Requisitos de Utilização e Acessos				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Os utilizadores / decisores e as necessidades de informação • Política de autenticação e autorização • Níveis de responsabilidade e de utilização e acesso • Política de segurança • Ferramentas de front-end de consulta • Dicionário de metadados	• Definir as necessidades de formação dos utilizadores • Parametrização das contas e perfis de acessos • Controlar os tipos de acessos e níveis de utilização • Identificar as aplicações que acedem ao DW • Monitorizar as consultas e optimizar a performance das tabelas mais procuradas • Assegurar o acesso aos metadados	• Os utilizadores chave • Arquitecto de sistemas de suporte à decisão • Responsáveis pelo desenvolvimento do ETL • Utilizadores finais • Responsáveis pelo desenvolvimento do repositório de metadados • Responsáveis pelas consultas na vertente do negócio • O líder de desenvolvimento aplicacional	• Má definição de requisitos de negócio • Níveis de utilização descontrolada • Utilização deficiente por desconhecimento dos utilizadores • Utilizadores com níveis de acesso despropositado • Reports e consultas pouco parametrizáveis • Acesso aos dados estratificado e sem metadados • Optimização das tabelas pouco orientada para o nível e tipo de pesquisa • Violação da confidencialidade dos dados	• PO4.6 Establishment of roles and Responsibilities • PO4.11 Segregation of duties • PO7.1 Personnel recruitment and retention • PO7.8 Job Change and Termination • AI2.4 Application security and Availability • DS5.3 Identity management • DS5.4 User account management • DS5.5 Security testing, surveillance and monitoring • DS5.11 Exchange of sensitive data • DS8.1 Service desk • DS8.2 Registration of customer Queries • ME1.2 Definition and collection of monitoring data

g) R.7 – Requisitos de Infra-estruturas

Excepto para os users e o pessoal técnico, todos os outros intervenientes no DW requerem algum suporte de hardware para conseguirem atingir o seu propósito. Adicionalmente, é necessário providenciar a conexão entre os diferentes sistemas.
Esta infra-estrutura básica de hardware e comunicações, adicionada ao software de base, não difere muito daquilo que é necessário para todos os outros sistemas informáticos, apesar de ter algumas particularidades. Frequentemente a infra-estrutura do DW é partilhada por outros sistemas da organização.
Assim abaixo se descrevem os principais objectivos de controlo da infra-estrutura do DW:

- Utilizar uma arquitectura de módulos para facilitar a gestão da mudança (Pang, 2008)
- A infra-estrutura deve ser estável em todos os aspectos do projecto
- A escolha do hardware e software deve obedecer ao seguinte critério de objectivos: Fornecedores; Retorno; preço; facilidade de administração; conformidade com os standards da organização; capacidade e plataforma de conexão; outras ferramentas
- As ferramentas devem ter capacidade de suportar e entregar metadados
- A infra-estrutura deve no mínimo contemplar: 1 - hardware; ferramentas de extracção; limpeza; transformação e carregamento; 2 – Middleware; ferramentas de metadata; gestores de bases de dados, administração, segurança e acesso
- Todos os elementos da infra-estrutura devem possuir capacidade de crescimento para suportar o crescente carregamento do DW com tempos de resposta aceitáveis
- Um plano específico de segurança deve ser desenvolvido para garantir a continuidade da operação e disponibilidade do sistema. O plano deve considerar a segurança física e lógica, bem como as emergências, backups e procedimentos de recuperação.

R.7 – Requisitos de Infra-estruturas				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Hardware; ferramentas de extracção; limpeza; transformação e carregamento • Middleware; ferramentas de metadata; gestores de bases de dados, administração, segurança e acesso • Plano de segurança da infra-estrutura	• Avaliar o volume de dados a tratar • A volatilidade dos dados, dependendo da frequência de actualização • O numero de utilizadores, actividade e localização • O numero de processos de negócio • O tipo de utilização • A disponibilidade de produtos • A Disponibilidade dos técnicos • Os Recursos económicos disponíveis • Fornecedores; Retorno; preço; facilidade de administração • A conformidade	• Sponsor do projecto DW • Responsáveis pelo desenvolvimento do ETL • Arquitecto de sistemas de suporte à decisão • Responsável pelo desenvolvimento do repositório de metadados • Responsáveis pelo desenvolvimento do ETL • O líder de desenvolvimento aplicacional • O analista de qualidade de dados • Gestor de	• Não conseguir assegurar prestação eficiente face ao crescimento do DW • Ferramentas de administração e integração complexas • Não cumprimento de requisitos de segurança, conformidade e negócio • Faltar suporte técnico • Impossibilidade de recuperar informação em caso de erro	• PO3.1 Technological direction planning • PO3.2 Technology infrastructure plan • PO3.5 IT architecture board • PO4.1 IT process Framework • PO5.3 IT budgeting • PO7.2 Personnel competencies • PO7.4 Personnel training • PO8.3 Development and acquisition Standards • AI1.1 Definition and maintenance of business functional and technical Requirements • AI3 Acquire and Maintain Technology Infrastructure • DS2.4 Supplier performance Monitoring • DS3.3 Future performance and Capacity • DS5 Ensure Systems Security • ME1 Monitor and Evaluate IT Performance

	com os standards da organização	projecto		

h) R.8 – Requisitos de Funções e Responsabilidades

Como foi referido no ponto 2.3.5 alínea a), vários são os papéis e responsabilidades associados ao desenvolvimento e operação do DW. Estes elementos são indispensáveis pela coordenação, gestão e operacionalização do projecto para que este possa atingir os objectivos.
Associados às funções e responsabilidades existem objectivos de controlo a ser satisfeitos, como por exemplo:

- Dependendo da funcionalidade das aplicações, da infra-estrutura e da arquitectura do DW, a equipa de projecto deve definir que técnicos são capazes de cumprir as diferentes tarefas
- A grande maioria dos técnicos da equipa de projecto deve ter experiência neste tipo de projectos
- A equipa de projecto deve também ter experiência nas ferramentas de suporte ao projecto
- Caso não exista a experiência suficiente, deve ser estabelecido um plano de formação adequado

R.8 – Requisitos de Funções e Responsabilidades				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Funções e responsabilidades • Pessoal técnico • Recursos técnicos do projecto • Politica de segurança	• Segregação de funções • Acções de formação • Definição das funções e pessoal chave • Transmissão de conhecimento • Recrutamento e selecção	• Os utilizadores chave • Arquitecto de sistemas de suporte à decisão • Responsáveis pelas consultas na vertente do negócio • Sponsor do projecto DW • Gestor de projecto • Arquitecto de sistemas de suporte à decisão	• Falta de resposta por inadequação técnica da resposta • Falha no projecto por falta de experiencia dos técnicos • Ferramentas de suporte sem técnicos de apoio • Falha no projecto por falta de formação técnica	• PO4.6 Establishment of roles and • Responsibilities • PO4.7 Responsibility for IT quality assurance (QA) • PO4.8 Responsibility for risk, security and compliance • PO4.9 Data and system ownership • PO4.11 Segregation of duties • PO4.13 Key IT personnel • PO7.1 Personnel recruitment and retention • PO7.2 Personnel competencies • PO7.3 Staffing of roles • PO10.8 Project resources • AI4.4 Knowledge transfer to operations and support staff • DS7.1 Identification of education and training needs

i) R.9 – Requisitos de Latência, Armazenamento e Arquivo

Independentemente da arquitectura adoptada para o DW, a frequência de actualização dos dados para consulta dos utilizadores do DW, a capacidade de armazenamento de dados do DW e a periodicidade com que se deve proceder ao arquivo, são aspectos determinantes para as decisões a tomar, quer no planeamento e desenvolvimento, quer na operação do DW.

Assim, a latência pode variar de uma taxa de actualização mensal, semanal, diária (ou mais habitual) ou até online ou em tempo real (como é o caso do DW da Amazon), o que implica desenvolver processos de ETL com características adequadas, bem como diferentes periodicidades de acesso aos sistemas operacionais para a extracção.
O modo de armazenamento de dados é outro dos requisitos fundamentais da arquitectura do DW pois trata-se do local ou locais onde ficarão residentes os dados para consulta e exploração, ou seja, o elemento central para todos os outros componentes do DW quer sejam de hardware, software ou utilização.
Conforme a arquitectura DW adoptada, os processos de armazenamento variam, podendo ser processos de replicação total de um DW monolítico para um DW idêntico de exploração, processos de fragmentação física dos outputs do back room em DataMarts e ficheiros ou tabelas desnormalizadas, ou até pela fragmentação lógica, ou 'views' em que os dados temáticos parecem isolados mas na realidade continuam ligados a um DW comum.

Por fim, o armazenamento de dados históricos em dispositivos próprios com finalidade de arquivo e de segurança (recuperação dos dados em caso de falha no sistema), é outros dos aspectos importantes a considerar no ciclo de vida do DW.

Assim, com a finalidade de controlar estes aspectos, abaixo se definem alguns objectivos de controlo importantes:

- Os processos de replicação devem considerar a capacidade de armazenamento, o risco de falhas no sistema e a dependência da organização da informação processada
- Potenciar o DW para suportar o disaster recovery
- Os DataMarts complementam o DW e não devem ser vistos como uma alternativa a este
- Os DataMarts devem ter procedimentos de segurança pelo menos idênticos aos sistemas fonte
- A escolha do sistema gestor de base de dados do DW deve considerar as restrições de acesso, o volume armazenado e a taxa de crescimento do DW, bem como a conectividade com outros sistemas, a conformidade com os standards, entre outros
- Os dispositivos de monitorização do sistema gestor das bases de dados devem garantir a sua performance na operação do DW
- Os dispositivos de arquivo devem ser adequados para suportar os dados históricos recebidos do DW e eficazes na performance de repor os dados no DW em caso de falha
- A frequência de actualização do DW deve considerar as janelas de oportunidade dos sistemas fonte, bem como a capacidade de resposta do sistema gestor da base de dados do DW

R.9 – Requisitos de Latência, Armazenamento e Arquivo				
Componentes a identificar	**Actividades a realizar**	**Pessoas envolvidas**	**Riscos**	**Standards de avaliação**
• Capacidade de armazenamento • Arquitectura do DW • Politica de segurança SI • Tipos de sistemas gestores de bases de dados • Arquitectura TI da organização	• Avaliara a performance do sistema gestor de bases de dados • Avaliar e prever a taxa de crescimento do DW	• Os utilizadores chave • Arquitecto de sistemas de suporte à decisão • Responsáveis pelas consultas na vertente do negócio • Sponsor do projecto DW • Gestor de projecto	• Falhas no armazenamento de dados no DW • Falhas no arquivo ou recuperação de dados do DW • Falhas na gestão das bases de dados por incapacidade de resposta ao seu crescimento • Impossibilidade de	• PO2.1 Enterprise information architecture model • PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO3.2 Technology infrastructure plan • PO4.1 IT process Framework • PO4.9 Data and system ownership

• Arquitectura dos sistemas fonte e períodos de menor utilização • Requisitos técnicos de armazenamento e arquivo	• Perceber as necessidades de conectividade do DW • Definir o calendário de arquivo de dados • Testar o sistema de recuperação de dados	• Arquitecto de sistemas de suporte à decisão • O analista de qualidade de dados • Responsáveis pelo desenvolvimento do ETL • Responsável pelo desenvolvimento do repositório de metadados • Os administradores das bases de dados operacionais	assegurar os períodos de latência por indisponibilidade dos sistemas fonte • Falhas na conectividade do DW com os sistemas que o rodeiam • Perda de performance do DW por falta de monitorização	• PO5.2 Prioritisation within IT budget • PO6.2 Enterprise IT risk and control Framework • AI3.1 Technological infrastructure acquisition plan • DS3.1 Performance and capacity planning • DS4.8 IT services recovery and resumption • DS5.2 IT security plan • DS11.2 Storage and retention Arrangements • DS11.5 Backup and restoration • DS11.6 Security requirements for data Management • DS13.2 Job scheduling

3.2.4 – Metodologia de aplicação do modelo

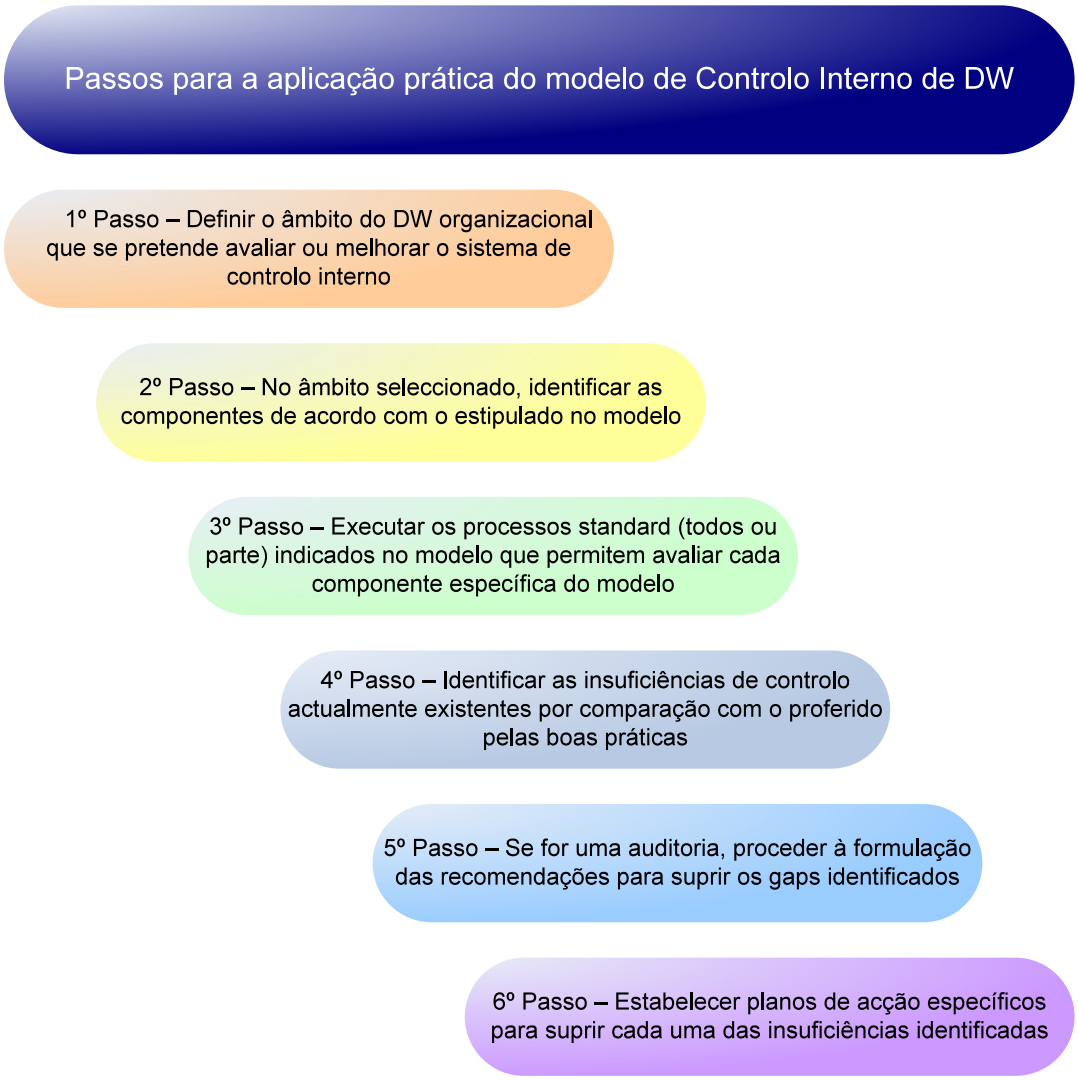

Ilustração 10 - Passos para a aplicação prática do modelo

4 – ESTUDO DE CASO: "OBJECTIVOS DE CONTROLO INTERNO DE UMA FERRAMENTA DE DATA WAREHOUSE"

A validação do modelo proposto no ponto anterior é efectuada através da realização de duas iniciativas distintas, nomeadamente, uma acção de auditoria ao DW de uma Instituição Financeira, realização de entrevistas aos principais responsáveis e intervenientes no DW de uma organização. No final deste capítulo apresentam-se as conclusões da validação efectuada, com especial enfoque nos contributos e impactos da utilização do modelo definido nesta investigação.

4.1 – Acção de Auditoria SI ao DW de uma Instituição Financeira

O estudo de caso abaixo apresentado tem o propósito de validar a aplicação prática do modelo definido nesta investigação, ou seja, se uma sistematização baseada em standards possibilita assegurar uma maior eficácia na avaliação do sistema de controlo interno do Data Warehouse e se com a utilização desta metodologia resulta mais fácil e intuitiva a realização de uma acção de auditoria interna a este tipo de sistemas de informação.
A acção de auditoria interna foi efectuada ao Data Warehouse de uma Instituição Financeira, tendo como recurso o modelo proposto.
Descrevem-se abaixo as características do DW auditado, os principais componentes analisados, a influência dos princípios estipulados no modelo e os resultados da avaliação efectuada.
De forma a preservar a confidencialidade da Instituição Financeira alvo do estudo, algumas especificidades dos dados apresentados foram propositadamente perturbadas, de modo a não ser possível identificar, nomeadamente, os nomes da instituição, os órgãos de estrutura e os intervenientes na acção de auditoria. Também foram alvo de perturbação todas as referências a empresas, marcas de software e hardware e outras tecnologias utilizadas nos processos de Data Warehousing testados.

4.1.1 – Caracterização do DW estudado

O Data Warehouse alvo deste estudo teve os seus primeiros desenvolvimentos há mais de 10 anos, tendo vindo a crescer desde essa altura, quer no âmbito do negócio, quer no número de Direcções clientes e número de utilizadores, quer em termos de tecnologias, de segurança e conformidade.

Tal como se pode observar na figura seguinte, a arquitectura do DW estudado identifica-se com o que Ariyachandra & Watson (2008) definiram por Hub and Spoke (Corporate Information Factory), tendo como característica fundamental a existência de um grande repositório central de recolha e validação de dados, sendo estes alvo de carregamento posterior em vários outputs de acesso e consulta dos utilizadores (ver ponto 2.1.3).

Trata-se portanto de uma estrutura DW de grandes proporções, tal como a dimensão da Instituição Financeira que serve, com um repositório com mais de 10 Tb, com procedimentos de extracção efectuados a todos os sistemas operacionais de negócio, sistemas de suporte e sistemas de outras empresas pertencentes ao Grupo da Instituição Financeira, oferecendo aproximadamente 300 relatórios (estáticos e dinâmicos) aos utilizadores.
Os procedimentos de ETL são suportados por mais de 6000 Jobs e as periodicidades variam deste os fluxos on-line até às extracções com periodicidades, diários, semanais, mensais e até anuais.

As Direcções utilizadoras do DW são bastante variadas, sendo a rede comercial e o Marketing, especialmente com o CRM, os clientes de maior utilização. No entanto, a Contabilidade e o Planeamento e Controlo também são utilizadoras assíduas da informação do DW.

O número de utilizadores (mais de 3000), as diversas áreas de utilização e a sensibilidade da informação obriga a que os procedimentos de segurança sejam uma prioridade do controlo interno do DW, nomeadamente a gestão de acessos e utilizadores.

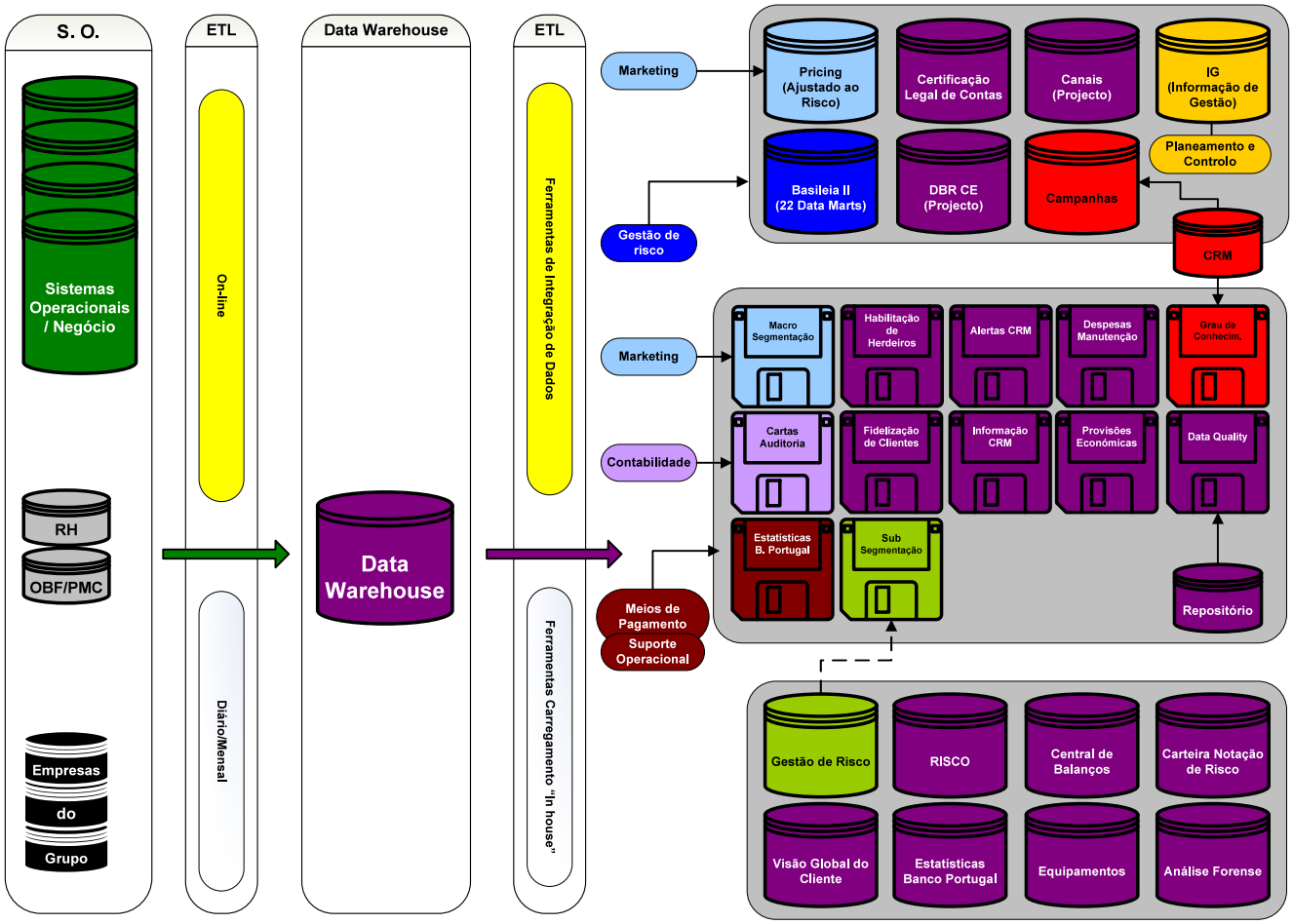

Ilustração 11 - Arquitectura do DW do Estudo de Caso

4.1.2 – Âmbito da auditoria ao DW

Antes de definir o âmbito do estudo de caso é importante enquadrar em que contexto se realizou a acção de auditoria ao DW abaixo descrita. Apesar de estarem instituídos no DW vários procedimentos controlo interno, nunca tinha sido formalmente realizada uma acção de auditoria interna a esta ferramenta.

Por ser a primeira intervenção desta natureza e devido à grande abrangência de negócio processada no DW, considerou a área de auditoria a sistemas de informação que a principal prioridade desta acção de auditoria seria a de avaliar a salvaguarda da informação corporativa e dos circuitos e procedimentos de segurança.

Assim, assegurar a confidencialidade, a integridade e a disponibilidade do DW, bem como garantir a segurança da informação, foram considerados os principais objectivos desta acção de avaliação, ou seja:

- Caracterização e análise, em termos orgânicos e funcionais, das diversas áreas que interagem com o DW
- Caracterização e análise dos recursos humanos que integram o subdomínio DW e seus acessos, com ênfase nas componentes de Autenticação e Autorização
- Caracterização e decomposição da arquitectura implementada no DW

- Caracterização e análise dos circuitos e dados de Input para o DW, assim como autorizações de acessos aos mesmos
- Caracterização e análise dos circuitos e dados de Output do DW, assim como autorizações de acessos aos mesmos
- Caracterização da informação em 'backup', controlo de acessos e prazos de retenção

O âmbito e objectivos desta auditoria incidem fundamentalmente na segurança da informação do DW, analisando os seus circuitos e acessos, de forma a possibilitar um conhecimento adequado dos riscos e impactos em todo este processo.

4.1.3 – Componentes auditadas, referenciais utilizados, deficiências e recomendações proferidas

Referenciando o âmbito da auditoria realizada ao DW no modelo definido por esta investigação, verifica-se que apenas uma parte deste último é abrangido, ou seja, apenas os componentes relacionados com os requisitos TI e uma pequena parte da Operação do DW, bem como os respectivos objectivos de controlo são considerados como referência:

- P.1 – Dados e Sistemas Fonte (P – Produção DW)
- P.2 – Aquisição ou Back Room (P – Produção DW)
- P.3 – Acesso ou Front Room (P – Produção DW)
- R.2 – Conformidade (R – Requisitos TI)
- R.4 – Qualidade de dados (R – Requisitos TI)
- R.5 – Segurança (R – Requisitos TI)
- R.6 – Utilização e Acessos (R – Requisitos TI)
- R.7 – Infra-Estruturas (R – Requisitos TI)
- R.9 – Armazenamento e Arquivo (R – Requisitos TI)

Componente avaliada	Referenciais de avaliação utilizados	Síntese das insuficiências e recomendações
• **Classificação da Informação (R.5 – Segurança)**	Política Global de Segurança de Informação da IF. CobiT® 4.1: PO2 (Definição da arquitectura de informação) PO4 (Definição dos processos, organização e relacionamentos em TI). Norma ISO/IEC 27002: 7.2 (Classificação da informação)	Não se encontra devidamente sistematizado o processo de classificação da informação do DW quanto à criticidade e confidencialidade. O sistema de classificação da informação deverá considerar níveis de confidencialidade, responsabilidade pelos dados, definições e controlos dos níveis de segurança.
• **Documentação do Processo (P.1 – Dados Fonte, P.2 – Aquisição)**	Aviso nº 5/2008 do Banco de Portugal: Artigo 22º Função de Auditoria Interna CobiT v4.1: PO2 (Definição da arquitectura de informação) PO4 (Definição dos processos, organização e relacionamentos em TI).	A documentação encontrada encontra-se desactualizada quanto a: - Arquitectura aplicacional e detalhe dos Datamarts Recomenda-se a actualização dos documentos referidos.
• **Procedimentos para a entrada de colaboradores (R.6 – Utilização e Acessos)**	Política Global de Segurança de Informação (PGSI): Ponto 6.15. CobiT® 4.1: PO4 (Definição dos processos, organização e relacionamentos em TI)	Os procedimentos de segurança para a entrada de novos colaboradores não são evidentes. O procedimento deverá abordar as seguintes matérias: Funções e responsabilidades; Políticas e procedimentos de segurança de

	PO7 (Gestão de recursos humanos de TI)	informação; Normativos internos
• **Procedimentos para a saída de colaboradores (R.6 – Utilização e Acessos)**	Política Global de Segurança de Informação (PGSI): Ponto 6.6. Regras e Procedimentos Básicos 7 (Utilizadores do SI), ponto 7.8 CobiT® 4.1: PO4 (Definição dos processos, organização e relacionamentos em TI) PO7 (Gestão de recursos humanos de TI) Norma ISO/IEC 27002: 8.3 (Cessação ou mudança de funções)	Os procedimentos de segurança para a saída de colaboradores não são evidentes. O procedimento de saída de colaboradores deverá abordar as seguintes matérias: Retirar de imediato os acessos aos SI; Assegurar a transmissão de conhecimento; Assegurar procedimentos de monitorização.
• **Assegurar a Continuidade de Serviços (R.5 – Segurança)**	CobiT® 4.1: DS4 (Assegurar a continuidade de serviços) Norma ISO/IEC 27002: 14.1 (Gestão da segurança de informação na continuidade de negócio)	Informação crítica não incluída no Plano de continuidade de negócio. *(Datamarts e clientes propositadamente ocultados)* Recomendam-se a inclusão desta informação no PCN e a reavaliação da criticidade da informação em conjunto com os Sponsors do DW
• **Contratos com Fornecedores (R.2 – Conformidade)**	CobiT® 4.1: AI5 (Obtenção de recursos de TI) PO4 (Definição dos processos, organização e relacionamentos em TI)	Alguns contratos de prestação de serviços estavam incompletos. Recomenda-se a sistematização dos tópicos a incluir obrigatoriamente em todos os contratos de prestação de serviços.
• **Contratos de Confidencialidade (R.2 – Conformidade)**	CobiT® 4.1: AI5 (Obtenção de recursos de TI) PO4 (Definição dos processos, organização e relacionamentos em TI) Norma ISO/IEC 27002: 6.1 (Organização interna)	Alguns colaboradores externos não tinham contratos de confidencialidade formalizados. Recomenda-se que a celebração de contratos de confidencialidade passe a ser obrigatório.
• **Data Marts e Ficheiros Output (P.3 – Acesso ou Front Room)**	CobiT® 4.1: DS11 (Gestão de dados) PO2 (Definição da arquitectura de informação)	Foram detectados casos de Data Marts e ficheiros de output sem evidências de utilização por parte dos clientes. Recomenda-se a reanálise juntamente com os clientes dos casos referidos
• **Componente Aplicacional (R.5 – Segurança)**	Política Global de Segurança de Informação (PGSI): Ponto 6.5 CobiT® 4.1: DS5 (Aquisição de recursos de TI); PO4 (Definição dos processos, organização e relacionamentos em TI) Norma ISO/IEC 27002: 10.1 (Responsabilidades e procedimentos operacionais)	Foram detectados casos de gestão não centralizada de acessos a aplicações do DW. Assegurar que a gestão de todos os acessos seja efectuado de modo centralizado e de acordo com a política de gestão de acessos.
• **Active Directory (R.6 – Utilização e Acessos)**	Política Global de Segurança de Informação (PGSI): Ponto 6.6 CobiT® 4.1: DS5 (Aquisição de recursos de TI); Norma ISO/IEC 27002:	Foram detectados dois casos de utilizadores com acessos sem que existisse uma responsabilidade. Rever os processos de criação, responsabilização e extinção de utilizadores, nomeadamente nos casos especiais associados à realização de testes.

	11.2 (Gestão de acessos de utilizadores)	
• **Backups (R.9 – Arquivo)**	CobiT® 4.1: DS11 (Gestão de dados)	
• **Gestão de Dispositivos Amovíveis (R.7 – Infra-Estruturas)**	Política Global de Segurança de Informação (PGSI): AI3 (Aquisição e Manutenção Infra-estrutura tecnológica); Norma ISO/IEC 27002: 10.7 (Manipulação de suportes amovíveis).	Foram detectados casos de equipamentos com portas USB activas. Recomenda-se a inibição destes acessos via USB, e uma política de permissões pontuais e apenas em casos estritamente necessários.
• **Acesso à informação (R.6 – Utilização e acessos)**	Política Global de Segurança de Informação (PGSI): DS5.4 (Gestão de acessos) Norma ISO/IEC 27002: 10.1 (Responsabilidades e procedimentos operacionais).	Os processos de atribuição de níveis de restrição no acesso à informação do DW não estava implementado. Os acessos aos dados devem ser atribuídos apenas a utilizadores que deles necessitem para a prossecução das suas actividades e funções. Recomenda-se uma análise exaustiva aos requisitos definidos pela política de acessos.

4.2 – Entrevista aos principais responsáveis e intervenientes no processo DW de uma organização

O processo de validação do modelo de controlo e auditoria interna de DW conclui-se com a realização de um conjunto de entrevistas aos principais responsáveis e intervenientes do processo DW da Instituição financeira auditada.

Os responsáveis questionados foram os seguintes:

- Responsável Área de Desenvolvimento (RD)
- Auditor responsável pela Auditoria SI (ASI)
- Responsável pela validação da informação do DW (RVI)

Abaixo se apresenta uma síntese dos resultados das entrevistas efectuadas:

Questão 1: *Vantagem para o processo de controlo interno do DW que poderá ocorrer com a implementação de um modelo semelhante ao proposto no ponto 3 desta dissertação?*

(RVI) As vantagens de tal implementação estarão dependentes dos meios disponibilizados e procedimentos criados com vista a operacionalizar o modelo de controlo interno do DW. A robustez de tal processo de controlo está também muito dependente do modelo de governance adoptado, ao nível da integração de todas as áreas SI/TI com políticas transversais, nomeadamente de segurança de informação e qualidade dos dados.

(RD) A utilização do modelo proposto traria certamente oportunidades de melhoria ao actual sistema de controlo interno do DW, especialmente ao nível das métricas de controlo, auditabilidade e risco de segurança (operacional).

(ASI) Sobre o capítulo 3, que li com agrado, verifico que identificas com precisão todas as áreas chaves do DW para a implementação de um controlo interno robusto, o que traria muitas vantagens face ao sistema actual.

Questão 2: *Vantagens que se poderão obter com a implementação do modelo proposto, no domínio da qualidade, precisão e enfoque dos dados, para quem é utilizador da informação produzida pelo DW?*

(RVI) Do ponto de vista prático, sempre que se proceda à inclusão de best practices no sistema de controlo interno do DW, consideramos um passo positivo para a sua melhoria.

(ASI) As vantagens da implementar um processo sistematizado de Controlo Interno no DW permitiria melhorar: - A eficácia e a eficiência das operações; - A fiabilidade da informação; - Conformidade com as leis e regulações aplicáveis.

Questão 3: *Quais as possibilidades de esta instituição poder utilizar o modelo proposto (ou parte dele), na revisão do processo de controlo interno ou em futuras de acções de auditoria ao DW?*

(RVI) e (RD) É uma possibilidade com todo o sentido.

(ASI) Esta tua metodologia é perfeitamente aplicável em futuras acções de auditorias ao DW, tendo só em atenção que o DW é considerado como um "grande elefante" de informação, e como tal terá que ser analisado "às fatias", não podendo ser efectuado tudo de uma só vez.

Questão 4: *Sugestões de melhoria do modelo de controlo interno apresentado (a considerar numa segunda iteração da metodologia de investigação).*

(RD) Na minha óptica, no grupo do desenvolvimento DW, o modelo deveria ter um componente específico para o controlo interno do Reporting/ Dashboards. Adicionalmente, devido à importância determinante, o enfoque dado ao tema do Data Quality devia ser ainda maior do que o atribuído no modelo, no entanto, porque se trata de um tópico muito abrangente, faria sentido melhorar o controlo interno da qualidade dos dados a todos os níveis dos sistemas e tecnologias de informação da organização, não apenas no processo DW.

Questão 5: *Outras sugestões / observações que considere pertinentes para esta investigação.*

(RVI) A implementação de controlos coloca um dilema de gestão sensível porque, se os controlos são muito rigorosos, existirão operações mais atípicas que poderão não ser aceites ou mal processadas pelos sistemas, por outro lado, se os controlos são muito abertos, os erros operacionais serão mais facilmente aceites e processados pelos sistemas sem que sejam detectados.

5 – CONCLUSÕES

5.1 – Âmbito e elementos de análise

Antes de efectuar um balanço final sobre esta dissertação, é importante destacar os três pilares de análise que serviram para identificar e sistematizar as principais componentes de controlo interno de um DW. Assim, foi com base nos conceitos e metodologias identificados no capítulo II que construímos um modelo de controlo interno específico para Data Warehouses, constituído por três tipos de componentes de controlo: Controlos inerentes à fase de desenvolvimento, controlos da fase de produção e controlos relacionados com requisitos de SI/TI em geral.
Para cada um dos componentes de controlo do DW identificados analisámos detalhadamente os objectivos de controlo associados ao seu bom desempenho, os riscos de não possuir um sistema de controlo adequado e, por fim, mapeámos com exaustão os processos de avaliação de controlo interno difundidos pelos standards e boas práticas, nomeadamente do Cobit® 4.1, do ITIL® V3 e do ISO/IEC 27002. Deste modo, conseguimos apresentar um compromisso que, em nossa opinião, permite implementar um sistema que assegura a optimização da gestão do DW, nomeadamente, alinhando o processo de controlo interno do DW com as melhores práticas internacionalmente difundidas e amplamente aceites.

5.2 – Modelos análogos de avaliação do controlo interno de DW

No processo de investigação desta dissertação muitos foram os elementos bibliográficos e artigos identificados que versam sobre as particularidades associadas ao DW, como por exemplo, a segurança da informação, a avaliação do grau de sucesso do DW, a qualidade dos dados, gestão dos riscos, os papéis e responsabilidades associados ao DW, as suas arquitecturas, entre outros.
No entanto, em todas as fontes de pesquisa bibliográfica, sempre que procurámos modelos específicos para exercer e avaliar o controlo interno do DW, os resultados foram semelhantes, ou seja, não foram encontrados quaisquer modelos de âmbito e propósitos semelhantes ao que foi construído nesta investigação.
Os únicos trabalhos identificados que apresentam modelos para a auditoria e controlo interno de DW foram, o artigo de 1999 da autoria conjunta de Rodero et al, bem como um outro artigo, não disponível para consulta, que tinha o título elucidativo de 'Modelo para auditoria de DW'.
As razões para não existirem trabalhos disponíveis desta natureza só se podem justificar por duas razões:
- Não tem sido efectuada investigação suficiente para produzir modelos deste género;
- Até poderão existir modelos para avaliação do controlo interno do DW, no entanto, devido às características práticas deste tipo de ferramentas, o acesso para consulta é limitado às empresas proprietárias, normalmente consultoras especializadas, e portanto, de acesso muito reservado.

5.3 – Metodologia de desenvolvimento de um modelo para avaliação do controlo interno

Tal como sucedeu no processo de desenvolvimento de conhecidos modelos ou Frameworks de avaliação de TI/SI, como por exemplo o Cobit® (actualmente na versão 4.1) e o ITIL® (na versão 3.0), o modelo proposto nesta investigação, para ter sucesso e ser amplamente aceite, terá de passar por um processo de desenvolvimento iterativo ou cíclico, com várias iterações de desenvolvimento. Isto possibilitará identificar oportunidades de melhoria do modelo e da eficiência dos resultados obtidos com a sua implementação.
Este tipo de desenvolvimento iterativo, efectuado através de ciclos de análise, desenvolvimento evolutivo e validação prática, é impossível realizar integralmente durante o período normal de vigência de uma investigação de mestrado. Ou seja, apesar de podemos afirmar que o modelo aqui

proposto corresponde à versão inicial (versão 1.0) e que cumpriu o seu primeiro ciclo completo de análise, desenvolvimento e validação, temos a convicção que este poderá evoluir e melhorar em determinados aspectos, o que significa admitir que o modelo apresentado não é definitivo e tem oportunidades de melhoria em futuros trabalhos de investigação.
Assim, as conclusões do estudo de caso terão de ser vistas como resultantes da validação prática da primeira versão do modelo de controlo interno para o DW, podendo estas conclusões servir de elementos a considerar em novos ciclos de investigação deste modelo.

5.4 – A abrangência do modelo e as necessidades de avaliação do DW

Tal como se advoga para os standards e as melhores práticas nas organizações, o modelo de avaliação do controlo interno do DW não é uma panaceia para todos os males, ou seja, o sucesso do modelo nas organizações está dependente da forma como se processa a implementação, como se gere a mudança e são actualizados os procedimentos em resposta às insuficiências identificadas.

"Os modelos têm maior utilidade quando são aplicados como um conjunto de princípios e vistos como um ponto de partida para o desenvolvimento de procedimentos específicos." (ITGI, 2008)

Isto significa que um modelo é um guião que pode ser utilizado integralmente ou parcialmente consoante as necessidades da organização, e que o nível de implementação ou influência desse modelo depende das necessidades específicas de cada organização. Por exemplo, o estudo de caso, apresentado no ponto IV desta investigação, visou avaliar alguns aspectos específicos do DW, nomeadamente o controlo de requisitos mais transversais como a segurança da informação ou a gestão de acessos.
Neste caso concreto a utilização do modelo proposto foi obviamente parcial, referindo-se apenas ao âmbito que se pretendia avaliar.
Tal como para o Cobit®, o ITIL® e o ISO/IEC, não faz sentido aplicar em simultâneo todas as particularidades definidas nesses modelos, pois eles foram concebidos para abranger o maior número possível de componentes de controlo, mas tal não significa que essas componentes ocorram todas ao mesmo tempo numa organização. Por exemplo, os requisitos de avaliação do desenvolvimento de novas funcionalidades no DW, não são os mesmos que os requisitos para avaliar a operação diária desta ferramenta. Por outro lado, estas fases do ciclo de vida do DW ocorrem certamente em timings próprios, ou seja, a necessidade de avaliação é que deve definir a utilização do modelo e não o contrário.

5.5 – Contributos do modelo para a melhoria do controlo interno e auditoria do DW

Apesar do âmbito do estudo de caso estar limitado à avaliação de alguns requisitos transversais do DW, e portanto, apenas ter sido utilizada uma parte do modelo, a entrevista realizada aos intervenientes foi praticamente consensual, ou seja, a aplicação prática de um modelo desta natureza pode acrescentar vantagens significativas para o processo de controlo interno do sistema do DW da organização, nomeadamente em duas grandes vertentes, no planeamento e exercício do controlo interno do DW, e na avaliação ou auditabilidade do processo de controlo interno do DW.

Abaixo se sintetizam as principais vantagens da implementação do modelo são:

- Clarificação e sistematização das principais componentes de controlo interno do DW, dos seus riscos, intervenientes, objectivos e standards de avaliação;
- Maior facilidade para avaliar os riscos e definir prioridades nas acções de controlo do DW;
- Facilidade em identificar e definir as métricas de avaliação dos objectivos de controlo;
- Maior eficácia das acções de auditoria na avaliação das acções de controlo interno;

- Maior aceitação das recomendações de auditoria, dada a universalidade das métricas utilizadas na avaliação;
- Maior clareza na definição e cumprimento dos planos de acção para suprir as deficiências de controlo interno.

5.6 – Trabalhos futuros

Com o propósito de dar sequência ao processo de melhoria contínua do modelo de controlo interno proposto por esta dissertação e, simultaneamente, contribuir para a sua divulgação junto de comunidades especializadas em controlar e implementar ferramentas SI/DW, foram identificadas novas oportunidades de trabalho, quer ao nível da realização de acções que permitam reforçar a validação prática do modelo, quer ao nível da recolha de opiniões criticas e outros elementos de análise que justifiquem uma nova iteração no processo de investigação, quer ainda, ao nível da divulgação do modelo junto de entidades especializadas, nomeadamente através do envio de artigos e candidaturas para concursos. Assim, destacam-se os seguintes trabalhos a realizar brevemente:

Validação do modelo: Apresentação do modelo junto de consultoras especializadas em implementação de DW e/ou controlo interno SI/TI com realização de entrevista.

Recolha de elementos de análise: Recolher opiniões críticas sobre o modelo proposto e outros elementos de análise pertinentes para proceder a um novo ciclo de análise e desenvolvimento do modelo de controlo interno para DW.

Divulgar o modelo: Dar conhecimento do modelo de controlo interno para DW através da realização de artigos destinados a organizações e eventos especializados na divulgação deste tipo de estudos, bem como participar em concursos especializados.

BIBLIOGRAFIA

- Ariyachandra, Thilini & Watson, Hugh (2006), *Wich Data Warehouse Architecture Is Most Sucessful?* Business Intelligence Journal; First Quarter 2006; ABI/INFORM Global, Pg.4-8
- Bacik, Sandy (2008), *Building an Effective Information Security Policy Architecture*, CRC Press, New York
- Banco de Portugal (2008), *Aviso nº5/2008 – Sistema de Controlo Interno das Instituições Financeiras*, Banco de Portugal, Lisboa (Jun 2008)
- Berry, Michael & Linoff, Gordon (1997), *"Data Mining Techniques"*, Wiley Computer Publishing, New York
- Cannon, David & Bergmann, Timothy & Pamplin Brady (2006), *CISA Certified Information Systems Auditor Study Guide*, Wiley Publishing Inc, Indianapolis
- Carneiro, Alberto (2004) *Auditoria de Sistemas de Informação*, FCA – Editora de Informática, Lisboa
- Cascarino, Richard (2007), *Auditors Guide to Information Systems Auditing*, John Wiley and Sons, New Jersey
- COSO Committee of Sponsoring Organizations of the Treadway Commission (1992) *Guidance on Monitoring Internal Control Systems – Internal Control – Integrated Framework*, COSO NY (http://www.coso.org/IC-IntegratedFramework-summary.htm)
- Crawford, Curtis (2007), *Compliance & conviction: the evolution of enlightened corporate governance*, Santa Clara, Calif
- DeLuccia, James (2008), *IT Compliance and Controls - Best Practices for Implementation*, John Wiley & Sons, New Jersey
- Dijcks, Jean-Pierre (2004), Integrating Data Quality into Your Data Warehouse Architecture, Business Intelligence journal (Spring 2004); ABI/INFORM Global, Pg.18-24
- ECIIA – European Confederation of Institutes of Internal Auditing (2008), *Banking Internal Auditing in Europe – Overview and recommendation by the Banking Advisory Group*, Erich Schmidt Verlag, Rome
- Hammergren, Thomas & Simon, Alan (2009), *Data Warehousing for Dummies*, Wiley Publishing, Indiana
- Luhn, Hans (October 1958); *A Business Intelligence System*; IBM Journal. http://www.research.ibm.com/journal/rd/024/ibmrd0204H.pdf. Retrieved 2008-07-10.
- Hubbard, Douglas (2009), *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons, New York
- Hwang, Mark & Xu, Hongjiang (2008), *A Structural Model of Data Warehousing Success*, The Journal os Computer Information Systems (Fall 2008); ABI/Inform Global, Pg.49-59
- IIA – The Institute of Internal Auditors (2009), *International Professional Practices Framework (IPPF)*, IIA Research Foundation (www.theiia.org)
- Inmon, Bill. (2001), *The Data Warehouse and Data Mining*, Communications of the ACM, New York

- IT Governance Institute (2007) *COBIT® 4.1 – Framework, Control Objectives; Management Guidelines; Maturity Models*, ITGI, New York
- IT Governance Institute (2008), *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit - A Management Briefing from ITGI and OGC*, ITGI/OGC, Rowling Meadows, USA, Norwich, NY
- ITSMF (2006) *Fundamentos Do Gerenciamento De Servicos Em TI/ Foundations of IT Service Management (Portuguese Edition)*, Jan van Bon Publishing, New York
- Kay, Emily (1997), *Dirty Data Challenges Warehouses*, Software Magazine (Out 1997); Abi/Inform Global, Pg.5-6
- Kimball, Ralph & Caserta, Joe (2004), *The Data Warehouse ETL Toolkit,* John Wiley & Sons, New Jersey
- Kimball, Ralph & Ross, Margy (2002), *The Data Warehouse Toolkit 2nd Edition – The Complete Guide to Dimensional Modeling*, John Wiley & Sons, New Jersey
- Marakas, George & O'Brien, James (2008), *Management Information Systems,* Irwin McGraw-Hill New York
- Moss, Larissa & Atre, Shaku (2003), *Business Intelligence Roadmap – The complete lifecycle for decision-support applications,* Addison-Wesley Information Technology Series, New York
- Olson, Jack (2003), *Data Quality: The accuracy Dimension*, Morgan Kaufmann Publishers, San Francisco
- Pang, Les (2008), *Best Practices in Data Warehousing*, University of Maryland, Encyclopedia of Data Warehousing and Mining (2008), IGI Global
- Raymond, Elson & LeClerc, Rey (2005); *Security and Privacy Concerns in the Data Warehouse Environment*; Business Intelligence journal (Summer 2005); ABI/INFORM Global, Pg.51-72
- Rodero, José & Piattini, Mario & Toval, José (1999*), The Audit of the Data Warehouse* , Partially granted by CICYT (Science aand Technology Joint Committee), Spanish Ministry os Education and Spanish Ministry of Industry, CEUR-WS/Vol-19, Pg.1-14
- Senft, Sandra & Gallegos, Fredrik (2009), *Information Technology Control and Audit*, CRC Press, New York
- Sherman, Richard (1997), *Metadata: the missing link*, Miller Freeman, Inc, San Francisco
- Silvers, Fon (2008), *Building and Maintaining a Data Warehouse*, CRC Press New York
- Steinberg, Randy (2006), *Measuring ITIL: Measuring, Reporting and Modeling - the IT Service Management Metrics That Matter Most to IT Senior Executives*, Trafford Publishing Oxford
- Watson, Hugh & Abraham, Dorothea & Chen, Daniel & Preston, David & Thomas, Dominic (2004), *Data Warehousing ROI: Justifying and Assessing a Data Warehouse*, Business Intelligence journal (Spring 2004); ABI/INFORM Global, Pg.8-15
- Weill, Peter & Ross, Jeane (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston

ANEXO I – Mapeamento CobiT@4.1 – ITIL@V3 – ISO/IEC 27002

Excerto das páginas 23 a 59 da publicação da IT Governance Institute (2008), *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit - A Management Briefing from ITGI and OGC*, ITGI/OGC, Rowling Meadows, USA, Norwich, NY

Appendix I—Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives

For the purposes of this mapping:

- Text shown in **bold** indicates where it is considered that ITIL V3 or ISO/IEC 27002:2005 provides the best supporting detail for a CobiT 4.1 control objective
- Text shown in *italics* indicates where it is considered that ITIL V3 or ISO/IEC 27002:2005 provides some supporting detail for a CobiT 4.1 control objective, but is not necessarily the primary reference

This mapping is not intended to be definitive or prescriptive and is only a guide. Links have been shown only at a high level, pointing to the relevant section in the other documents.

ISACA and the ITGI carry out continuous detailed research into the mapping between CobiT 4.1 and other standards and best practices. More information can be found at *www.isaca.org/cobit*.

CobiT 4.1 Domain: Plan and Organise (PO)			
PO1 Define a Strategic IT Plan			
IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO1.1 IT value management	• Business case • Allocation of funds • Benefit realisation • Business case evaluation	• **SS 2.2 What are services?** • **SS 3.1 Value creation** • **SS 3.4 Service structures** • **SS 4.4 Prepare for execution** • **SS 5.1 Financial management** • **SS 5.2 Return on investment** • **SS 5.3 Service portfolio management** • **SS 5.4 Service portfolio management method**	
PO1.2 Business-IT alignment	• IT alignment with business strategy • Bi-directional and reciprocal involvement in strategic planning	• **SS 2.1 What is service management?** • **SS 2.3 The business process** • **SS 2.4 Principles of service management**	
PO1.3 Assessment of current capability and performance	• Baseline of current performance • Assessment of business contribution, functionality, stability, complexity, costs, strengths and weaknesses	• **SS 4.4 Prepare for execution** • **CSI 5.2 Assessments**	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO1 Define a Strategic IT Plan *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO1.4 IT strategic plan	• Definition of IT goals • Contribution to enterprise objectives, budgets, funding, sourcing and acquisition strategy	• **SS 3.3 Service provider types** • **SS 3.5 Service strategy fundamentals** • **SS 4.1 Define the market** • **SS 4.2 Develop the offerings** • **SS 4.3 Develop strategic assets** • **SS 4.4 Prepare for execution** • **SS 5.5 Demand management** • **SS 6.5 Sourcing strategy**	
PO1.5 IT tactical plans	• IT initiatives • Resource requirements • Monitoring and managing benefit achievement	• **SS 4.4 Prepare for execution** • **SS 7.1 Implementation through the lifecycle** • **SS 7.2 Strategy and design** • **SS 7.3 Strategy and transitions** • **SS 7.4 Strategy and operations**	
PO1.6 IT portfolio management	• Defining, prioritising, managing programmes • Clarifying outcomes and scope of effort • Assigning accountability • Allocating resources and funding	• **SS 2.5 The service lifecycle** • **SS 3.4 Service structures** • **SS 4.2 Develop the offerings** • **SS 4.3 Develop strategic assets** • **SS 5.3 Service portfolio management** • **SS 5.4 Service portfolio management methods** • **SS 5.5 Demand management** • **SD 3.4 Identifying and documenting business requirements and drivers** • **SD 3.6.1 Designing service solutions** • **SD 3.6.2 Designing supporting systems, especially the service portfolio**	
PO2 Define the Information Architecture			
The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO2.1 Enterprise information architecture model	• Decision support analysis • Information architecture model maintained • Corporate data model	• *SD 3.6 Design aspects* • *SD 3.6.3 Designing technology architectures* • *SD 3.9 Service-oriented architecture* • *SD 3.10 Business service management* • *SD 5.2 Data and information management* • *ST 4.7 Knowledge management*	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO2 Define the Information Architecture *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO2.2 Enterprise data dictionary and data syntax rules	• Corporate data dictionary • Common data understanding	• *SD 5.2 Data and information management* • *SD 7 Technology considerations*	• *7.1.1.1 Inventory of assets* • *11.1.1 Access control policy*
PO2.3 Data classification scheme	• Information classes • Ownership • Retention • Access rules • Security levels for each information class	• *SD 5.2 Data and information management*	• *7.2.1 Classification guidelines* • *10.7.1 Management of removable data* • *10.8.1 Information exchange policies and procedures* • *10.8.2 Exchange agreements* • *11.1.1 Access control policy*
PO2.4 Integrity management	• Integrity and consistency of data	• *SD 5.2 Data and information management* • *ST 4.7 Knowledge management*	
PO3 Determine Technological Direction			
The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO3.1 Technological direction planning	• Available technologies • Enablement of IT strategy • Systems architecture • Technological direction • Migration strategies	• *SS 8 Technology and strategy*	• *5.1.2 Review of the information security policy* • *14.1.1 Including information security in the business continuity management process* • *14.1.5 Testing, maintaining and re-assessing business continuity plans*
PO3.2 Technology infrastructure plan	• Technological infrastructure plan • Acquisition direction • Economies of scale • Interoperability of platforms	• *SD 3.6.3 Designing technology architectures*	
PO3.3 Monitor future trends and regulations	• Business sector, industry, technology, infrastructure, legal and regulatory trends	• *SS 2.4 Principles of service management* • *SD 4.3.5.7 Modelling and trending*	• *6.1.1 Management commitment to information security*
PO3.4 Technology standards	• Technology forum • Product standards and guidelines		• *10.3.2 System acceptance* • *10.8.2 Exchange agreements* • *11.7.2 Teleworking*
PO3.5 IT architecture board	• Technology architecture guidelines and standards		• *6.1.1 Management commitment to information security*

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO4 Define the IT Processes, Organisation and Relationships			
An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO4.1 IT process framework	• IT process structure and relationships • Process ownership • Integration with business processes, enterprise portfolio management and business change processes	• SS 2.6 Functions and processes across the life cycle • SS 3.4 Service structures • SS 7.1 Implementation through the life cycle • SS 9.1 Complexity • SS 9.2 Co-ordination and control • SS 9.3 Preserving value • SS 9.4 Effectiveness in measurement • SD 2.4.2 Scope • SD 3.6.3 Designing technology architectures • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics • SD 4 Service design processes • SD 6.1 Functional roles analysis • SD 6.2 Activity analysis • SD 6.3 Skills and attributes • SD 6.4 Roles and responsibilities • SD 8 Implementing service design • SD App C Process documentation templates (example) • ST 3.2.7 Establish effective controls and disciplines • ST 4 Service transition processes • ST 6.1 Generic roles • ST 8 Implementing service transition • SO 2.3 Functions and processes across the life cycle • SO 4 Service operation processes • SO 4.6 Operational activities of processes covered in other life cycle phases • SO 6 Organising for service operation • SO 8 Implementing service operation • CSI 3.11 Frameworks, models, standards and quality systems • CSI 4 Continual service improvement processes	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO4 Define the IT Processes, Organisation and Relationships *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO4.1 IT process framework *(cont.)*		• **CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes** • **CSI 5.2 Assessments** • **CSI 5.5 The Deming Cycle** • **CSI 8 Implementing continual service improvement**	
PO4.2 IT strategy committee	• Board direction • IT governance • Strategic direction • Review of investments	• *SD 2.4.2 Scope*	
PO4.3 IT steering committee	• Prioritisation of investment programmes and project status tracking • Resource resolution • Monitor services		• *6.1.1 Management commitment to information security* • *6.1.4 Authorisation process for information processing facilities*
PO4.4 Organisational placement of the IT function	• Business significance of IT • CIO reporting lines	• *SS 6.1 Organisational development* • *SO 3.2.4 Reactive vs. proactive organisations*	• *6.1.1 Management commitment to information security* • *6.1.2 Information security co-ordination* • *6.1.3 Allocation of information security responsibilities* • *6.1.4 Authorisation process for information processing facilities*
PO4.5 IT organisational structure	• Organisational alignment with business needs	• **SS 2.6 Functions and processes across the life cycle** • **SS 6.1 Organisational development** • **SS 6.2 Organisational departmentalisation** • **SS 6.3 Organisational design** • **SS 6.5 Sourcing strategy** • **SS App B2 Product managers** • **SD 6.3 Skills and attributes** • **ST 4.2.6.8 Change advisory board** • **ST 6.2 Organisational context for transitioning a service** • **ST 6.3 Organisation models to support service transition** • **SO 3.1 Functions, groups, teams, departments and divisions** • **SO 3.2 Achieving balance in service operation** • **SO 3.3 Providing service** • **SO 6.1 Functions** • **SO 6.2 Service desk** • **SO 6.3 Technical management** • **SO 6.4 IT operations management** • **SO 6.5 Application management** • **SO 6.7 Service operation organisation structures**	• *6.1.1 Management commitment to information security* • *6.1.2 Information security co-ordination*

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO4 Define the IT Processes, Organisation and Relationships *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO4.6 Establishment of roles and responsibilities	• Explicit roles and responsibilities • Clear accountabilities and end-user authorities	• **SS 2.6 Functions and processes across the life cycle** • **SD 6.2 Activity analysis** • **SD 6.4 Roles and responsibilities** • **ST 6.3 Organisation models to support service transition** • **SO 6.6 Service operation roles and responsibilities** • **CSI 6 Organising for continual service improvement**	• *6.1.2 Information security co-ordination* • *6.1.3 Allocation of information security responsibilities* • *6.1.5 Confidentiality agreements* • *8.1.1 Roles and responsibilities* • *8.1.2 Screening* • *8.1.3 Terms and conditions of employment* • *8.2.2 Information security awareness, education and training* • *15.1.4 Data protection and privacy of personal information*
PO4.7 Responsibility for IT quality assurance (QA)	• Responsibility, expertise and placement of QA according to organisational requirements	• *CSI 6 Organising for continual service improvement*	
PO4.8 Responsibility for risk, security and compliance	• Ownership of IT risks in the business • Roles for managing critical risks • Enterprisewide risk and security management • System-specific security • Direction on risk appetite and acceptance of residual risks	• *SD 6.4 Roles and responsibilities*	• **6.1.1 Management commitment to information security** • **6.1.2 Information security co-ordination** • **6.1.3 Allocation of information security responsibilities** • **8.1.1 Roles and responsibilities** • **8.2.1 Management responsibilities** • **8.2.3 Disciplinary process** • **15.1.1 Identification of applicable legislation** • **15.1.2 Intellectual property rights (IPR)** • **15.1.3 Protection of organisational records** • **15.1.4 Data protection and privacy of personal information** • **15.1.6 Regulation of cryptographic controls** • **15.2.1 Compliance with security policies and standards**
PO4.9 Data and system ownership	• Enablement of business ownership of data • Decision making about information classification	• *SO 6.3 Technical management*	• *6.1.3 Allocation of information security responsibilities* • *6.1.4 Authorisation process for information processing facilities* • *7.1.2 Ownership of assets* • *9.2.5 Security of equipment off premises*

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO4 Define the IT Processes, Organisation and Relationships *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO4.10 Supervision	• Roles and responsibilities • Review of key performance indicators (KPIs)		• *6.1.2 Information security co-ordination* • *6.1.3 Allocation of information security responsibilities* • *7.1.3 Acceptable use of assets* • *8.2.1 Management responsibilities*
PO4.11 Segregation of duties	• Proper execution of roles and responsibilities • Avoidance of compromise of critical processes	• *ST 3.2.13 Assure the quality of the new or changed service* • *SO 5.13 Information security management and service operation*	• *8.2.1 Management responsibilities* • *10.1.3 Segregation of duties* • *10.1.4 Separation of development, test and operational facilities* • *10.6.1 Network controls*
PO4.12 IT staffing	• Number and competency; requirements evaluation	• *SO 6.2 Service desk*	
PO4.13 Key IT personnel	• Key roles defined • Minimising staff dependency		
PO4.14 Contracted staff policies and procedures	• Knowledge and compliance of policies • Information assets protected		• *6.1.5 Confidentiality agreements* • *6.2.1 Identification of risks related to external parties* • *6.2.3 Addressing security in third-party agreements* • *9.1.5 Working in secure areas* • *15.1.5 Prevention of misuse of information processing facilities*
PO4.15 Relationships	• Optimal co-ordination • Communications and liaison	• *SO 4.2.5.9 Develop contracts and relationships*	• *6.1.6 Contact with authorities* • *6.1.7 Contact with special interest groups*
PO5 Manage the IT Investment			
A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realisation of business benefits and the ROI of IT-enabled investments.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO5.1 Financial management framework	• Portfolio management • Investment and cost management of IT assets	• *SS 3.1 Value creation* • *SS 5.1 Financial management* • *SS 5.2 Return on investment* • *SS App A Present value of an annuity*	
PO5.2 Prioritisation within IT budget	• Allocation of IT resources • Optimisation of ROI	• *SS 5.2 Return on investment* • *SS 5.3 Service portfolio management* • *SS 5.4 Service portfolio management methods*	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO5 Manage the IT Investment *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO5.3 IT budgeting	• Budgeting process • Ensuring that budget is in line with investment portfolio of programmes and services • Budget review and approval	• **SS 5.2.2 Return on investment**	• *5.1.2 Review of the information security policy*
PO5.4 Cost management	• Comparison of costs to budgets • Cost reporting • Remediation of cost deviations from plan	• **SS 5.1 Financial management (esp. 5.1.2.7)**	• *5.1.2 Review of the information security policy* • *13.2.2 Learning from information security incidents*
PO5.5 Benefit management	• Benefits monitoring and analysis • Improvement of IT's contribution • Maintenance of business cases	• *SS 2.2 What are services?* • *SS 5.1 Financial management* • *SS 5.2 Return on investment* • *ST 4.4.5.10 Review and close service transition* • *ST 4.4.5.8 Early life support*	
PO6 Communicate Management Aims and Direction			
Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO6.1 IT policy and control environment	• Management philosophy and operating style • Integrity, ethics, competences, accountability and responsibility • Culture of value delivery while managing risks	• *SS 6.4 Organisational culture*	• *5.1.1 Information security policy document control framework* • *13.2.1 Management of information security incidents and improvements*
PO6.2 Enterprise IT risk and control framework	• Promulgating and controlling policy • Alignment with enterprise risk and control		• **5.1.1 Information security policy document control framework** • **6.2.2 Addressing security when dealing with customers** • **7.1.3 Acceptable use of assets** • **8.2.2 Information security awareness, education and training** • **8.3.2 Return of assets** • **9.1.5 Working in secure areas** • **9.2.7 Removal of property** • **10.7.3 Information handling procedures** • **10.8.1 Information exchange policies and procedures** • **10.9.3 Publicly available information** • **11.1.1 Access control policy**

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO6 Communicate Management Aims and Direction *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO6.2 Enterprise IT risk and control framework (cont.)			• **11.3.1 Password use** • **11.3.2 Unattended user equipment** • **11.3.3 Clear desk and clear screen policy** • **11.7.1 Mobile computing and communications** • **11.7.2 Teleworking** • **12.3.1 Policy on the use of cryptographic controls** • **15.1.2 Intellectual property rights (IPR)** • **15.1.5 Prevention of misuse of information processing facilities** • **15.2.1 Compliance with security policies and standards**
PO6.3 IT policies management	• Creation of policies • Policy intent and roles and responsibilities		• *5.1.1 Information security policy document* • *5.1.2 Review of the information security policy* • *6.1.1 Management commitment to information security* • *8.1.1 Roles and responsibilities*
PO6.4 Policy, standard and procedures rollout	• Distribution and enforcement of policy to staff		• *6.1.1 Management commitment to information security* • *6.1.8 Independent review of information security* • *6.2.3 Addressing security in third-party agreements* • *8.2.2 Information security awareness, education and training*
PO6.5 Communication of IT objectives and direction	• Awareness and understanding of business and IT objectives	• *ST 5.1 Managing communications and commitment* • *SO 3.6 Communication*	• *5.1.1 Information security policy document* • *6.1.1 Management commitment to information security* • *6.1.2 Information security co-ordination*
PO7 Manage Human Resources			
A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO7.1 Personnel recruitment and retention	• An enterprise policy based on personnel recruitment and promotion practices • Skills mapped to organisational goals		• *8.1.1 Roles and responsibilities* • *8.1.2 Screening* • *8.1.3 Terms and conditions of employment*
PO7.2 Personnel competencies	• Definition and of core competencies • Verification of competencies		• *8.1.1 Roles and responsibilities* • *8.2.2 Information security awareness, education and training*

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO7 Manage Human Resources *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO7.3 Staffing of roles	• Defined roles and responsibilities • Adequate level of supervision		• *8.1.1 Roles and responsibilities* • *8.1.3 Terms and conditions of employment* • *8.2.1 Management responsibilities*
PO7.4 Personnel training	• Organisational induction and ongoing training to raise technical and management skill levels	• *SD 6.3 Skills and attributes*	• *8.2.2 Information security awareness, education and training*
PO7.5 Dependence upon individuals	• Addressing resource availability of key functions • Knowledge capture • Succession planning		
PO7.6 Personnel clearance procedures	• Security clearance dependent upon sensitivity of position		• *8.1.2 Screening*
PO7.7 Employee job performance evaluation	• Performance evaluation reinforced by award system		• *8.2.2 Information security awareness, education and training*
PO7.8 Job Change and termination	• Knowledge transfer and reassignment so as to minimise risks		• *8.2.3 Disciplinary procedures* • *8.3.1 Termination responsibilities* • *8.3.2 Return of assets* • *8.3.3 Removal of access rights*
PO8 Manage Quality			
A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.1 Quality management system	• Standard approach aligned to business requirements covering quality requirements and criteria • Policies and methods for detecting and correcting quality non-conformance	• *SS 7.5 Strategy and improvement* • *ST 4.4.5.3 Build and test*	
PO8.2 IT standards and quality practices	• Standards and procedures to guide meeting QMS	• *SS 7.5 Strategy and improvement* • *ST 3.2.13 Assure the quality of the new or changed service* • *ST 4.5 Service validation and testing (ITIL is not just focused on ST, but on ongoing test of the service)* • *CSI App A Complementary guidance*	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO8 Manage Quality *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.3 Development and acquisition standards	• Life cycle standards for deliverables	• *SS 6.5 Sourcing strategy* • *SD 3.5 Design activities* • *SD 3.6 Design aspects* • *SD 3.9 Service-oriented architecture* • *SD 3.11 Service design models* • *SD 5.3 Application management* • *SD 7 Technology considerations* • *ST 3.2.3 Adopt a common framework and standards* • *ST 4.1.4 Policies, principles and basic concepts* • *ST 4.1.5.1 Transition strategy*	• **6.1.5 Confidentiality agreements** • **6.2.3 Addressing security in third-party agreements** • **12.5.5 Outsourced software development**
PO8.4 Customer focus	• Customer-oriented QMS • Roles and responsibilities for conflict resolution	• **SS 5.5 Demand management** • **SD 4.2.5.4 Collate, measure and improve customer satisfaction** • **ST 3.2.6 Establish and maintain relationships with stakeholders**	
PO8.5 Continuous improvement	• Communication processes promoting continuous improvement	• **SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall security information officer (SIO)** • **SO 5.14 Improvement of operational activities** • **CSI 1 Introduction** • **CSI 2 Service management as a practice** • **CSI 3 Continual service improvement principles** • **CSI 4.1 The seven-step improvement process** • **CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes** • **CSI 4.4 Return on investment for CSI** • **CSI 4.5 Business questions for CSI** • **CSI 5 Continual service improvement methods and techniques** • **CSI 5.1 Methods and techniques** • **CSI 5.5 The Deming Cycle** • **CSI 5.6 CSI and other service management processes** • **CSI 5.6.7 Summary** • **CSI 6 Organising for continual service improvement** • **CSI 8 Implementing continual service improvement** • **CSI 9 Challenges, critical success factors and risks**	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO8 Manage Quality *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.6 Quality measurement, monitoring and review	• Monitoring compliance to QMS and value of QMS	• **CSI 5.2 Assessments** • **CSI 5.3 Benchmarking** • **CSI 5.4 Measuring and reporting frameworks**	
PO9 Assess and Manage IT Risks			
A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO9.1 IT risk management framework	• Alignment to enterprise risk framework	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
PO9.2 Establishment of risk context	• Internal and external context and goals of each assessment	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation* • *SD 4.5.5.2 Stage 2—Requirements and strategy*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
PO9.3 Event identification	• Important threats exploiting vulnerabilities having negative business impact • Risk registry	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *ST 9 Challenges, critical success factors and risks* • *CSI 5.6.3 IT service continuity management*	• **13.1.1 Reporting information security events** • **13.1.2 Reporting**
PO9.4 Risk assessment	• Likelihood and impact of all identified risks • Qualitative and quantitative assessment • Inherent and residual risk	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *SD 8.1 Business impact analysis (not in detail)* • *ST 4.6 Evaluation*	• **5.1.2 Review of the information security policy** • **14.1.2 Business continuity and risk assessment**
PO9.5 Risk response	• Cost-effective controls mitigating exposure • Risk avoidance strategies in terms of avoidance, mitigation or acceptance	• *SS 9.5 Risks* • *SD 4.5.5.3 Stage 3—Implementation* • *ST 4.6 Evaluation*	
PO9.6 Maintenance and monitoring of a risk action plan	• Prioritising and planning risk responses • Costs, benefits and responsibilities • Monitoring deviations	• *SS 9.5 Risks* • *SD 4.5.5.4 Stage 4—Ongoing operation*	

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO10 Manage Projects			
A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO10.1 Programme management framework	• Identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling all investment programmes of projects • Co-ordination, interdependence, resource conflicts		
PO10.2 Project management framework	• Scope and boundaries of managing projects and method to be adopted		
PO10.3 Project management approach	• Approach commensurate with size, complexity and requirements of each project • Project governance structure • Project sponsors	• *ST 3.2 Policies for service transition*	
PO10.4 Stakeholder commitment	• Commitment and participation of stakeholders	• *ST 3.2.6 Establish and maintain relationships with stakeholders* • *ST 3.2.12 Ensure early involvement in the service life cycle*	
PO10.5 Project scope statement	• Approval of nature and scope of project	• *SD 3.4 Identifying and documenting business requirements and drivers* • *SD 3.5 Design activities*	
PO10.6 Project phase initiation	• Approval of initiation of each phase • Programme governance decisions		
PO10.7 Integrated project plan	• Integrated plan covering business and IT resources • Activities and interdependencies between projects	• *SD App D Design and planning documents and their contents*	
PO10.8 Project resources	• Responsibilities, relationships, authorities, and performance criteria of project team • Planning procurement of resources	• *ST 3.2.11 Proactively manage resources across service transitions*	
PO10.9 Project risk management	• Systematic process for planning, identifying, analysing, responding to, monitoring and controlling risks		
PO10.10 Project quality plan	• Defined and agreed-upon quality management plan and QMS		
PO10.11 Project change control	• Change control system for each project (cost, schedule, scope, quality)	• **ST 3.2.10 Anticipate and manage course corrections**	
PO10.12 Project planning of assurance methods	• Assurance tasks required to support accreditation		

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*			
PO10 Manage Projects *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO10.13 Project performance measurement, reporting and monitoring	• Measuring project performance against key criteria • Assessing deviations, recommending and implementing remedial actions		
PO10.14 Project closure	• Project stakeholders' review of achievement of results and benefits • Communicating outstanding actions and documenting lessons learned		

CobiT 4.1 Domain: Acquire and Implement (AI)			
AI1 Identify Automated Solutions			
The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI1.1 Definition and maintenance of business functional and technical requirements	• Identifying, prioritising and specifying requirements for all initiatives related to investment programmes	• **SS 7.5 Strategy and improvement** • **SS 8.1 Service automation** • **SD 3.2 Balanced design** • **SD 3.3 Identifying service requirements** • **SD 3.4 Identifying and documenting business requirements and drivers** • **SD 3.5 Design activities** • **SD 3.6.1 Designing service solutions** • **SD 3.6.2 Designing supporting systems, especially the service portfolio** • **SD 3.6.3 Designing technology architectures** • **SD 3.6.4 Designing processes** • **SD 3.6.5 Design of measurement systems and metrics** • **SD 3.8 Design constraints** • **SD 3.9 Service-oriented architecture** • **SD 4.3.5.8 Application sizing** • **SD App D Design and planning documents and their contents** • **ST 3.2.5 Align service transition plans with the business needs**	• *8.2.2. Information security awareness, education and training* • *10.1.1 Security requirements analysis and specification* • *10.3.2 System acceptance*
AI1.2 Risk analysis report	• Analysis of all significant threats and potential vulnerabilities affecting the requirements	• *SD 2.4.2 Scope* • *SD 3.6 Design aspects* • *SD 4.5.5.2 Stage 2—Requirements and strategy*	• *11.6.2 Sensitive system isolation* • *12.1.1 Security requirements analysis and specification*

CobiT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI1 Identify Automated Solutions *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI1.3 Feasibility study and formulation of alternative courses of action	• Alternative solutions to satisfying business requirements assessed by the business and IT	• *SD 3.6.1 Designing service solutions* • *SD 3.7.1 Evaluation of alternative solutions* • *ST 3.2.4 Maximise reuse of established processes and systems*	
AI1.4 Requirements and feasibility decision and approval	• Business sponsor's approval of requirements, feasible options, solutions and the acquisition approach	• *SD 3.6.1 Designing service solutions*	• *6.1.4 Authorisation process for information processing facilities* • *10.3.2 System acceptance*
AI2 Acquire and Maintain Application Software			
Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI2.1 High-level design	• Translation of business requirements to high-level design for acquisition • Alignment with technological direction and information architecture	• *SD 3.6.1 Designing service solutions* • *SD 3.6.3 Designing technology architectures*	
AI2.2 Detailed design	• Technical design and application requirements • Criteria for acceptance	• *SS 8.2 Service interfaces* • *SD 4.2.5.2 Determine, document and agree requirements for new services and produce service level requirements (SLR)* • *SD 5.3 Application management*	
AI2.3 Application control and auditability	• Business controls with automated application controls for accurate, complete, authorised and auditable processing		• **10.10.1 Audit logging** • **10.10.5 Fault logging** • **12.2.1 Input data validation** • **12.2.2 Control of internal processing** • **12.2.3 Message integrity** • **12.2.4 Output data validation** • **13.2.3 Collection of evidence** • **15.3.1 Information systems audit controls** • **15.3.2 Protection of information systems audit tools**

CobiT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI2 Acquire and Maintain Application Software *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI2.4 Application security and availability	• Security and availability requirements addressed	• *SD 3.6.1 Designing service solutions* • *SO 4.4.5.11 Errors detected in the development environment*	• **6.1.4 Authorisation process for information processing facilities** • **7.2.1 Classification guidelines** • **10.3.2 System acceptance** • **11.6.2 Sensitive system isolation** • **12.1.1 Security requirements analysis and specification** • **12.2.3 Message integrity** • **12.3.1 Policy on the use of cryptographic controls** • **12.4.3 Access control to program source code** • **12.5.2 Technical review of applications after operating system changes** • **12.5.4 Information leakage** • **15.3.2 Protection of information systems audit tools**
AI2.5 Configuration and implementation of acquired application software	• Configuration of acquired software packages		• *12.5.3 Restrictions on changes to software packages*
AI2.6 Major upgrades to existing systems	• Applying similar development process when making major changes		• *12.5.1 Change control procedures*
AI2.7 Development of application software	• Developing functionality in accordance with design, standards and QA requirements • Legal and contractual requirements followed by third-party developers	• *SD 3.7.3 Develop the service solution*	• *12.5.5 Outsourced software development*
AI2.8 Software quality assurance	• QA plan to obtain quality per the requirement and quality policy		• *10.3.2 System acceptance*
AI2.9 Applications requirements management	• Tracking status of all requirements through change management process	• *ST 3.2.6 Establish and maintain relationships with stakeholders* • *ST 3.2.10 Anticipate and manage course corrections*	
AI2.10 Application software maintenance	• Strategy and plan for software maintenance		
AI3 Acquire and Maintain Technology Infrastructure			
Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI3.1 Technological infrastructure acquisition plan	• Acquisition, implementation and maintenance plan for infrastructure, aligned with business need and technological direction	• *SD 3.6.3 Designing technology architectures*	
AI3.2 Infrastructure resource protection and availability	• Protection of resources using security and auditability measures • Use of sensitive infrastructure	• *SD 4.6.5.1 Security controls* • *SO 5.4 Server management and support*	• *12.1.1 Security requirements analysis and specification*

COBIT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI3 Acquire and Maintain Technology Infrastructure *(cont.)*			
COBIT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI3.3 Infrastructure maintenance	• Change control, patch management, upgrade strategies and security requirements	• **SO 5.4 Server management and support** • **SO 5.5 Network management** • **SO 5.7 Database administration** • **SO 5.8 Directory services management** • **SO 5.9 Desktop support** • **SO 5.10 Middleware management** • **SO 5.11 Internet/web management**	• *9.1.5 Working in secure areas* • *9.2.4 Equipment maintenance* • *12.4.2 Protection of system test data* • *12.5.2 Technical review of applications after operating system changes* • *12.6.1 Control of technical vulnerabilities*
AI3.4 Feasibility test environment	• Development and test environments; feasibility and integration tests	• *ST 4.4.5.1 Planning* • *ST 4.4.5.2 Preparation for build, test and deployment* • *ST 4.4.5.3 Build and test* • *ST 4.5.5.7 Test clean up and closure* • *ST 4.5.7 Information management*	• *10.1.4 Separation of development, test and operational facilities*
AI4 Enable Operation and Use			
Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.			
COBIT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI4.1 Planning for operational solutions	• Identification and planning of all technical, operational and usage aspects of solutions	• **SD 3.6.1 Designing service solutions** • **ST 3.2.5 Align service transition plans with the business needs** • **ST 3.2.9 Plan release and deployment packages** • **ST 4.4.5.1 Planning** • **ST 4.4.5.2 Preparation for build, test and deployment** • **ST 4.4.5.5 Plan and prepare for deployment**	
AI4.2 Knowledge transfer to business management	• Enable ownership, delivery, quality and internal control of solution	• *ST 3.2.5 Align service transition plans with the business needs* • *ST 4.7 Knowledge management*	
AI4.3 Knowledge transfer to end users	• End-user knowledge and skills for use as part of business processes	• **ST 3.2.8 Provide systems for knowledge transfer and decision support** • **ST 4.4.5.8 Early life support** • **ST 4.7 Knowledge management**	
AI4.4 Knowledge transfer to operations and support staff	• Knowledge and skills to enable operation and support of systems and infrastructure	• **ST 3.2.8 Provide systems for knowledge transfer and decision support** • **ST 4.4.5.5 Plan and prepare for deployment** • **ST 4.7 Knowledge management** • **SO 3.7 Documentation** • **SO 4.4.5.11 Errors detected in the development environment** • **SO 4.6.6 Knowledge management (as operational activities)**	• *10.1.1 Documented operating procedures* • *10.3.2 System acceptance* • *10.7.4 Security of system documentation* • *13.2.2 Learning from information security incidents*

CobiT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI5 Procure IT Resources			
IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI5.1 Procurement control	• Standards and procedures aligned to enterprise procurement process	• *SD 3.7.2 Procurement of the preferred solution*	• *6.1.5 Confidentiality agreements*
AI5.2 Supplier contract management	• Contract initiation and life cycle management	• *SD 4.2.5.9 Develop contracts and relationships* • *SD 4.7.5.3 Establishing new suppliers and contracts*	• *6.1.5 Confidentiality agreements* • *6.2.3 Addressing security in third-party agreements* • *10.8.2 Exchange agreements* • *12.5.5 Outsourced software development*
AI5.3 Supplier selection	• Fair and formal selection process • Viable best fit to requirements	• **SD 3.7.1 Evaluation of alternative solutions** • **SD 4.7.5.3 Establishing new suppliers and contracts** • **SD App I Example contents of a statement of requirement (SoR) and/or invitation to tender (ITT)**	
AI5.4 IT resources acquisition	• Protection of enterprise interests in contractual agreements • Rights and obligations of all parties	• **SD 3.7.2 Procurement of the preferred solution**	
AI6 Manage Changes			
All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI6.1 Change standards and procedures	• Formal change management procedures • Standardised approach	• **SD 3.2 Balanced design** • **SD 3.7 The subsequent design activities** • **ST 3.2 Policies for service transition** • **ST 3.2.1 Define and implement a formal policy for service transition** • **ST 3.2.2 Implement all changes to services through service transition** • **ST 3.2.7 Establish effective controls and disciplines** • **ST 4.1 Transition planning and support** • **ST 4.1.4 Policies, principles and basic concepts** • **ST 4.2 Change management**	• *10.1.2 Change management* • *12.5.3 Restrictions on changes to software packages*

CobiT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI7 Install and Accredit Solutions and Changes			
New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI7.1 Training	• Training of users and operations in accordance with implementation plan	• **ST 4.4.5.2 Preparation for build, test and deployment**	• *8.2.2 Information security awareness, education and training*
AI7.2 Test plan	• Test plan defining roles and responsibilities	• **ST 4.5.5.1 Validation and test management** • **ST 4.5.5.2 Plan and design test** • **ST 4.5.5.3 Verify test plan and test design** • **ST 4.5.5.4 Prepare test environment**	• *12.5.1 Change control procedures* • *12.5.2 Technical review of applications after operating system changes*
AI7.3 Implementation plan	• Implementation plan including fallback and backout strategies	• **ST 3.2.9 Plan release and deployment packages** • **ST 4.1.5.2 Preparation for service transition** • **ST 4.4.5.2 Preparation for build, test and deployment** • **ST 4.4.5.3 Build and test** • **ST 4.4.5.4 Service testing and pilots** • **ST 4.4.5.5 Plan and prepare for deployment**	
AI7.4 Test environment	• Secure test environment based on operational conditions	• *ST 3.2.14 Proactively improve quality during service transition* • *ST 4.4.5.2 Preparation for build, test and deployment* • *ST 4.4.5.3 Build and test* • *ST 4.4.5.4 Service testing and pilots*	• *10.1.4 Separation of development, test and operational facilities* • *12.4.3 Access control to program source code* • *12.5.2 Technical review of applications after operating system changes*
AI7.5 System and data conversion	• Data conversion and infrastructure migration		
AI7.6 Testing of changes	• Independently testing changes prior to migration	• *ST 3.2.14 Proactively improve quality during service transition* • *ST 4.4.5.4 Service testing and pilots* • *ST 4.5.5.5 Perform tests* • *ST 4.5.5.6 Evaluate exit criteria and report*	• *6.1.4 Authorisation process for information processing facilities* • *12.4.3 Access control to program source code* • *12.5.2 Technical review of applications after operating system changes*
AI7.7 Final acceptance test	• Business process owners and stakeholders evaluating outcome of testing	• *ST 4.4.5.4 Service testing and pilots* • *ST 4.5.5.5 Perform tests* • *ST 4.5.5.6 Evaluate exit criteria and report*	• *10.3.2 System acceptance* • *12.5.2 Technical review of applications after operating system changes* • *12.5.4 Information leakage*
AI7.8 Promotion to production	• Controlled handover to operations, software distribution, parallel processing	• **ST 4.4.5.5 Plan and prepare for deployment** • **ST 4.4.5.6 Perform transfer, deployment and retirement** • **SO 4.3.5.4 Fulfilment**	

CobiT 4.1 Domain: Acquire and Implement (AI) *(cont.)*			
AI7 Install and Accredit Solutions and Changes *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI7.9 Post-implementation review	• Evaluating whether objectives have been met and benefits realised • Action plan to address issues	• **ST 3.2.13 Assure the quality of the new or changed service** • **ST 4.1.5.3 Planning and co-ordinating service transition** • **ST 4.4.5.10 Review and close service transition** • **ST 4.4.5.7 Verify deployment** • **ST 4.4.5.9 Review and close a deployment** • **ST 4.6 Evaluation** • **SO 4.3.5.5 Closure**	

CobiT 4.1 Domain: Deliver and Support (DS)			
DS1 Define and Manage Service Levels			
Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS1 Service level management framework	• Formal service level management process and continuous alignment to business requirements • Facilitating common understanding between customer and provider	• **SS 2.6 Functions and processes across the life cycle** • **SS 4.3 Develop strategic assets** • **SS 4.4 Prepare for execution** • **SS 7.2 Strategy and design** • **SS 7.3 Strategy and transitions** • **SS 7.5 Strategy and improvement** • **SD 4.2.5.1 Designing SLA frameworks** • **SD 4.2.5.9 Develop contracts and relationships**	• *10.2.1 Service delivery*
DS1.2 Definition of services	• Services defined based on service characteristics and business requirements in a service catalogue	• **SS 4.2 Develop the offerings** • **SS 4.3 Develop strategic assets** • **SS 5.4 Service portfolio management methods** • **SS 5.5 Demand management** • **SS 7.2 Strategy and design** • **SS 7.3 Strategy and transitions** • **SS 7.4 Strategy and operations** • **SS 7.5 Strategy and improvement** • **SS 8.2 Service interfaces** • **SD 3 Service design principles** • **SD 3.1 Goals** • **SD 3.2 Balanced design** • **SD 3.4 Identifying and documenting business requirements and drivers** • **SD 3.5 Design activities** • **SD 3.6 Design aspects** • **SD 4.1 Service catalogue management**	• *10.2.1 Service delivery*

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS1 Define and Manage Service Levels *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS1.3 Service level agreements	• Defining SLAs based on customer requirements and IT capabilities • Service metrics, roles and responsibilities	• **SD 4.2.5.2 Determine, document and agree upon requirements for new services and produce SLR** • **SD App F Sample SLA and operating level agreement (OLA)**	• *10.2.1 Service delivery*
DS1.4 Operating level agreements	• Definition of technical delivery to support the SLA(s)	• **SD 4.2.5.5 Review and revise underpinning agreements and service scope** • **SD App F Sample SLA and OLA**	
DS1.5 Monitoring and reporting of service level achievements	• Continuous monitoring of service performance	• **SS 5.3 Service portfolio management** • **SD 4.2.5.3 Monitor service performance against SLA** • **SD 4.2.5.6 Produce service reports** • **SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO** • **SD 4.2.5.10 Complaints and compliments** • **SD 4.3.8 Information management** • **CSI 4.2 Service reporting** • **CSI 4.3 Service measurement**	• *10.2.2 Monitoring and review of third-party services* • *10.2.3 Managing changes to third-party services*
DS1.6 Review of service level agreements and contracts	• Regular review of SLAs and underpinning contracts for effectiveness and being up to date	• **SD 4.2.5.4 Collate, measure and improve customer satisfaction** • **SD 4.2.5.5 Review and revise underpinning agreements and service scope** • **SD 4.2.5.8 Review and revise SLAs, service scope and underpinning agreements**	
DS2 Manage Third-party Services			
The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS2.1 Identification of all supplier relationships	• Categorising services according to supplier type, significance and criticality	• **SS 7.3 Strategy and transitions** • **SD 4.7.5.1 Evaluation of new suppliers and contracts** • **SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD)**	• *6.2.1 Identification of risks related to external parties*

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS2 Manage Third-party Services *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS2.2 Supplier relationship management	• Liaising with regard to customer and supplier issues • Trust and transparency	• **SD 4.2.5.9 Develop contracts and relationships** • **SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD)** • **SD 4.7.5.4 Supplier and contract management and performance** • **SD 4.7.5.5 Contract renewal and/ or termination**	• *6.2.3 Addressing security in third-party agreements* • *10.2.3 Managing changes to third-party services* • *15.1.4 Data protection and privacy of personal information*
DS2.3 Supplier risk management	• Risk identification, contract conformance and supplier viability	• **SD 4.7.5.3 Establishing new suppliers and contracts** • **SD 4.7.5.5 Contract renewal and/ or termination**	• *6.2.1 Identification of risks related to external parties* • *6.2.3 Addressing security in third-party agreements* • *8.1.2 Screening* • *8.1.3 Terms and conditions of employment* • *10.2.3 Manage changes to third-party services* • *10.8.2 Exchange agreements*
DS2.4 Supplier performance monitoring	• Meeting business requirements, adherence to contract and competitive performance	• **SD 4.7.5.4 Supplier and contract management and performance**	• *6.2.3 Addressing security in third-party agreements* • *10.2.1 Service delivery* • *10.2.2 Monitoring and review of third-party services* • *12.4.2 Protection of system test data* • *12.5.5 Outsourced software development*
DS3 Manage Performance and Capacity			
The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS3.1 Performance and capacity planning	• Ensuring capacity and performance are available to meet SLAs	• **SD 4.3.5.1 Business capacity management** • **SD App J The typical contents of a capacity plan** • **CSI 5.6.2 Capacity management**	• *10.3.1 Capacity management*
DS3.2 Current performance and capacity	• Assessment of current performance and capacity	• **SD 4.3.5.2 Service capacity management** • **SD 4.3.5.3 Component capacity management** • **SO 4.1.5.2 Event notification** • **SO 4.1.5.3 Event detection** • **SO 5.4 Server management and support** • **CSI 4.3 Service measurement**	• *10.3.1 Capacity management*

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS3 Manage Performance and Capacity *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS3.3 Future performance and capacity	• Forecasting of resource requirements • Workload trends	• **SD 4.3.5.1 Business capacity management** • **SD 4.3.5.2 Service capacity management** • **SD 4.3.5.3 Component capacity management** • **SD 4.3.5.7 Modelling and trending** • **SD 4.3.8 Information management**	• *10.3.1 Capacity management*
DS3.4 IT resources availability	• Provision of resources, contingencies, fault tolerance and resource prioritisation	• **SD 4.3.5.3 Component capacity management** • **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.4 Availability management** • **SD 4.4.5.1 The reactive activities of availability management** • **SD 4.4.5.2 The proactive activities of availability management** • **SO 4.6.5 Availability management (as operational activities)** • **CSI 5.6.1 Availability management**	
DS3.5 Monitoring and reporting	• Maintaining and tuning performance and capacity, and reporting service availability to the business	• **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.3.5.5 Threshold management and control** • **SD 4.3.5.6 Demand management** • **SD 4.4.5.1 The reactive activities of availability management**	
DS4 Ensure Continuous Service			
The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS4.1 IT continuity framework	• Enterprisewide consistent approach to continuity management	• *SD 4.5 IT service continuity management* • *SD 4.5.5.1 Stage 1—Initiation* • *CSI 5.6.3 IT Service continuity management*	• **6.1.6 Contact with authorities** • **6.1.7 Contact with special interest groups** • **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment** • **14.1.4 Business continuity planning framework**
DS4.2 IT continuity plans	• Individual continuity plans based on framework • Business impact analysis • Resilience, alternative processing and recovery	• **SD 4.5.5.2 Stage 2—Requirements and strategy** • **SD 4.5.5.3 Stage 3—Implementation** • **SD App K The typical contents of a recovery plan**	• *6.1.6 Contact with authorities* • *6.1.7 Contact with special interest groups* • *14.1.3 Developing and implementing continuity plans including information security*

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS4 Ensure Continuous Service *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS4.3 Critical IT resources	• Focus on critical infrastructure, resilience and prioritisation • Response for different time periods	• *SD 4.4.5.2 The proactive activities of availability management* • *SD 4.5.5.4 Stage 4—Ongoing operation*	• *14.1.1 Including information security in the business continuity management process* • *14.1.2 Business continuity and risk assessment*
DS4.4 Maintenance of the IT continuity plan	• Changing control to reflect changing business requirements	• **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.5 Testing of the IT continuity plan	• Regular testing • Implementing action plan	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.6 IT continuity plan training	• Regular training for all concerned parties	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.7 Distribution of the IT continuity plan	• Proper and secure distribution to all authorised parties	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.8 IT services recovery and resumption	• Planning for period when IT is recovering and resuming services • Business understanding and investment support	• **SD 4.4.5.2 The proactive activities of availability management** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• *14.1.1 Including information security in the business continuity management process* • *14.1.3 Maintain or restore operations and ensure availability of information*
DS4.9 Offsite backup storage	• Offsite storage of all critical media, documentation and resources needed in collaboration with business process owners	• **SD 4.5.5.2 Stage 2—Requirements and strategy** • **SO 5.2.3 Backup and restore**	• *10.5.1 Information backup*
DS4.10 Post-resumption review	• Regular management assessment of plans	• *SD 4.5.5.3 Stage 3—Implementation* • *SD 4.5.5.4 Stage 4—Ongoing operation*	• *14.1.5 Testing, maintaining and reassessing business continuity plans*
DS5 Ensure Systems Security			
The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS5.1 Management of IT security	• High-level placement of security management to meet business needs	• *SD 4.6 Information security management* • *SO 5.13 Information security management and service operation*	• **6.1.1 Management commitment to information security** • **6.1.2 Information security co-ordination** • **6.2.3 Addressing security in third-party agreements** • **8.2.2 Information security awareness, education and training**

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS5.2 IT security plan	• Translation of business, risk and compliance requirements into a security plan	• *SD 4.6.4 Policies/principles/basic concepts* • *SD 4.6.5.1 Security controls (high-level coverage, not in detail)*	• **5.1.1 Information security policy document** • **5.1.2 Review of the information security policy** • **6.1.2 Information security co-ordination** • **6.1.5 Confidentiality agreements** • **8.2.2 Information security awareness, education and training** • **11.1.1 Access control policy** • **11.7.1 Mobile computing and communications** • **11.7.2 Teleworking**
DS5.3 Identity management	• Identification of all users (internal, external and temporary) and their activity	• *SO 4.5 Access management*	• **5.1.1 Information security policy document** • **5.1.2 Review of the information security policy** • **6.1.2 Information security co-ordination** • **6.1.5 Confidentiality agreements** • **8.2.2 Information security awareness, education and training** • **11.1.1 Access control policy** • **11.7.1 Mobile computing and communications** • **11.7.2 Teleworking**
DS5.4 User account management	• Life cycle management of user accounts and access privileges	• *SO 4.5 Access management* • *SO 4.5.5.1 Requesting access* • *SO 4.5.5.2 Verification* • *SO 4.5.5.3 Providing rights* • *SO 4.5.5.4 Monitoring identity status* • *SO 4.5.5.5 Logging and tracking access* • *SO 4.5.5.6 Removing or restricting rights*	• **6.1.5 Confidentiality agreements** • **6.2.1 Identification of risks related to external parties** • **6.2.2 Addressing security when dealing with customers** • **8.1.1 Roles and responsibilities** • **8.3.1 Termination responsibilities** • **8.3.3 Removal of access rights** • **10.1.3 Segregation of duties** • **11.1.1 Access control policy** • **11.2.1 User registration** • **11.2.2 Privilege management** • **11.2.4 Review of user access rights** • **11.3.1 Password use** • **11.5.1 Secure logon procedures** • **11.5.3 Password management system** • **11.6.1 Information access restriction**

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS5.5 Security testing, surveillance and monitoring	• Proactive testing of security implementation • Timely accreditation • Timely reporting of unusual events	• *SO 4.5.5.6 Removing or restricting rights* • *SO 5.13 Information security management and service operation*	• **6.1.8 Independent review of information security** • **10.10.2 Monitoring system use** • **10.10.3 Protection of log information** • **10.10.4 Administrator and operator logs** • **12.6.1 Control of technical vulnerabilities** • **13.1.2 Reporting security weaknesses** • **15.2.2 Technical compliance checking** • **15.3.1 Information systems audit controls**
DS5.6 Security incident definition	• Definition and classification of security incident characteristics	• **SD 4.6.5.1 Security controls (high-level coverage, not in detail)** • **SD 4.6.5.2 Management of security breaches and incidents**	• **8.2.3 Disciplinary process** • **13.1.1 Reporting information security events** • **13.1.2 Reporting security weaknesses** • **13.2.1 Responsibilities and procedures** • **13.2.3 Collection of evidence**
DS5.7 Protection of security technology	• Resistance to tampering	• *SO 5.4 Server management and support*	• **6.1.4 Authorisation process for information processing facilities** • **9.1.6 Public access, delivery and loading areas** • **9.2.1 Equipment siting and protection** • **9.2.3 Cabling security** • **10.6.2 Security of network services** • **10.7.4 Security of system documentation** • **10.10.1 Audit logging** • **10.10.3 Protection of log information** • **10.10.4 Administrator and operator logs** • **10.10.5 Fault logging** • **10.10.6 Clock synchronisation** • **11.3.2 Unattended user equipment** • **11.3.3 Clear desk and clear screen policy** • **11.4.3 Equipment identification in networks** • **11.4.4 Remote diagnostic and configuration port protection**

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS5.7 Protection of security technology *(cont.)*			• 11.5.1 Secure logon procedures • 11.5.4 Use of system utilities • 11.5.5 Session time-out • 11.5.6 Limitation of connection time • 11.6.2 Sensitive system isolation • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking • 12.4.1 Control of operational software • 12.6.1 Control of technical vulnerabilities • 13.1.2 Reporting security weaknesses • 13.2.3 Collection of evidence • 15.2.2 Technical compliance checking • 15.3.2 Protection of information systems audit tools
DS5.8 Cryptographic key management	• Life-cycle management of cryptographic keys		• 10.8.4 Electronic messaging • 12.2.3 Message integrity • 12.3.1 Policy on the use of cryptographic controls • 12.3.2 Key management • 15.1.6 Regulation of cryptographic controls
DS5.9 Malicious software prevention, detection and correction	• Up-to-date patches, virus controls and protection from malware		• 10.4.1 Controls against malicious code • 10.4.2 Controls against mobile code
DS5.10 Network security	• Controls to authorise access and information flows from and to networks	• *SO 5.5 Network management*	• 6.2.1 Identification of risks related to external parties • 10.6.1 Network controls • 10.6.2 Security of network services • 11.4.1 Policy on use of network services • 11.4.2 User authentication for external connections • 11.4.3 Equipment identification in networks • 11.4.4 Remote diagnostic and configuration port protection • 11.4.5 Segregation in networks • 11.4.6 Network connection control • 11.4.7 Network routing control • 11.6.2 Sensitive system isolation

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS5.11 Exchange of sensitive data	• Trusted path and authentication controls, proof of receipt and non-repudiation		• **6.2.1 Identification of risks related to external parties** • **10.6.1 Network controls** • **10.6.2 Security of network services** • **11.4.1 Policy on use of network services** • **11.4.2 User authentication for external connections** • **11.4.3 Equipment identification in networks** • **11.4.4 Remote diagnostic and configuration port protection** • **11.4.5 Segregation in networks** • **11.4.6 Network connection control** • **11.4.7 Network routing control** • **11.6.2 Sensitive system isolation**
DS6 Identify and Attribute Costs			
The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS6.1 Definition of services	• Identification of all costs linked to IT services and associated business processes	• **SS 5.1 Financial management** • **SD 4.1 Service catalogue management**	
DS6.2 IT accounting	• Allocation of costs according to enterprise cost model	• **SS 5.1 Financial management**	
DS6.3 Cost modelling and charging	• IT costing models based on service definitions, and charge-back process	• **SS 5.1 Financial management** • **SS 7.2 Strategy and design**	
DS6.4 Cost model maintenance	• Regular review and benchmark of cost/recharge model	• **SS 5.1 Financial management**	
DS7 Educate and Train Users			
Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS7.1 Identification of education and training needs	• Training curriculum for each group of employees	• *SO 5.13 Information security management and service operation* • *SO 5.14 Improvement of operational activities*	• **8.2.2 Information security awareness, education and training**
DS7.2 Delivery of training and education	• Identifying and appointing trainers • Training schedule		• *8.2.2 Information security awareness, education and training*
DS7.3 Evaluation of training received	• Evaluating training delivery and future improvement		

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS8 Manage Service Desk and Incidents			
Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS8.1 Service desk	• User interface • Call handling • Incident classification and prioritisation based on services and SLAs	• **SO 4.1 Event management** • **SO 4.2 Incident management** • **SO 6.2 Service desk**	• *14.1.4 Business continuity planning framework*
DS8.2 Registration of customer queries	• Logging and tracking of all calls, incidents, service requests and information needs	• **SO 4.1.5.3 Event detection** • **SO 4.1.5.4 Event filtering** • **SO 4.1.5.5 Significance of events** • **SO 4.1.5.6 Event correlation** • **SO 4.1.5.7 Trigger** • **SO 4.2.5.1 Incident identification** • **SO 4.2.5.2 Incident logging** • **SO 4.2.5.3 Incident categorisation** • **SO 4.2.5.4 Incident prioritisation** • **SO 4.2.5.5 Initial diagnosis** • **SO 4.3.5.1 Menu selection**	• *13.1.1 Reporting information security events* • *13.1.2 Reporting security weaknesses can be added as they pertain to event identification* • *13.2.1 Responsibilities and procedures* • *13.2.3 Collection of evidence*
DS8.3 Incident escalation	• Incident escalation according to limits in SLAs	• **SO 4.1.5.8 Response selection** • **SO 4.2.5.6 Incident escalation** • **SO 4.2.5.7 Investigation and diagnosis** • **SO 4.2.5.8 Resolution and recovery** • **SO 5.9 Desktop support**	• *13.1.2 Reporting security weaknesses can be added as they pertain to event identification* • *13.2.3 Collection of evidence* • *14.1.1 Including information security in the business continuity management process* • *14.1.4 Business continuity planning framework*
DS8.4 Incident closure	• Recording of resolved and unresolved incidents	• **SO 4.1.5.10 Close event** • **SO 4.2.5.9 Incident closure**	• *13.2.2 Learning from information security incidents* • *13.2.3 Collection of evidence*
DS8.5 Reporting and trend analysis	• Reports of service performance and trends of recurring problems	• **SO 4.1.5.9 Review and actions** • **CSI 4.3 Service measurement (vague)**	• *13.2.2 Learning from information security incidents*
DS9 Manage the Configuration			
Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS9.1 Configuration repository and baseline	• Recording configuration items, monitoring and recording all assets, and implementing a baseline for every system and service as a change recovery checkpoint	• **SS 8.2 Service interfaces** • **ST 4.1.5.2 Prepare for service transition** • **ST 4.3.5.2 Management and planning**	• *7.2.2 Information labelling and handling* • *12.4.1 Control of operational software* • *12.4.2 Protection of system test data*

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS9 Manage the Configuration *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS9.2 Identification and maintenance of configuration items	• Configuration procedures to support logging of all changes in configuration database	• **ST 4.1.5.2 Prepare for service transition** • **ST 4.3.5.3 Configuration identification** • **ST 4.3.5.4 Configuration control** • **ST 4.3.5.5 Status accounting and reporting**	• *7.1.1 Inventory of assets* • *7.1.2 Ownership of assets* • *7.2.2 Information labelling and handling* • *10.7.4 Security of system documentation* • *11.4.3 Equipment identification in networks* • *12.4.2 Protection of system test data* • *12.5.3 Restrictions on changes to software packages* • *12.6.1 Control of technical vulnerabilities* • *15.1.5 Prevention of misuse of information processing facilities*
DS9.3 Configuration integrity review	• Periodic review of configuration data integrity • Control of licensed software and unauthorised software	• **ST 4.3.5.6 Verification and audit** • **SO 5.4 Server management and support** • **SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4)**	• *7.1.1 Inventory of assets* • *10.7.4 Security of system documentation* • *12.5.2 Technical review of applications after operating system changes* • *15.1.5 Prevention of misuse of information processing facilities*
DS10 Manage Problems			
Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximises system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS10.1 Identification and classification of problems	• Problem classification, allocation to support staff	• **SO 4.4.5.1 Problem detection** • **SO 4.4.5.3 Problem categorisation** • **SO 4.4.5.4 Problem prioritisation** • **SO App C Kepner and Tregoe** • **SO App D Ishikawa diagrams**	• *13.2.2 Learning from information security incidents*
DS10.2 Problem tracking and resolution	• Audit trails, tracking and analysis of root causes of all problems • Initiating solutions to address root causes	• **SO 4.4.5.2 Problem logging** • **SO 4.4.5.5 Problem investigation and diagnosis** • **SO 4.4.5.6 Work-arounds** • **SO 4.4.5.7 Raising a known error record** • **SO 4.4.5.8 Problem resolution**	• *13.2.2 Learning from information security incidents*
DS10.3 Problem closure	• Closure procedures after elimination of error or alternative approach	• **SO 4.4.5.9 Problem closure** • **SO 4.4.5.10 Major problem review**	
DS10.4 Integration of configuration, incident and problem management	• Integration to enable effective management of problems		

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS11 Manage Data			
Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS11.1 Business requirements for data management	• Input form design • Minimising errors and omissions • Error-handling procedures	• *SD 5.2 Data and information management*	• *10.8.1 Information exchange policies and procedures*
DS11.2 Storage and retention arrangements	• Document preparation • Segregation of duties	• **SD 5.2 Data and information management** • **SO 5.6 Storage and archive**	• *10.5.1 Information backup* • *10.7.1 Management of removable media* • *15.1.3 Protection of organisational records*
DS11.3 Media library management system	• Completeness and accuracy		• **10.7.1 Management of removable media** • **10.7.2 Disposal of media** • **12.4.3 Access control to program source code**
DS11.4 Disposal	• Detection, reporting and correction		• **9.2.6 Secure disposal or reuse of equipment** • **10.7.1 Management of removable media** • **10.7.2 Disposal of media**
DS11.5 Backup and restoration	• Legal requirements • Retrieval and reconstruction mechanisms	• **SO 5.2.3 Backup and restore**	• **10.5.1 Information backup**
DS11.6 Security requirements for data management	• Data input by authorised staff	• *SD 5.2 Data and information management*	• **10.5.1 Information backup** • **10.7.3 Information handling procedures** • **10.8.3 Physical media in transit** • **10.8.4 Electronic messaging** • **12.4.2 Protection of system test data** • **12.4.3 Access control to program source code**
DS12 Manage the Physical Environment			
Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS12.1 Site selection and layout	• Site selection based on technology strategy, risk, legal and regulatory requirements		• **9.1.1 Physical security perimeter** • **9.1.3 Securing offices, rooms and facilities** • **9.1.6 Public access, delivery and loading areas**
DS12.2 Physical security measures	• Securing the location, including protection from unauthorised access, natural risks and power outages	• *SO App E Detailed description of facilities management*	• **9.1.1 Physical security perimeter** • **9.1.2 Physical entry controls** • **9.1.3 Securing offices, rooms and facilities** • **9.2.5 Security of equipment off premises** • **9.2.7 Removal of property**

CobiT 4.1 Domain: Deliver and Support (DS) *(cont.)*			
DS12 Manage the Physical Environment *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS12.3 Physical access	• Controlled access to premises by all parties	• *SO App E Detailed description of facilities management* • *SO App F Physical access control*	• **6.2.1 Identification of risks related to external parties** • **9.1.2 Physical entry controls** • **9.1.5 Working in secure areas** • **9.1.6 Public access, delivery and loading areas** • **9.2.5 Security of equipment off premises**
DS12.4 Protection against environmental factors	• Monitoring and control of environmental factors	• **SO App E Detailed description of facilities management**	• **9.1.4 Protecting against external and environmental threats** • **9.2.1 Equipment siting and protection** • **9.2.2 Supporting utilities** • **9.2.3 Cabling security**
DS12.5 Physical facilities management	• Management of facilities according to business, legal and regulatory requirements	• **SO 5.12 Facilities and data centre management**	• *9.2.2 Supporting utilities* • *9.2.4 Equipment maintenance*
DS13 Manage Operations			
Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS13.1 Operations procedures and instructions	• Procedures and familiarity with operational tasks	• **SO 3.7 Documentation** • **SO 5 Common service operation activities** • **SO App B Communication in service operation**	• *10.1.1 Documented operating procedures* • *10.7.4 Security of system documentation*
DS13.2 Job scheduling	• Organisation of job schedules maximising throughput and utilisation to meet SLAs	• **SD 4.3.5.5 Threshold management and control** • **SD 4.3.5.6 Demand management** • **SO 5.2.2 Job scheduling** • **SO 5.3 Mainframe management**	
DS13.3 IT infrastructure monitoring	• Monitoring infrastructure for critical events • Logging of information to enable review	• **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.3.5.5 Threshold management and control** • **SO 4.1 Event management** • **SO 4.1.5.1 Event occurs** • **SO 4.1.5.9 Review and actions** • **SO 5.2.1 Console management/ operations bridge**	
DS13.4 Sensitive documents and output devices	• Physical safeguards for sensitive assets, and negotiable instruments	• *SO 5.2.4 Print and output*	
DS13.5 Preventive maintenance for hardware	• Maintenance to reduce impact of failures	• *SO 5.3 Mainframe management* • *SO 5.4 Server management and support*	• *9.2.4 Equipment maintenance*

CobiT 4.1 Domain: Monitor and Evaluate			
ME1 Monitor and Evaluate IT Performance			
Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME1.1 Monitoring approach	• General monitoring framework • Integration with corporate approach	• SD 8.5 Measurement of service design • ST 4.5.5.1 Validation and test management • SO 3.5 Operational health • CSI 4.1 The seven-step improvement process • CSI 4.1a Step one—Define what you should measure • CSI 4.1b Step two—Define what you can measure • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 4.1.2 Metrics and measurement • CSI 4.3 Service measurement • CSI 4.4 Return on investment for CSI • CSI 4.5 Business questions for CSI • CSI 5.1 Methods and techniques • CSI 5.2 Assessments	
ME1.2 Definition and collection of monitoring data	• Balanced set of objectives approved by stakeholders • Benchmarks, availability and collection of measurable data	• SD 4.2.5.10 Complaints and compliments • CSI 4.1c Step three—Gathering data • CSI 4.1d Step four—Processing the data	• *10.10.2 Monitoring system use*
ME1.3 Monitoring method	• Method for capturing and reporting results	• ST 4.5.5.2 Plan and design test • ST 4.5.5.3 Verify test plan and test design • ST 4.5.5.4 Prepare test environment • CSI 4.1b Step two—Define what you can measure • CSI 4.1f Step six—Presenting and using the information • CSI 5.4 Measuring and reporting frameworks	
ME1.4 Performance assessment	• Review of performance against targets • Remedial actions • Root cause analysis	• SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO • CSI 3 Continual service improvement principles • CSI 4.1e Step five—Analysing the data • CSI 5.3 Benchmarking • CSI 8 Implementing continual service improvement	

COBIT 4.1 Domain: Monitor and Evaluate *(cont.)*			
ME1 Monitor and Evaluate IT Performance *(cont.)*			
COBIT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME1.5 Board and executive reporting	• Reports of IT's contribution to the business for service and investment portfolios and programmes	• *CSI 4.1f Step six—Presenting and using the information* • *CSI 4.2 Service reporting*	
ME1.6 Remedial actions	• Follow-up on and remediation of all performance issues	• **CSI 4.1g Step seven—Implementing corrective action**	
ME2 Monitor and Evaluate Internal Control			
Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.			
COBIT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME2.1 Monitoring of internal control framework	• Continual review and improvement of internal controls		• *5.1.1 Information security policy document* • *15.2.1 Compliance with security policies and standards*
ME2.2 Supervisory review	• Review of managerial review controls		• *5.1.2 Review of the information security policy* • *6.1.8 Independent review of information security* • *10.10.2 Monitoring system use* • *10.10.4 Administrator and operator logs* • *15.2.1 Compliance with security policies and standards*
ME2.3 Control exceptions	• Analysis of control exceptions and root causes		• *15.2.1 Compliance with security policies and standards*
ME2.4 Control self-assessment	• Evaluation of controls' effectiveness through self-assessment		• *15.2.1 Compliance with security policies and standards*
ME2.5 Assurance of internal control	• Third-party reviews to provide added assurance		• *5.1.2 Review of the information security policy* • *6.1.8 Independent review of information security* • *10.10.2 Monitoring system use* • *10.10.4 Administrator and operator logs* • *15.2.1 Compliance with security policies and standards* • *15.2.2 Technical compliance checking* • *15.3.1 Information systems audit controls*
ME2.6 Internal control at third parties	• Status of external providers controls and compliance		• *6.2.3 Addressing security in third-party agreements* • *10.2.2 Monitoring and review of third-party services* • *15.2.1 Compliance with security policies and standards*
ME2.7 Remedial actions	• Remediation of control assessment exceptions		• *5.1.2 Review of the information security policy* • *15.2.1 Compliance with security policies and standards*

CobiT 4.1 Domain: Monitor and Evaluate *(cont.)*			
ME3 Ensure Compliance With External Requirements			
Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME3.1 Identification of external legal, regulatory and contractual compliance requirements	• Continuous identification of compliance requirements for incorporation into policies and practices		• **6.1.6 Contact with authorities having potential impact on IT** • **15.1.1 Identification of applicable legislation** • **15.1.2 Intellectual property rights (IPR)** • **15.1.4 Data protection and privacy of personal information**
ME3.2 Optimisation of response to external requirements	• Review and adjustment of policies and practices to ensure compliance		
ME3.3 Evaluation of compliance with external requirements	• Confirmation of compliance		• *6.1.6 Contact with authorities having potential impact on IT* • *15.1.1 Identification of applicable legislation* • *15.1.2 Intellectual property rights (IPR)* • *15.1.4 Data protection and privacy of personal information*
ME3.4 Positive assurance of compliance	• Reporting assurance of compliance and confirming remediation of any corrective actions		• *6.1.6 Contact with authorities having potential impact on IT* • *15.1.1 Identification of applicable legislation* • *15.1.2 Intellectual property rights (IPR)* • *15.1.4 Data protection and privacy of personal information*
ME3.5 Integrated reporting	• Integrated reporting of compliance with the enterprise		
ME4 Provide IT Governance			
Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME4.1 Establishment of an IT governance framework	• IT governance framework aligned to enterprise governance • Based on suitable IT process and control model • Confirmation framework ensuring compliance and confirming delivery of enterprise strategy for IT	• *CSI 3.10 Governance* • *CSI App A Complementary guidance*	
ME4.2 Strategic alignment	• Board understanding of IT strategy, strategic direction, confidence and trust between business and IT, co-responsibility for strategic decisions, and benefit realisation	• *SD 3.10 Business service management*	

CobiT 4.1 Domain: Monitor and Evaluate *(cont.)*			
ME4 Provide IT Governance *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
ME4.3 Value delivery	• Delivery of optimum value to support enterprise strategy • Understanding of expected business outcomes; effective business cases; management of economic life cycle and realisation of benefits; enforcement of portfolio, programme and project management; and business ownership of investments	• *SS 3.1 Value creation*	
ME4.4 Resource management	• Regular assessment to ensure appropriate resourcing and alignment with current and future objectives		
ME4.5 Risk management	• Appetite for risk, appropriate risk management practices, embedding risk responsibilities, regular assessment of risk and transparent risk reporting	• *SS 9.5 Risks*	
ME4.6 Performance measurement	• Confirming objectives have been met, reviewing any remedial actions, reporting performance to senior management and enabling review of progress	• *SS 4.4 Prepare for execution* • *SS 9.4 Effectiveness in measurement* • *SD 3.6.5 Design of measurement systems and metrics* • *CSI 4.3 Service measurement*	
ME4.7 Independent assurance	• Obtaining where appropriate independent (internal or external) assurance of conformance with objectives and external requirements		• *5.1.2 Review of the information security policy* • *6.1.8 Independent review of information security* • *10.10.2 Monitoring system use*