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

AUDITORIA AOS SISTEMAS DE INFORMAÇÃO COM BASE NO *CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)*

Osman Abdul Aziz

Lisboa, novembro de 2019

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

AUDITORIA AOS SISTEMAS DE INFORMAÇÃO COM BASE NO *CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)*

Osman Abdul Aziz

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica do Doutor Fernando Rodrigues, Professor Adjunto na área das Ciências da Informação e Comunicação.

Constituição do Júri:

Presidente: Professor Especialista (Mestre) Gabriel Correia Alves

Arguente: Professor Doutor Jorge Sequeira

Vogal: Professor Doutor Fernando João Leitão Rodrigues

Lisboa, novembro de 2019

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

Resumo

Os Sistemas de Informação (SI) têm vindo a revelar cada vez mais um forte pilar para o sucesso de muitas organizações onde a presença destes sistemas é incontestável.

Este projeto tem como objetivo investigar a importância e o impacto da existência da auditoria nos SI com base no *Control Objectives for Information and related Technology* (COBIT) e toda a sua estrutura.

A evolução e a dependência das Tecnologias de Informação (TI) nas organizações levaram à adoção de medidas novas, de modo a atingir os objetivos da organização, que por resultado melhoram o desempenho do negócio empresarial e onde procuram otimizar as áreas relacionadas às TI.

Como tal, os auditores surgem para as organizações como forma de acrescentar valor, uma vez que são orientados para garantir independentemente a conformidade e aderência das políticas e exigências legais das organizações, bem como, verificar a qualidade de resposta na existência de falhas de conformidade.

Palavras-chave: Auditoria; *COBIT*; Sistemas de Informação; Governação; Tecnologias de Informação.

Abstract

The information systems have come to reveal to be a strong pillar for the success of many organizations, the presence of these systems is indisputable.

This project's aim is to research the importance and impact of auditing on the information systems based on Control Objectives for Information and related Technology (COBIT) and all his structure.

The evolution and dependency of the information technology (IT), on the organizations led to the need of new measures, to achieve the organization's goals, which by result improve the performance and seek to optimize the IT-related areas.

As such, the auditors appear to the organizations to add-value, since they are guided to assure independently the compliance and adhesion of internal policies and legal requirements of the organizations, and to verify the capacity do take corrective actions if any failure of compliance exists.

Keywords: Auditing; *COBIT*; Information Systems; Governance; Information Technology.

Índice

Índice de Tabelas

Índice de Figuras

Índice de Anexos

Lista de Abreviaturas

APO – *Align, Plan and Organize*

BAI – *Build, Acquire and Implement*

BSC – *Balance Scorecard*

CAAT - *Computer Assisted Auditing Techniques*

CIO - *Chief Information Officer*

COBIT - *Control Objectives for Information and Related Technology*

DSS – *Deliver, Service and Support*

EDM – *Evaluate, Direct and Monitor*

GEIT – Governance of Enterprise Information Technology

ISACA - *Information Systems Audit and Control Association*

ISO/IEC – *International Standards Organization / International Electrotechnical Commission*

KPI – *Key Performance Indicator*

MEA - *Monitor, Evaluate and Assess*

RACI – *Responsible, Accountable, Consulted and Informed*

SAP – *System Application Products*

SI – Sistemas de Informação

SIG – Sistema de Informação Geográfica

TI – Tecnologias de Informação

TOGAF - *The Open Group Architecture Framework*

1. Introdução

A presente investigação tem como tema **"*Auditoria aos Sistemas de Informação com base no Control Objetives for Information and related Technology (COBIT)*"**.

Na sua elaboração, pretende-se compreender qual o papel da Auditoria no âmbito dos SI com base na *framework* do COBIT e a importância desta *framework* perante os diversos cenários de risco e medidas específicas implementadas pelas organizações.

De forma a apurar a informação supramencionada, será objeto de análise a estrutura do COBIT, onde o foco será no COBIT 5 com algumas referências ao COBIT 4.1, acompanhada da sua evolução desde o seu lançamento em 1996 de forma sintetizada, incluindo a última atualização COBIT 2019 apresentada pública e recentemente em novembro de 2018.

Note-se que a investigação científica realizada não foi baseada num estudo meramente empírico, mas sim através do cruzamento de diversos métodos. Desde logo o de observação direta conjugado com o método crítico para validar factos e acontecimentos que se consideram fora dos padrões normais. Através do método inquisitivo foi possível reunir informação obtida através de especialistas e certificados em auditoria aos SI e outros igualmente relevantes. Na qualidade de convidado, foi possível participar em eventos, discussões e diálogos sobre a temática, aplicando através do método sistemático a obtenção de um resultado próximo da situação atual (e real) da auditoria a SI.

Em sequência, são apresentados dados primários pesquisados e validados com base num questionário realizado aos inquiridos conduzindo através de entrevistas formais, semiformais e informais, em que os entrevistados responderam a um conjunto de perguntas que fazem parte de um guião, com vista a satisfazer a necessidade da situação presente e específica numa orientação técnica e atividades relacionadas.

Em suma, aos entrevistados foi-lhes permitido avaliar o COBIT envolvendo a realidade do negócio num estudo projetivo sendo possível aplicar na presente dissertação um levantamento prático de acordo com a realidade portuguesa.

1.1. Objeto da investigação

Lançado em 1996, pela ISACA (anteriormente conhecida como *Information Systems Audit and Control Association*), o COBIT apresentou uma evolução real da *framework* ao longo destes vinte e três anos, evidenciando sete versões, cada uma dedicada a eventos diferentes:

Tabela 1.1 - Evolução da *framework* COBIT

Versão	Ano	Âmbito
COBIT 1	1996	Auditoria
COBIT 2	1998	Controlo
COBIT 3	2000	Gestão de TI
COBIT 4	2005	Governação de TI
COBIT 4.1	2007	Governação de TI
COBIT 5	2012	Governação e Gestão de TI
COBIT 2019	2019	Governação e Gestão de TI

Fonte: Autoria própria

O COBIT surgiu inicialmente como um modelo de referência para a gestão de TI e com base numa estrutura de gestão de riscos.

Dado à evolução de TI, os gestores reconhecem o impacto que a informação tem a nível organizacional, o que levou à existência destas versões de forma a acompanhar a expansão de TI, que hoje em dia, num mercado cada vez mais competitivo, exige a troca de informação. No entanto, é necessário que esta criação e partilha de informação seja efetuada de forma segura, através do COBIT.

Posto isto, uma estratégia importante é conduzir uma auditoria aos SI presente na organização, com o objetivo de conseguir identificar falhas no sistema, falta de conformidade com leis e regulamentos e ajudar a definir se as medidas implementadas são adequadas. O principal objetivo de uma auditoria aos SI é garantir que todas as ações consideradas pela organização, são preventivas e ativas em relação às vulnerabilidades existentes.

No âmbito da investigação, o problema reflete-se em **compreender a forma e importância de atuação dos auditores no exercício da função de Auditoria no âmbito dos SI com base no *framework* do COBIT.**

As questões centrais da investigação são:

1. É a *framework* COBIT adotada pelas organizações a nível nacional?

2. Quão viável é utilizar o COBIT como uma ferramenta / orientação para através de análises baseadas em eficácia e eficiência, executar uma auditoria aos SI?

3. Os objetivos e processos da *framework* COBIT vão ao encontro das necessidades das organizações face à realidade nacional?

As questões supra indicadas foram respondidas no decorrer da investigação realizada no terreno, tendo sido possível fazer algumas considerações finais relevantes.

1.2. Objetivos da investigação

1.2.1. Objetivo geral

O objetivo geral da presente investigação é relacionar o trabalho de auditoria aos SI com base no *COBIT*, perceber de que forma a presença do COBIT nas organizações otimiza o investimento em TI, através de recursos disponíveis, como aplicações, informações, infraestruturas e pessoas, como também, as diversas dificuldades na sua implementação.

Assim sendo, o foco principal da investigação encontra-se plasmado no objeto da investigação já referido.

1.2.2. Objetivos específicos

Com vista a responder ao ponto principal da investigação, os objetivos específicos a analisar são os seguintes:

- Enquadramento teórico;
- Perceber o contributo do papel de auditoria aos SI – uma abordagem detalhada aos componentes do COBIT;
- A função e os objetivos da ISACA – abordagem com foco no COBIT 5;
- A problemática de utilização do COBIT 5.

1.3. Relevância e Justificação da Problemática

As problemáticas primárias deparadas no decorrer desta investigação através dos dados recolhidos por vários testemunhos ligados a organizações, que por motivos de privacidade e confidencialidade não será possível identificá-los, foram:

- A *framework* COBIT exige das pequenas e médias empresas a nível nacional, um investimento muito superior ao seu apetite e capacidade de investimento, contendo uma complexidade que resulta na dificuldade em adaptá-la;
- Numa outra vertente, no âmbito da aplicabilidade de metodologias, estas têm muito que se diga, ou seja, qualquer metodologia deve ser utilizada como um indicador, tornando-se apenas úteis se forem implementadas e adaptadas ao negócio em causa.

Assim sendo, verifica-se uma falta de evidência na utilização do COBIT 5 nas estruturas organizacionais a nível nacional, onde a *framework* apenas é utilizada parcialmente como um guia de orientação, nalguns casos como mera promoção comercial.

Existe no entanto, uma considerável falta de abordagem académica e conteúdos disponíveis em termos práticos e realistas, quer seja na avaliação da implementação e adaptação de *frameworks* semelhantes, quer seja para a prática de governação em departamentos de TI.

Razão pela qual este estudo procura fomentar o interesse em linhas de investigação futuras.

1.4. Metodologia de Investigação

Este projeto tem como primeiro método de investigação, pesquisas bibliográficas e documentais, no que se refere ao enquadramento teórico e desenvolvimento do tema, através de livros, revistas científicas, legislação nacional e internacional. Pretende-se obter resultados fidedignos e para isso foram combinadas as várias fontes de dados supracitadas.

Um segundo método de investigação fundamenta-se na experimentação com ligação ao conteúdo prático da presente investigação. O método experimental traduz-se em pesquisas feitas através das entrevistas realizadas com base num questionário aplicado a diversos ambientes empresariais, orientado devida e especificamente para o presente estudo, ou seja, através dessas entrevistas estrutura-se a composição e a formulação das questões mais precisas que devolvem os conceitos críticos relacionados.

Deste modo, cruzam-se os vários métodos em investigação científica já referidos, de forma mais ampla, detalhada e realisticamente explorar o tema da presente investigação.

Numa outra fase, com maior conhecimento e capacitação sobre a temática relacionada com as boas práticas, são dados três passos essenciais:

- **Primeiro**, são analisadas quais as frameworks e guias existentes nas organizações a nível nacional;
- **Segundo**, dos respondentes solicita-se que indiquem quais as principais preocupações a nível da organização e de TI submetidas a inquérito, quais os processos sistematizados montados e implementados na sua estrutura organizacional;
- **Terceiro**, são comparadas as preocupações e os processos existentes em ambiente real com a framework COBIT de forma a mapear e cruzar os vários objetivos definidos.

Depois destes três passos alcançados é possível visualizar e identificar quais os objetivos que as organizações abordadas entendem ser os mais importantes, com base nos processos organizacionais existentes. Através da *framework* COBIT e do resultado da comparação efetuada, permite perceber se as *frameworks* e projetos escolhidos entregam mais valor, o mesmo, ou menos que o COBIT, em oposição à sua não adoção ou mesmo implementação.

1.5. Descrição da estrutura da dissertação

No capítulo 2, é feita uma breve introdução às três categorias envolventes no tema da investigação: SI, COBIT e Auditoria (ponto 2.1); a seguir, com base no "Modelo Corporativo para Governança e Gestão de TI da Organização" publicado pela ISACA em 2015, é pretendido através de uma visão geral indicar os principais aspetos da *framework* COBIT 5 (ponto 2.2); é feito o enquadramento teórico do cruzamento entre a auditoria e os SI (ponto 2.3); e, por último, uma breve introdução (por falta de maturidade) da atualização mais recente da *framework* "COBIT2019" (ponto 2.4).

No capítulo 3, é feita a descrição dos métodos e procedimentos para dados obtidos dos questionários e das respostas das entrevistas realizadas.

No capítulo 4, consta a análise e o resultado do tratamento de dados, evidenciando a importação dos dados recolhidos, a caracterização da amostra, a discussão por questões ou por grupo de questões e por último é feita uma análise final com base em toda a informação recolhida.

No capítulo 5, com base na revisão literária, nas entrevistas e discussões sobre a presente investigação, foi possível fazer algumas conclusões e considerações gerais e finais bem como fazer referência sobre as limitações e implicações durante a investigação. É sugerido como linha de investigação futura uma investigação com base numa análise durante a execução de uma auditoria.

Por último, são introduzidas figuras, tabelas e similares no capítulo designado de “Apêndices e Anexos”, que permitiram apoiar a revisão da literatura e fundamentação da análise e discussão dos dados obtidos.

2. Enquadramento Teórico

2.1. Breve introdução aos SI, COBIT e à Auditoria

2.1.1. Definição de SI

Sistemas de Informação é uma expressão utilizada para descrever um Sistema, seja ele automatizado (e que pode ser denominado de várias maneiras) ou até mesmo manual que abrange pessoas, máquinas e/ou métodos organizados para recolher, processar, transmitir e disseminar dados que representam informação para o utilizador e/ou para um cliente (Marques, A.M., & Anjos, M., & Vaz, S. Q., 2002).

2.1.2. Control Objectives for Information and related Technology (COBIT)

O COBIT foi lançado em 1996, pela ISACA (anteriormente conhecida como *Information Systems Audit and Control Association*), apresentou uma evolução ao longo destes vinte e dois anos com seis versões, tendo sido a última edição em 2012 (COBIT 5).

Com a sua evolução, o COBIT 5 demonstrou ser a única estrutura para a governação e gestão de TI, apresentando cinco princípios básicos que contém grande parte do conteúdo da *framework* do COBIT 5, que surgem pela seguinte ordem:

- 1º Princípio: Atender às necessidades das partes interessadas;
- 2º Princípio: Cobrir a organização / negócio de ponta a ponta;
- 3º Princípio: Aplicar um modelo único integrado;
- 4º Princípio: Permitir uma abordagem holística;
- 5º Princípio: Distinguir a governação da gestão.

A orientação desta estrutura consiste em objetivos de negócio ligados a objetivos de TI, sendo um modelo de processos de TI organizado em dois domínios de processo principais:

- **Governação –** Consiste em cinco processos de governação e dentro de cada processo determinadas práticas para Avaliar, Orientar, Monitorizar (*Evaluate, Direct and Monitor - EDM*);
- **Gestão –** Consiste em quatro domínios, em consonância com os departamentos responsáveis por planear, construir, executar e monitorizar. O domínio principal cobre todas as funções e processos (cobertura das atividades numa lógica ponta a ponta).

A gestão está ordenada pela seguinte maneira:

- ✓ Alinhar, Planear e Organizar – (*Align, Plan and Organise* – (APO)
- ✓ Construir, Adquirir e Implementar - (*Build, Acquire and Implement* – (BAI)
- ✓ Entregar, Serviços e Suporte - (*Deliver, Service and Support* - (DSS)
- ✓ Monitorizar, Avaliar e Analisar - (*Monitor, Evaluate and Assess* – (MEA)

O COBIT 5 apresenta um conjunto de 37 processos de governação e de gestão, que o torna um modelo completo e abrangente, mas não é o único modelo de processos no âmbito das TI possível para uma organização, sendo que cada realidade empresarial deve atender ao seu ambiente e desafios específicos.

2.1.3. A função da Auditoria nos SI

A ISACA posiciona-se como uma entidade independente e sem fins lucrativos, onde desenvolve padrões internacionais de controlo e auditoria de SI que ajudam as partes interessadas a garantir confiança e valor dos SI.

Esta organização preocupa-se com a atualização do COBIT, o que ajuda os profissionais de TI e os líderes das organizações a cumprirem com as suas responsabilidades de gestão e governação de TI, nomeadamente nas áreas de garantia, segurança, risco e controlo, além da criação de valor para qualquer organização, seja ela pública ou privada.

Os objetivos dos auditores, mediante a sua atuação interna ou externa, são:

- Verificar a existência, a suficiência e a aplicação do SI, bem como, contribuir para o seu aperfeiçoamento;
- Verificar se as normas estão implementadas, refletem a legislação em vigor e se estão a ser cumpridas;
- Verificar a capacidade de resposta numa eventual falha de SI.

2.2. Control Objectives for Information and Related Technology (COBIT) - A *Framework*

A *framework* surgiu para ser e ainda é, uma das estruturas globais mais significativas para a gestão e governação de TI (Al Omari, Barnes, & Pitman, 2012a; Weill & Ross, 2004, p.20).

A atualização desta *framework* publicada em 2012, designada de COBIT 5, veio desempenhar um papel consolidador e fundamental na governação e gestão de TI, através de

um modelo único e integrado devido ao seu alinhamento com outros padrões e modelos, tais como, ITIL, orientação a *standards* ISO, BSC, entre outros.

O COBIT 5 junta os cinco princípios já referidos, que permitem a organização construir um modelo de gestão e de governação baseado em sete *enablers*, que otimizam o investimento em TI em benefício das partes interessadas (ISACA, 2012).

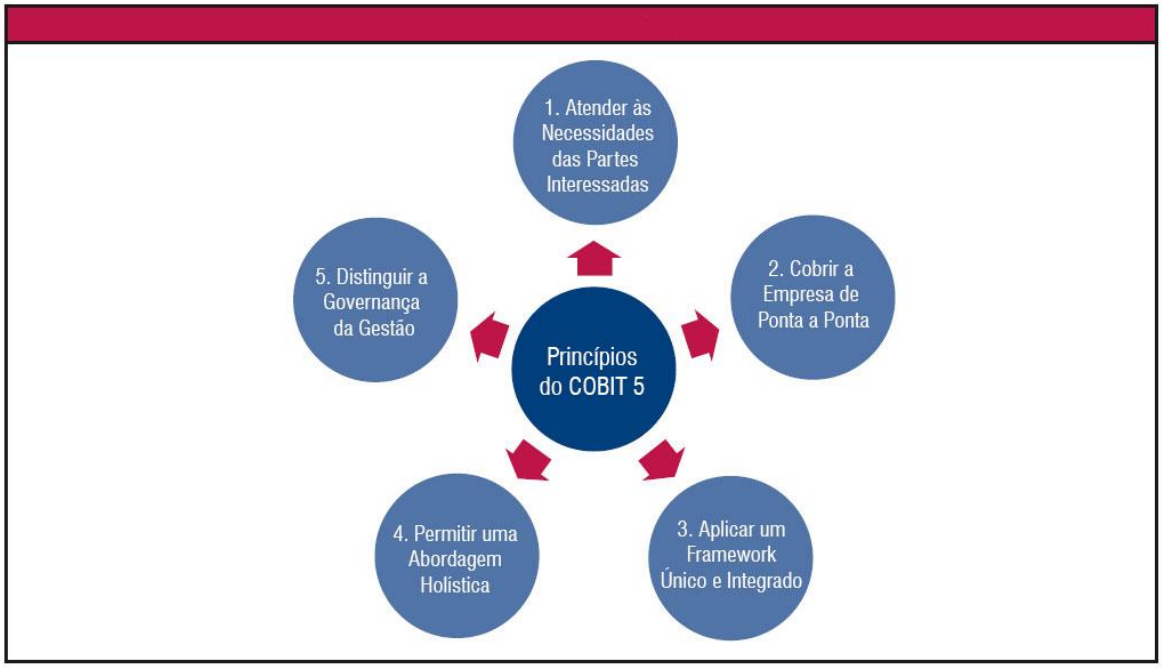


Figura 2.1 - Princípios do COBIT 5, **Fonte**: ISACA, COBIT® 5, 2012

- 1º Princípio: Atender às necessidades das partes interessadas.

As organizações têm diversos *Stakeholders,* cada um com uma perspetiva diferente do que é importante, no entanto, todos concordam que as organizações devem acrescentar valor.

Este princípio surge como uma função de governação. O sistema de governação deve considerar todas as partes interessadas ao tomar decisões de benefício, risco e avaliação de recursos.

Numa perspetiva de governação de TI, o principal objetivo do COBIT é permitir a criação de valor por meio da garantia de que os benefícios sejam percebidos, os riscos reduzidos e os recursos otimizados. Também é apresentado para fornecer às partes interessadas do negócio um modelo de governação de TI que aprimore a gestão dos riscos associados ao departamento de TI (Oliver, D., & Lainhart, J. 2012).

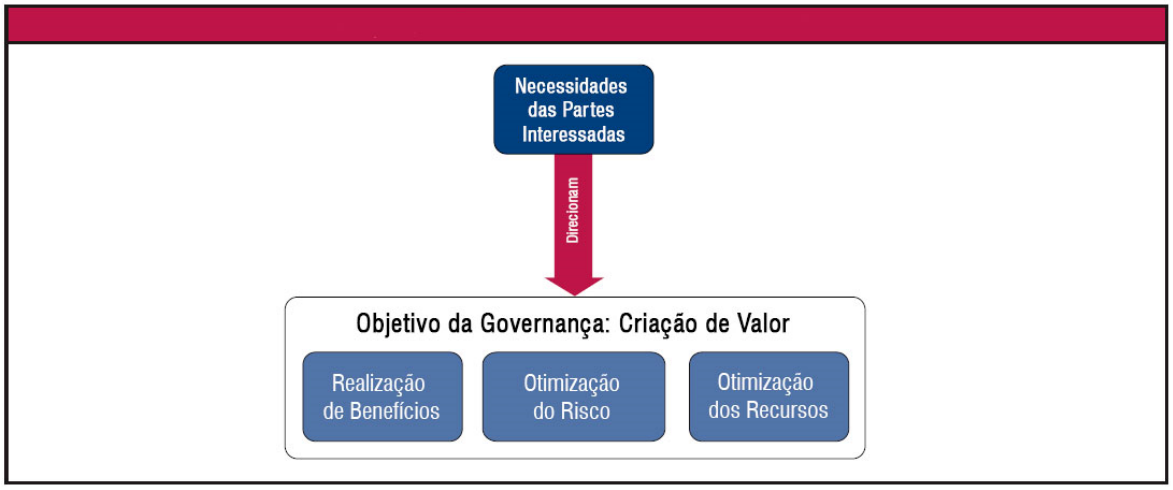


Figura 2.2 - Objetivo da Governação: Criação de Valor **Fonte**: ISACA, COBIT® 5, 2012

Os objetivos da organização são definidos assim que forem entendidas as necessidades das partes interessadas. Existe criação de valor quando ocorre uma das três perspetivas apresentadas na Figura 2.2. Para uma melhor compreensão sobre o que as partes interessadas pretendem, o COBIT 5 introduz três questões:

- ✓ Para quem são os benefícios?
- ✓ Quem assume o risco?
- ✓ Quais os recursos necessários?

Por vezes, os *Stakeholders* não partilham a mesma ideia de criação de valor, criando conflito entre os mesmos, outras vezes, as organizações são influenciadas por diversos fatores internos e externos, por exemplo, mercado, indústria, política, cultura e risco de negócio, entre outros. Assim, considerando as diversas necessidades das partes interessadas e os fatores internos e externos, a função de governação deve suportar o apoio na concretização dos objetivos. É sugerido neste contexto que exista uma função de governação e gestão personalizada, dando origem à Cascata de Objetivos do COBIT 5.

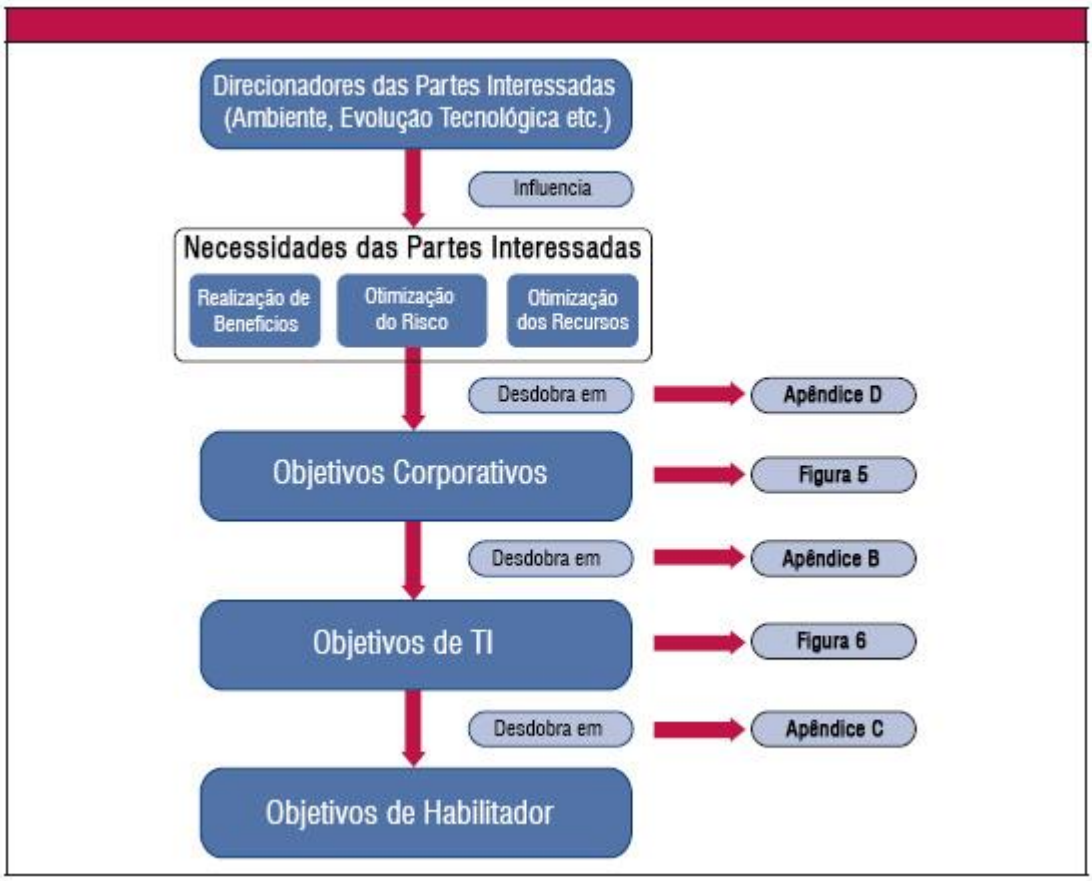


Figura 2.3 - Visão Geral da Cascata de Objetivos do COBIT 5, **Fonte**: ISACA, COBIT® 5, 2012

A Cascata dos Objetivos presente na figura 2.3, é um conceito importante na *framework* COBIT 5, no sentido em que traduz as necessidades das partes interessadas em estratégias para o sucesso dos objetivos da organização, ou seja, é o mecanismo utilizado para transformar as necessidades das partes interessadas em objetivos da organização, objetivos de TI e objetivos de *enablers*. A essência da Cascata dos Objetivos, tal como o nome indica, têm uma abordagem *Top-Down.*

Ao aplicar a Cascata dos Objetivos, seguem-se uma série de processos que permitem utilizar o COBIT 5 eficazmente, ou seja, perceber os objetivos em função das necessidades das partes interessadas, tem a função de alinhar as necessidades da organização com os serviços e soluções de TI, podendo ser aplicado em diversos níveis.

A Cascata dos Objetivos compreende quatro passos:

- ✓ 1º Passo – As tendências do mercado e da própria organização influenciam as necessidades das partes interessadas, por exemplo, alterações estratégicas, ambiente organizacional, evolução tecnológica, etc.;

- ✓ 2º Passo – Os objetivos da organização são o resultado das necessidades do cliente e do próprio negócio. A Cascata dos Objetivos organiza este passo alinhando-se com as perspetivas do BSC, em dezassete objetivos comuns e gerais que podem ser transformados em objetivos específicos da empresa.

  O COBIT 5, disponibiliza um mapa designado de "Apêndice D" (Anexo 1) que define os objetivos mais comuns nas organizações de modo a responderem às necessidades das partes interessadas através de um grupo de vinte e duas perguntas que permitem identificar essas necessidades.

- ✓ 3º Passo – Os objetivos da organização desdobram-se em objetivos de TI. Estes objetivos organizacionais podem ser mais eficazmente alcançados se os objetivos de TI tiverem sucesso (no contexto COBIT 5 apenas as atividades e os objetivos de TI são considerados). Cada um dos dezassete objetivos comuns mencionados no Apêndice D (2º passo) estão mapeados com dezassete objetivos relacionados com as TI definidos neste 3º passo, sempre estruturadas de acordo com as perspetivas do BSC.

  O COBIT 5 disponibiliza um mapa designado de "Apêndice B" (Anexo 2) que cruza dos objetivos de TI com os objetivos organizacionais.

- ✓ 4º Passo – Os objetivos de TI desdobram-se em objetivos de *enablers.*

  Para os objetivos de TI serem alcançados é necessário que uma parte dos *enablers* tenha sucesso na sua aplicação.

  Um destes *enablers* são os processos. Em alinhamento aos passos já referidos, cada um dos objetivos de TI está orientado a um ou mais processos. O COBIT 5 tem trinta e sete processos.

  Disponibiliza ainda um mapa designado de "Apêndice C" (Anexo 3) que define os vários processos já referidos categorizados por 5 domínios da *framework* e alinhados com os objetivos de TI.

Cada um dos resultados no cruzamento do Apêndice C (Anexo 3) é representado pela seguinte escala/legenda:

- **'P'** – com o significado de primário, expressa uma relação direta importante, ou seja, quando um processo do COBIT 5 for um apoio fundamental para a consecução dos objetivos de TI.

- **'S'** – com o significado de secundário, expressa uma relação ainda forte, mas menos importante, ou seja, quando um processo do COBIT 5 for um apoio em menor grau para a consecução dos objetivos de TI.

Atende-se ainda ao facto das organizações terem diversos objetivos. É expectável personalizar o COBIT 5 de forma a servir a organização através da Cascata dos Objetivos e assim alcançar com sucesso as necessidades das partes interessadas.

- 2º Princípio: Cobrir a organização numa visão ponta-a-ponta / abordagem à governação;

O âmbito do COBIT 5 compreende toda a informação e tecnologia relacionada na organização. Este princípio, inclui toda a gestão e governação abordada pelo departamento de TI, ou seja, por um lado, o sistema de governação TI, está inserido no sistema de governação de toda a organização, por outro lado, todas as funções e processos que são utilizados pela gestão e governação também estão incluídos. Este é o significado a reter quando se fala numa organização orientada a processos numa visão "ponta-a-ponta". De acordo com o COBIT 5, trata-se de uma "abordagem à governação".

Esta abordagem à governação consiste em quatro elementos principais:

- ✓ Objetivo da Governação: Criação de Valor (ver figura 2.2);
- ✓ *Enablers* de governação (também presente na figura 2.7)

  Como *enablers* entende-se:

  - Princípios, políticas e *frameworks;*
  - Processos;
  - Estruturas Organizacionais;
  - Cultura, ética e comportamento;
  - Informação;
  - Serviços, infraestrutura e aplicações;
  - Pessoas e competências.
- ✓ Âmbito da governação;
- ✓ Principais funções, atividade e relações, conforme se segue na figura seguinte;

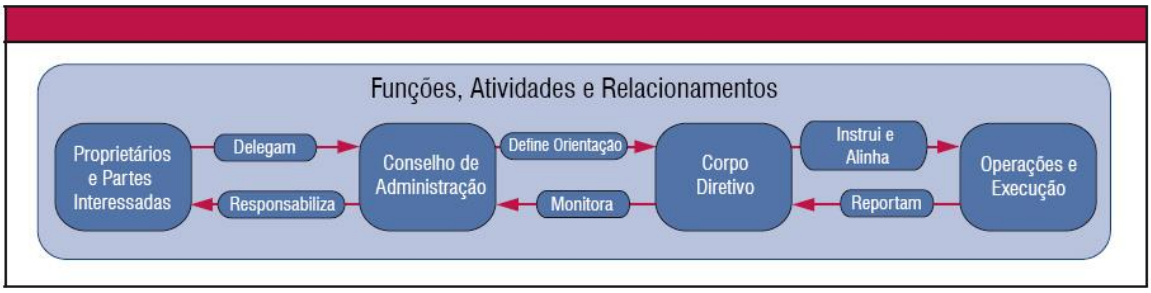


Figura 2.4 - Principais funções, atividades e relações, **Fonte**: ISACA, COBIT® 5, 2012

Assim, a sua aplicação deve ser completa na cobertura da organização (visão ponta-a-ponta), ou seja, não só alinhada à função de TI, mas com todas as funções e processos da organização. A sua abordagem trata de toda a informação e tecnologia relacionada como qualquer outro ativo seria tratado na organização.

A governação de TI consiste em estruturas, processos e mecanismos operacionais que trabalham em conjunto para garantir que os investimentos em TI e os objetivos de negócio estejam alinhados (De Haes & Van Grembergen, 2005, p. 1-3).

- 3º Princípio: Aplicar um modelo único integrado;

As organizações têm cada vez mais o dever de tratar e gerir toda a informação e tecnologias relacionadas, isto deve-se à evolução tecnológica e à pressão dos clientes, fornecedores, bem como reguladores e legisladores. Faz assim sentido, com estes deveres e obrigações, que a organização precise de uma *framework* que seja segura e consistente, mas que também tenha a capacidade de se ajustar conforme o tipo de organização. O COBIT 5, apresenta um papel de modelo único e integrado devido a quatro razões principais:

- ✓ Considera as normas, padrões e *frameworks* mais recentes, permitindo que o COBIT 5 seja a estrutura principal que alinha todas as atividades de governação e gestão;
- ✓ Por integrar outras *frameworks*, normas e práticas, apresenta uma posição única e integrada em orientação com uma linguagem comum não-técnica;
- ✓ É uma *framework* que resume e elabora guias de orientação, fornece um conjunto de elementos de apoio que incluem, *ISACA Research,* ITIL, TOGAF, ISO, bem como, uma série de instrumentos de apoio relacionados com o COBIT 5;
- ✓ Integra todo o tipo de informação presente nos diversos modelos da ISACA sobre governação e gestão de TI, assim como, as suas boas práticas.

A figura 2.5 identifica quais os padrões e modelos que o COBIT 5 utiliza como referência para as boas práticas de governação e de gestão.

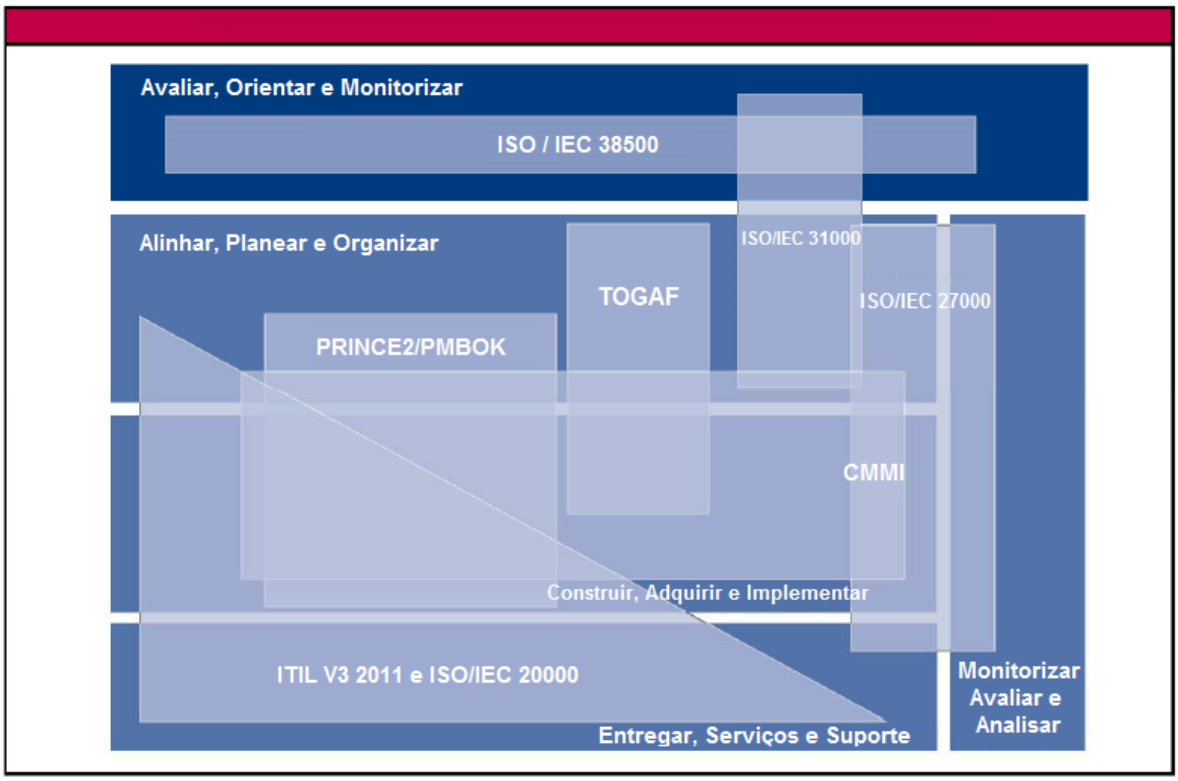


Figura 2.5 - Adaptado do COBIT 5 e a cobertura das diferentes frameworks, **Fonte**: COBIT® 5, 2012

- 4º Princípio: Permitir uma abordagem holística;

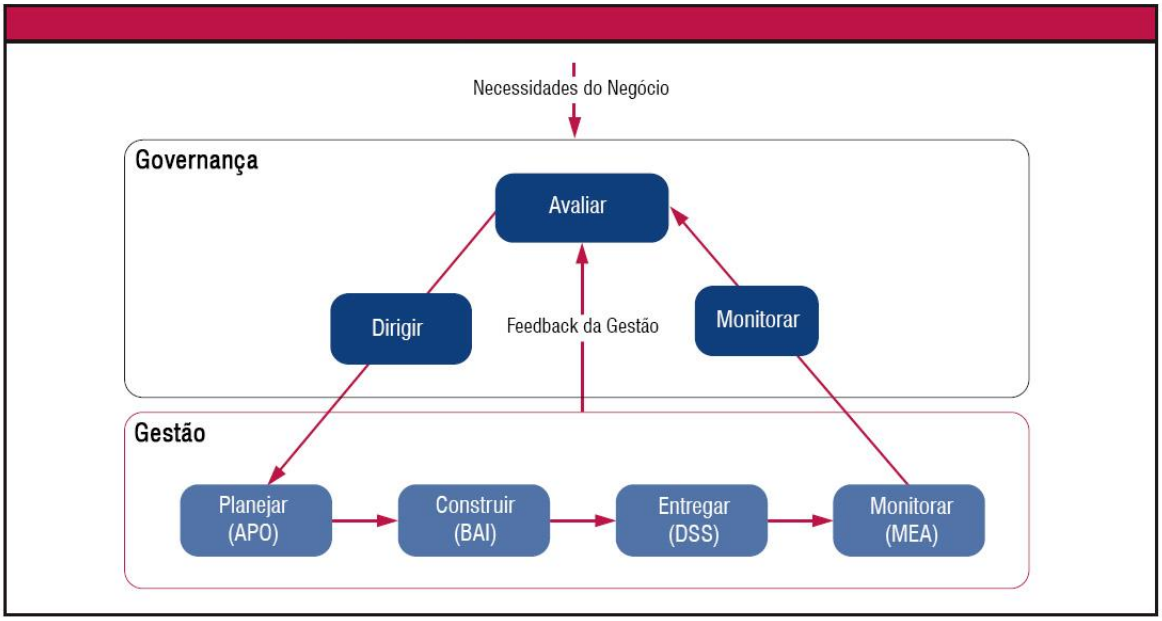


Figura 2.6 - Principais áreas de governação do COBIT 5, **Fonte**: ISACA, COBIT® 5, 2012

Como se verifica na figura anterior, Para uma gestão e governação de TI ser eficiente e eficaz dentro de uma organização, requer que seja considerado uma série de fatores díspares, designados de *enablers*. Portanto, quando são tomadas decisões, é necessário que exista o máximo de informação possível, ou seja, é necessária uma visão global e completa da organização, nomeadamente, em termos de processos de gestão e de governação e toda a estrutura.

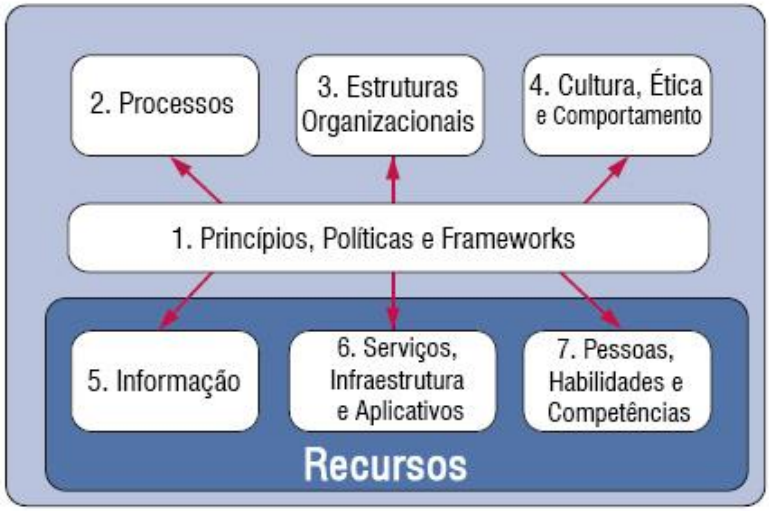


Figura 2.7 - Enablers, **Fonte**: ISACA, COBIT® 5, 2012

Cada *enabler* influencia o resultado das atividades de gestão e governação, podem ser tratados individualmente ou em conjunto, de modo a compreender a melhor abordagem a ter com a gestão e governação de TI na organização.

Os *enablers* são aplicáveis ao nível de toda a organização, incluindo todos os recursos, internos e externos, relacionados com o departamento de TI, bem como, as atividades e responsabilidades dentro e fora das funções de TI. Entende-se que cada *enabler* precisa de outro *enabler* para produzirem efeitos/resultados, por exemplo, processos precisam de dados e informação ou as estruturas organizacionais precisam de pessoas e competências. Por outro lado, o conjunto de dados e informações, pessoas e comportamentos tornam os processos eficientes.

- 5º Princípio: Distinguir a **governação** da **gestão**.

Com base na literatura pesquisada, a diferença entre governação e gestão não é muito clara como devia ser. O COBIT 5 faz uma clara distinção, indicando que cada um serve um propósito diferente com responsabilidades, atividades e estruturas organizacionais também diferentes.

O COBIT 5 utiliza as siglas, EDM e PBRM, respetivamente para governação e gestão. Sendo que EDM traduz-se para Avaliar, Orientar, Monitorizar (*Evaluate, Direct and Monitor*), e PBRM para Planear, Construir, Entregar e Monitorizar (*Plan, Build, Run and Monitor*).

A função de governação ou EDM, é a de garantir que as necessidades das partes interessadas são avaliadas de modo a determinar os objetivos organizacionais que têm de ser alcançados, define uma orientação através da escala 'P' e 'S' para melhor prioritização e tomadas de decisão, e monitoriza o desempenho e a conformidade de acordo com os objetivos estabelecidos.

A função de gestão ou PBRM, é a de garantir que as atividades estão alinhadas com as orientações indicadas pela função de governação.

O COBIT 5 inclui um modelo de referência de processos que divide os processos de governação e de gestão em dois domínios principais já mencionados, EDM e PBRM, que identifica o conjunto de trinta e sete processos entre as funções de governação e gestão.

No final, o COBIT 5 reconhece que as organizações são diferentes em dimensões, estruturas e complexidades, sendo esta a razão pela qual as organizações podem e devem organizar os seus processos conforme seja ajustável, incluindo sempre todos os objetivos de governação e gestão.

2.3. Diferenças entre o COBIT 4.1 e o COBIT 5

O COBIT 5 consolida/une as várias *frameworks* separadas como, RiskIT, ValIT, BMIS e COBIT 4.1 numa *framework* única. Assim, proporciona um mecanismo de criação de valor mais eficaz de modo a atender uma maior diversificação de necessidades de partes interessadas. Já referido no 3º Princípio, é um modelo único integrado, isto porque consegue integrar outras *frameworks*, como ITIL, TOGAF, ISO 27000, ISO 38500, ISO 31000, COSO, entre outros referenciais como o Prince2 e PMBOK.

Apresenta um número de conteúdos novos, tais como:

- ✓ Cinco novos princípios de governação (ver ponto 2.2.);
- ✓ Maior foco nos sete *enablers* já mencionados;
- ✓ O modelo de referência de processos de TI que define e descreve em detalhe estes processos de governação e gestão;
- ✓ Processos novos e modificados, que incluem uma reestruturação individual dos processos de TI e descrição de cada atividade;
- ✓ Objetivos e métricas;

- ✓ Novas matrizes de responsabilidade;
- ✓ Modelo de avaliação de maturidade e capacidade de processos;
- ✓ Distinção de governação e gestão.

Toda a *framework* sofreu uma reestruturação/reorganização de um modelo de processo de TI para uma *framework* de gestão e governação de TI da organização.

2.4. Avaliação de maturidade e capacidade de processos de governação de TI

De acordo com Cascata dos Objetivos da metodologia de gestão do COBIT é relativamente fácil determinar quais desses processos e em que extensões são importantes (Radovanovic D., Radojevic T., Lucic D. & Sarac M., 2010, p.3-4). As avaliações de maturidade são baseadas no modelo CMMI adquirido pelo ISACA em 2016, onde o modelo COBIT demonstra ser muito detalhado e capaz de explicar cada processo. A avaliação da maturidade dos processos de governação de TI está definida num intervalo de 0 a 5:

- 0 - Não existem processos, ou seja, os processos de governação de TI não existem. A gestão de topo não reconhece a importância deste conceito, o que torna as decisões sobre os investimentos em TI descontroladas, fora da supervisão do sistema e avaliação de risco;
- 1 – Existem processos iniciais, a organização depara-se com a existência de problemas e a necessidade de resolução dos mesmos, embora não existam procedimentos formais, a gestão e supervisão das TI é baseada principalmente numa base individual e não controlada e as ações são tomadas individualmente (caso a caso). Não existem normas, nem regras organizacionais, nem obrigações e responsabilidades em relação a este assunto. A gestão de topo geralmente não está totalmente ciente da importância do risco de TI. A governação de TI e a sua medição de desempenho são atividades que são executadas dentro do departamento de TI e na gestão não existe qualquer instrução ou conhecimento deste assunto.
- 2 – Existem processos repetidos e processos de governação de TI que seguem um padrão regular, mas são descoordenados e iniciados principalmente pelo departamento de TI ou a outro nível organizacional. Muitas vezes acontece que diversas pessoas realizam a mesma tarefa (questão de segregação de funções). Não existe formação e as políticas organizacionais não existem ou não são transmitidas aos colaboradores.

- 3 – Existem processos definidos, os procedimentos de governação de TI estão claros e documentados e constantemente aprimorados através de formações. Os procedimentos e regras organizacionais, embora existam formalmente, não são sofisticados, maduros nem orientados ao modelo do negócio da organização. Estes representam apenas a formalização dos procedimentos existentes. Embora existam procedimentos, a responsabilidade pela sua execução contínua não tem qualquer supervisão do sistema, é improvável que se possam detetar anomalias relativas a este nível.
- 4 – Os processos de gestão existentes, procuram aplicar as políticas e procedimentos organizacionais. Também é possível monitorizar constantemente a sua execução, medir o desempenho e fazer as correções necessárias de acordo com as necessidades. Os processos e atividades são continuamente aprimorados. Os objetivos são muito sofisticados de governação de TI, estreitamente alinhados com os objetivos de negócio que os definem. Usam os métodos e *frameworks* atuais e as devidas atualizações (COBIT, BSC, ITIL e outros normativos) na medição de desempenho, no entanto, a auditoria de TI é necessária.
- 5 – Os processos existentes estão otimizados. Existe um domínio dos processos de governação de TI que estão considerados num nível ótimo. As melhores práticas são seguidas e automatizadas, os processos foram aprimorados para um nível de melhores práticas, com base nos resultados de melhoria contínua e *benchmarking* com outras organizações e melhores práticas do setor. Uma tal transparência na governação de TI, os responsáveis organizacionais têm supervisão sobre a TI através de uma série de mecanismos de controlo. As TI são utilizadas como elementos de apoio e suporte aos objetivos estratégicos, como recurso e informação de negócio e atividades (investimentos, projetos, riscos, etc.) funcionam de forma ótima se alinhadas com as prioridades do negócio.

2.5. Perigos ao evitar a *framework* COBIT 5

As organizações que não implementem ou utilizem uma *framework* de governação e gestão de TI, como o COBIT 5, começam a deparar-se com diversos desafios. Verifica-se assim:

- Risco na falta de conformidade com regulamentos ou legislação relevante dos quais são exigidos internamente pela entidade ou até mesmo entidades externas, que podem resultar em penalidades, coimas, perda potencial no negócio, entre outros.

- ✗ É suscetível existirem processos de governação de TI ineficazes, por exemplo, EDM e também processos orientados à gestão ineficazes (políticas de gestão ou avaliação). No entanto esta ineficácia é vital para o departamento TI responder às necessidades da organização;
- ✗ Alta probabilidade de uma governação de TI ineficaz ou até mesmo não existente, que pode significar pouco envolvimento (ou nenhum) do departamento TI, o que leva à falta de responsabilidade por falhas em iniciativas TI;
- ✗ Por último, existe um risco elevado de ausência de alinhamento entre o departamento de TI e os objetivos/estratégia da organização, que conduz a decisões pouco consistentes e sem conhecimento prévio do real valor das TI. Consequentemente podem originar gastos não controlados de TI. Por outro lado, a falta de alinhamento causado por iniciativas TI contribui para a fraca inovação e obtenção de benefícios pretendidos pela organização.

2.6. Auditoria aos SI

Auditoria pode ser definida como uma avaliação sistemática pela qual uma equipa competente e independente obtém e avalia objetivamente as asserções sobre uma entidade ou evento económico, com a finalidade de emitir uma opinião sobre o grau de conformidade com um conjunto de normas e padrões.

Note-se que uma discussão sobre auditoria deve incluir o âmbito da auditoria, objetivos da auditoria, critérios, procedimentos de auditoria, evidências, conclusões e opiniões, bem como relatórios.

A auditoria aos SI pode ser definida como qualquer auditoria que englobe a revisão e avaliação (total ou parcial) de sistemas automatizados de processamento de informações, processos não automatizados relacionados e as interfaces entre eles.

Numa perspetiva de auditoria e avaliação, o COBIT tem um forte impacto na monitorização e permite a avaliação dos processos e estruturas de governação de TI existentes, através de um testemunho com a certificação em auditoria aos SI. O auditor de SI deve entender os procedimentos para testar e avaliar os controlos de SI.

Esses procedimentos podem incluir:

- ✓ O uso de *softwares* de auditorias generalizadas para pesquisar o conteúdo de bases de dados (incluindo *logs* do sistema);

- ✓ A utilização de *softwares* especializados para avaliar o conteúdo das bases de dados e parâmetros do sistema operativo (ou detetar deficiências nas configurações dos parâmetros do sistema);
- ✓ Técnicas aplicadas através de fluxogramas para documentar aplicativos automatizados a processos de negócio;
- ✓ O uso de relatórios de auditoria disponíveis através de sistemas operacionais;
- ✓ Revisão de documentação;
- ✓ Observação.

Neste sentido, os padrões e diretrizes de auditoria aos SI da ISACA estabelecem muitas especificações sobre a documentação de auditoria, incluindo, como usá-las por outros auditores ou a necessidade de documentar o plano de auditoria, programa e evidência ou o uso de CAATs ou amostragens, entre outros.

Como tal, para os auditores de SI qualquer tecnologia capaz de aumentar a produtividade da auditoria é bem-vinda. A automatização de papéis de trabalho afeta a produtividade diretamente de maneira óbvia e também indiretamente (concedendo acesso a outros auditores, reutilizando documentos ou partes deles em auditorias recorrentes, etc.)

O risco de auditoria pode ser definido como o risco das informações / relatório financeiro, poderem conter erros materiais que podem passar despercebidos durante a auditoria. Cada vez mais as organizações optam por uma abordagem de auditoria baseada em risco, que no geral é adaptada para desenvolver e melhorar o processo contínuo de auditoria. Esta abordagem é usada para avaliar riscos e para auxiliar a decisão de um auditor de SI, com o objetivo de serem realizados testes de conformidade ou testes substantivos.

Uma abordagem de auditoria baseada numa análise de risco, feita assim, os auditores de SI não se baseiam apenas no risco, mas também nos controlos internos e operacionais, bem como, o conhecimento da empresa ou das áreas de negócio. Este tipo de decisão de avaliação de risco pode ajudar a relacionar a análise de custo-benefício do controlo ao risco conhecido, permitindo escolhas práticas.

Compreendendo a natureza do negócio, os auditores de SI podem identificar e categorizar os tipos de riscos que determinarão melhor o modelo ou a abordagem de risco na condução da auditoria.

Numa visão orientada da auditoria aos SI, o conceito de materialidade requer um julgamento correto do auditor de SI. O auditor de SI pode detetar um pequeno erro que pode ser considerado significativo a nível operacional, mas pode não ser considerado significativo para a gestão de topo.

As considerações de materialidade combinadas com um entendimento do risco de auditoria são conceitos essenciais para planear as áreas a serem auditadas e o teste específico a ser realizado numa determinada auditoria.

A materialidade pode ser mais difícil de interpretar para o auditor de SI. Por exemplo, uma configuração de parâmetro de segurança lógica que permite a um programador aceder, sem autorização, ao código-fonte de todos os programas pode ser um erro material. Da mesma forma, acessos a apenas alguns programas mais insignificantes podem não ser considerados materiais para o auditor de SI. A materialidade aqui é considerada em termos do impacto potencial total para a organização.

2.7. Cruzamento do COBIT com a Auditoria e o Controlo Interno.

Ao nível organizacional, a função de governação e de controlo interno encontram-se por vezes separadas, conduzindo a uma falta de comunicação, ineficácia nos controlos e para a falta de capacidade de criar valor para os *Stakeholders.*

A auditoria interna tem vindo a ser designada como o "novo pilar da gestão", devido a posicionar-se como um elemento-chave na estrutura organizacional, contribuindo assim para o reforço do controlo interno, gestão de risco e governação da empresa.

A *framework* COBIT 5, surge pois como uma *framework* de orientação para as boas práticas de governação e gestão da organização, tem um papel relevante no aparecimento da função de auditoria interna como novo pilar em vários domínios. O modelo de governação consegue simplificar e eliminar as ineficácias nos vários departamentos, alinhando os controlos existentes com os objetivos corporativos, criando uma metodologia que se aplica em toda a organização apoiando as funções de gestão de risco e conformidade. (ISACA News, 2015).

Os controlos internos são definidos através de um ambiente de controlo, onde o COBIT 5 sustenta o mesmo ambiente através dos *enablers* (já referido nos cinco princípios explanados anteriormente). O tratamento destes *enablers* são o elemento chave para o sucesso da execução de uma auditoria, numa medida implementada, no sentido em que, todo o seu conjunto de recursos permite uma abordagem e visão holística da organização (ISACA HQ, 2017).

Ao nível de auditoria, torna-se assim indispensável, a utilização da *framework* COBIT 5 como uma ferramenta orientadora em relação ao âmbito da auditoria, sobre qual o procedimento de auditoria a executar conforme a tarefa do COBIT 5 selecionada (ISACA Astana, 2018).

2.8. O COBIT 2019

Existiu um esforço enorme da ISACA em reestruturar a *framework* COBIT 5 para colmatar aquilo que podiam ser as suas fragilidades, como foi anunciado em novembro de 2018 a última atualização da sua *framework*, o COBIT 2019, que evolui do COBIT 5, sendo esta a resposta da ISACA à comunidade que estava insatisfeita com um conjunto de aspetos do COBIT 5, nomeadamente, o facto de não se conseguir transmitir a essência da própria *framework*.

No entanto, a ISACA continuará a prestar suporte às organizações que tenham introduzido o COBIT 5 e que tencionem manter essa versão.

Importa neste contexto clarificar algumas atualizações do COBIT 2019.

De acordo com o evento decorrido na 3ª Conferência Internacional do ISACA *Lisbon Chapter* **(**Anexo 5**)**, *Webinar* – Introdução ao COBIT 2019 do ISACA e Welcome COBIT 2019! do ISACA Lisbon Chapter e após a publicação das *guidelines*, foi possível verificar algumas diferenças da versão antecessora COBIT 5 para o COBIT 2019. Basicamente incluem:

- ✓ Princípios modificados (de 5 para 6);
- ✓ Novas áreas que merecem atenção;
- ✓ Elementos de construção para novos objetivos de governação e gestão;
- ✓ Alterações nos processos e na sua designação, agora designados como Objetivos de Governação e Gestão, como se pode verificar na figura 2.8 (um novo objetivo e o desdobramento de um objetivo em dois, passou-se de trinta e sete para quarenta objetivos), cinco objetivos de governação, trinta e cinco objetivos de gestão, identificando-se no total quarenta objetivos que são suportados. Em termos práticos, cada um dos objetivos está detalhado, quais são os processos que os alimentam, as estruturas organizacionais, as políticas, a cultura, os serviços, infraestruturas e aplicações e as competências;
- ✓ Atualização da Cascata dos Objetivos;
- ✓ O conceito "componentes de governação" substituiu os *enablers* do COBIT 5;
- ✓ Novos objetivos foram detalhados em termos de governação e gestão.

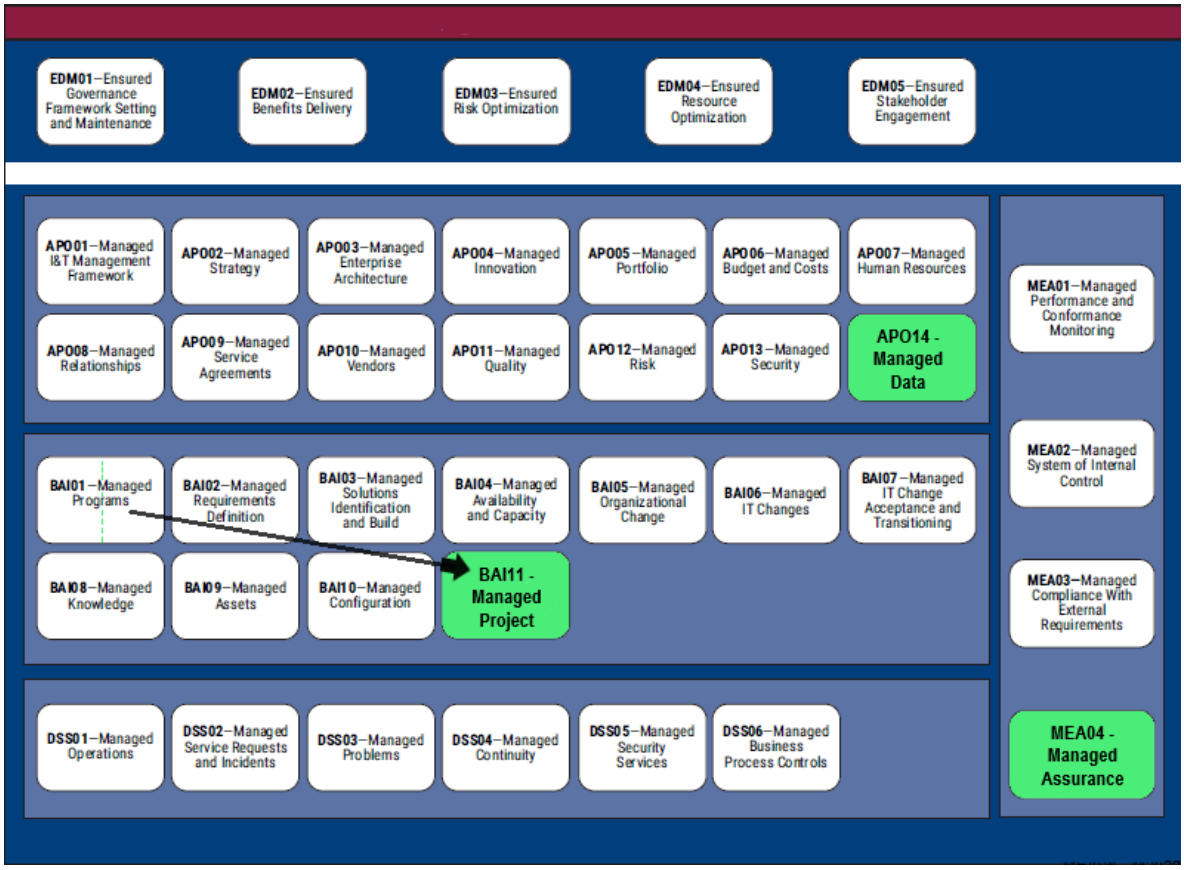


Figura 2.8 - Adaptado do Modelo do COBIT 2019 (Objetivos), **Fonte:** COBIT® 2019, 2018

O ISACA procurou reforçar tudo aquilo que a *framework* COBIT é (e que não é) ou seja:

- ✓ Indicar que é uma *framework* para que os objetivos corporativos e os objetivos de IT estejam alinhados, no contexto dos SI;
- ✓ Clarificar que não é uma norma, logo, não se implementa:
- ✓ Comunicar aos profissionais que não existe uma certificação COBIT, logo, não é possível auditar contra a própria *framework*;
- ✓ É uma *framework* de referência, utiliza-se e adapta-se.

Sendo que o "adapta-se" é a palavra-chave para o COBIT 2019 com a introdução de uma nova ferramenta na nova estrutura da *framework*, designada de *"Design Factors"* visível na figura 2.9. No mesmo contexto do COBIT 5, a *framework* pretende acompanhar a linha de transformação tecnológica, garantindo assim uma visão ainda mais holística, introduzindo um novo processo, a Gestão de Dados identificado como APO14.

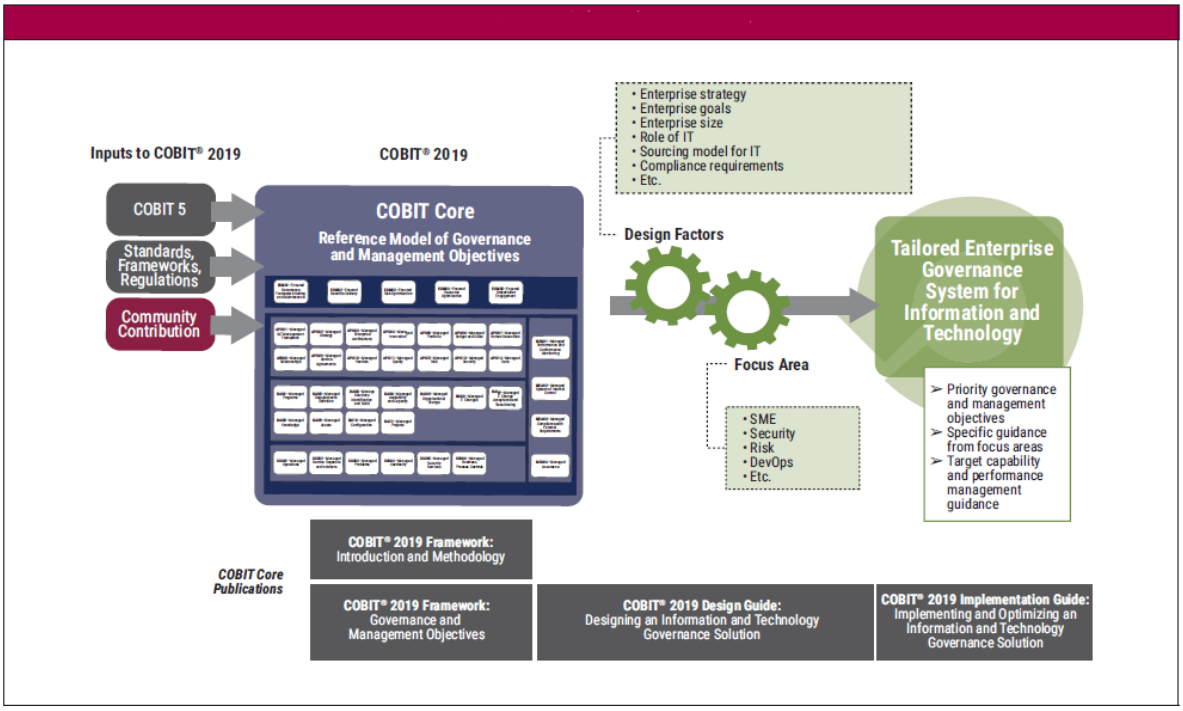


Figura 2.9 - Visão Geral do COBIT 2019, **Fonte:** COBIT® 2019, 2018

Finalmente é importante reter que a *framework* COBIT não entra na "guerra comercial" das *frameworks* ao nível operacional, ou seja, não é de nenhuma área de risco ou de controlo, mas sim, apresenta-se como elemento de apoio que são transversais à organização, conhecidas como áreas de governação e gestão. Perante esta visão, aparentemente, permite acrescentar valor à organização através dos SI, ao nível da satisfação das necessidades das partes interessadas, da otimização dos componentes e da mitigação de riscos.

3. Métodos e procedimentos

A presente investigação é resultado de um diagnóstico das necessidades de informação e seleção que todas as variáveis relevantes, análise prática em contexto de negócio, registos validados e fiáveis com o objetivo de apresentar um trabalho científico e independente.

Foram utilizados diversos métodos de investigação científica, observação direta, método crítico, método inquisitivo, em que as técnicas utilizadas para recolha de dados foram feitas através de um questionário, assente na observação crítica dos acontecimentos e método sistemático, tendo sido este instrumento baseado nos interrogatórios escritos e orais realizados, ou seja, através do método inquisitivo já referido.

É importante referir também que para a necessária interpretação dos acontecimentos, foram também utilizados os métodos histórico e indutivo. No primeiro método (histórico) foi importante analisar os fenómenos e processos em estudo, atendendo às reais aplicações práticas e potencial desenvolvimento, treino e formação dos eventos registados.

No que diz respeito ao método indutivo, baseando-se num raciocínio que parte do particular para o geral, a validade dos resultados depende sempre da representatividade da amostra e trabalho estatístico obtido através do questionário, sendo certo que este tipo de hipóteses de investigação permite obter "considerações gerais" e "conclusões".

A ferramenta analítica utilizada neste estudo é o procedimento padrão COBIT emitido pela ISACA, cujos dados puderam ser obtidos por diversos métodos, nomeadamente:

- o questionário, que foi distribuído pessoalmente a cada responsável pelo departamento de SI / TI (quando aplicável) e esteve estruturado em duas vertentes, com vista a entender quais são as preocupações da organização e quais são as preocupações do departamento de TI.

Tabela 3.1 - Questionário 1

Questionário 1 – Organização	
1	Em que setor se encontra inserida a sua organização?
2	Qual o cargo que tem na sua organização?
3	Qual o número médio de empregados durante o período?
4	Em que ano foi constituída a sua empresa?
5	Quais são as principais preocupações da sua organização?

Fonte: Autoria própria

As questões da tabela 3.1, permitem entender quais as preocupações da organização em função das necessidades das partes interessadas, considerando o setor e a dimensão em que se insere, o início da atividade e o cargo do respondente, priorizando três preocupações.

De acordo com o Apêndice D (Anexo 1), foi apresentada aos respondentes apenas a lista com os dezassete objetivos organizacionais previstos no COBIT 5 de modo a refletir melhor quais as preocupações da organização em que estão inseridos.

Tabela 3.2 - Questionário 2

	Questionário 2 – Departamento de TI
1	Que processos foram implementados para a mitigação das preocupações?
2	Quais foram as metodologias que serviram de base para os processos?
3	Existe um responsável pela área dos processos implementados?
4	Existe um departamento de Sistemas de Informação (SI) ou Tecnologias de Informação (TI) na sua organização?
5	Se respondeu sim à questão anterior, indique quais são as principais preocupações do departamento de SI/TI?
6	Que processos foram implementados para a mitigação das preocupações?

Fonte: Autoria própria

As questões da tabela 3.2, permitem entender quais as preocupações do departamento de TI da organização, com vista a claraficar quais os processos que estão automatizados, formalizados, sistematizados, estáveis que efetivamente foram implementados.

De acordo com o Apêndice B (Anexo 2), foi apresentada aos respondentes apenas a lista com os dezassete objetivos do TI previstos no COBIT 5 de modo a compreender quais as suas preocupações neste domínio.

A importância indicada nas questões n.º 5 e 10 corresponde a uma pontuação que é distribuída entre 1-17 pontos de acordo com a prioridade escolhida, sendo a primeira prioridade 17 pontos e a última prioridade 1 ponto - onde **X** é o somatório das várias posições que a preocupação escolhida teve ao longo das respostas e **N** o número de preocupações (17). Assim a fórmula utilizada para calcular a importância através do Survio, um sistema de preparação de questionários, recolha e análise de dados e partilha dos resultados, é $\mathbf{R} = \frac{\boldsymbol{\Sigma X}}{\boldsymbol{N}}$, onde **R** é a importância referida. Por último, é definida uma posição ordinal correspondente ao valor obtido em **R**.

Na sequência das respostas obtidas é possível avaliar através da *framework* COBIT se as preocupações do departamento de TI estão alinhadas com os objetivos da organização tendo em conta as necessidades das partes interessadas, caso contrário, quais deveriam ser as reais e importantes preocupações.

4. Descrição dos dados

4.1. Introdução

Para responder às questões centrais da investigação, os estudos de caso trataram de validar de empresas e indivíduos em particular. Por motivos de privacidade e confidencialidade, como já foi referido, não será possível dar a conhecer o nome exato das empresas e dos inquiridos, pelo que, simplesmente são designados por letras conforme vão surgindo ao longo desta análise.

4.2. Amostra da investigação

Os dados recolhidos nesta investigação incluem uma avaliação de dois conjuntos de questões de 21 entrevistados cujas respostas individuais não foram rastreáveis. Para produzir a lista classificada de objetivos gerais da organização e de TI, as avaliações das duas secções do questionário foram analisadas para fornecer uma pontuação total que evidenciam as principais preocupações da perspetiva dos respondentes. Os dados foram classificados em ordem decrescente com base nos totais com apoio do Survio.

Com base nas considerações dos questionários feitos, uma tabela de especialistas e responsáveis foi composta por 19 profissionais de diversos setores, todos com conhecimento para responder as questões em causa. Através do método inquisitivo, 21 especialistas estiveram envolvidos na recolha dos dados num total de 135 elementos que compõem a amostra, existindo 2 que foram descartados por não se enquadrarem no perfil pretendido. A distribuição dos 19 perfis envolvidos na pesquisa é mostrada na tabela 4.6 do ponto 4.3 de acordo com o setor, dimensão e antiguidade.

Adicionalmente, foram realizadas duas entrevistas com dois auditores de SI, um dos quais com certificação CISA, que responderam abertamente às questões que lhes foram colocadas no âmbito da *framework* COBIT, desde a sua evidência à sua aplicabilidade, ou contribuíram através da sua experiência e visão própria, para a presente dissertação.

Estas duas últimas entrevistas revelaram-se fundamentais para melhorar a seleção das questões dos 21 entrevistados e das suas respetivas análises das conclusões.

Entrevista – Sujeito A

No encontro com o entrevistado A, alto quadro de uma das maiores empresas portuguesas, foram coocadas as questões e obtidas as respostas que a seguir se apresentam:

Q. A1: A organização ou o departamento de TI baseia-se ou tenciona adotar a metodologia da *framework* COBIT?

R. A1: "Não. Que seja do meu conhecimento, a *framework* COBIT não é utilizada em Portugal, o nível de investimento associado à sua utilização é exorbitante face à realidade nacional. Poderá por vezes, não ser utilizada totalmente na organização, mas sim parcialmente para algumas situações específicas."

Q. A2: "Qual é a sua opinião quanto à aplicabilidade e utilização da *framework COBIT?"*

*R. A2: "*A aplicabilidade de metodologias tem muito que se diga, ou seja, qualquer metodologia deve ser vista como um indicador. Quem faz tudo *by the book*, seguindo à risca a metodologia utilizada é bastante provável que não funcione, existindo a necessidade de adaptar. Como auditor, a *framework* COBIT é vista como um «chapéu» de referências."

Q. A3: "Concorda que a *framework* COBIT acrescenta valor aos profissionais de auditoria?"

R. A3: "Como auditor aos sistemas de informação, a dificuldade prende-se na avaliação da eficácia dos controlos, para tal, é preciso entender na íntegra quais são os objetivos de controlo.

Numa perspetiva dos controlos de TI, os mesmos podem ser mais facilmente monitorizados e auditados quando o objetivo em causa é organizado de forma clara.

Posto isto, a vantagem da *framework* COBIT é que ajuda o auditor a identificar quais são esses objetivos.

O *Process Capability Model*, indica ao auditor quais os processos que merecem uma maior atenção face ao seu nível de maturidade através dos níveis descritos na *framework* COBIT, permitindo uma avaliação com maior rigor e confiança durante a execução da auditoria."

Nota: Para melhor compreensão do *Process Capability Model* ver Anexo 4.

Entrevista – Sujeito B

Para uma segunda entrevista, foi estabelecido o contacto no âmbito do evento "3ª Conferência Internacional do ISACA Lisbon Chapter" com Osman Azab, Diretor Geral Adjunto no *Arab International International Bank* e antigo Vice-Presidente da ISACA de Egito, com certificações CISA, CISM, CGEIT, CRISC. Na reunião acordada com o referido responsável foi manifestado, pelo próprio, o interesse de contribuir para a dissertação, não através de questionário pré-definido, tal como verificado no Sujeito A, mas através da sua experiência e visão pessoal destas matérias. Para Osman Azab, o auditor deve seguir questionários devidamente focalizados de forma a apoiar o auditor a perceber e avaliar, na fase do Planeamento do Compromisso de Auditoria Interna, o estado corrente da governação de TI na organização.

Neste sentido, o entrevistado, proporcionou um conjunto de questionários com cinco focos que serviram como contributo para a investigação e que a seguir se apresentam:

Estruturas de organização e governação

As questões seguintes permitem o auditor interno a entender o grau ou a presença da governação de TI na organização:

Tabela 4.1 - Estruturas de Organização e Governação

Questões	**Avaliação**
Existe um CIO destacado cuja função é de um membro da equipa de gestão *sénior*?	
A estrutura da organização e seus componentes operacionais estão organizados de forma clara, de modo que a função de TI possa ajudar de forma eficiente e eficaz a alcançar os objetivos da organização?	
Existe alguém responsável pela tomada de decisão para permitir o alinhamento das necessidades organizacionais com os serviços de TI e eles têm a capacidade de responder e ser responsabilizados pelos atos?	
As necessidades da organização e os requisitos de serviços de TI são definidos em planos estratégicos e monitorizados?	
O CIO e a gestão de topo reúnem e discutem o progresso dos planos regularmente?	

Liderança executiva e suporte

As questões seguintes permitem ao auditor interno entender o grau de envolvimento da função de TI na organização:

Tabela 4.2 - Liderança Executiva e Suporte

Questões	Avaliação / Comentários
A gestão de topo define claramente e comunica as funções e responsabilidades para a função de TI com vista ao sucesso das estratégias delineadas pela organização?	
O papel e as responsabilidades do CIO estão claramente definidos e comunicados?	
A organização reconhece na elaboração da estratégia que a função de TI é um fator que contribui significativamente para o sucesso dos objetivos, bem como, apoiar a organização numa base diária?	
O CIO reúne com regularidade com os superiores hierárquicos e com a gestão de topo para discutir e comunicar o serviço prestado pela função de TI relacionado com os planos estratégicos estabelecidos?	
O departamento de TI tem o apoio financeiro adequado para atender às necessidades da organização?	

Planeamento Estratégico e Operacional

As questões seguintes permitem ao auditor interno a perceber o desempenho do planeamento estratégico implementado pela gestão de topo:

Tabela 4.3 - Planeamento Estratégico e Operacional

Questões	Avaliação / Comentários
O conselho de administração e a gestão consideram o departamento de TI como uma função organizacional estratégica?	
O plano estratégico da organização refere como a função de TI é necessária para apoiar e permitir acrescentar de valor À organização?	
O plano estratégico é apoiado por planos operacionais específicos que têm em conta os requisitos e a prestação de serviço de TI?	
Os principais indicadores de desempenho (KPIs) são utilizados pela gestão para medir e monitorizar a eficácia da função de TI?	
As decisões estratégicas de investimento em TI são baseadas em análises precisas de benefícios de custo e avaliadas após a implementação para determinar se o ROI esperado foi realizado?	
Os resultados obtidos são considerados nas futuras decisões de investimento em TI pela administração e gestão de topo?	
A organização do departamento de TI está estruturada de forma eficaz em relação à dimensão e composição da organização?	
O CIO e os responsáveis em TI são qualificados e experientes?	

Mensuração e prestação de serviços

As questões seguintes permitem o auditor interno a entender se gestão financeira da função de TI é adequada:

Tabela 4.4 - Mensuração e Prestação de Serviços

Questões	**Avaliação / Comentários**
A administração e a gestão de topo têm uma noção clara dos custos envolvidos com a função de TI e como os mesmos contribuem para a realização dos objetivos estratégicos da organização?	
Os administradores da organização mensuram o valor (criado, acrescentado e preservado) com a função de TI? Se sim, como?	
São os custos de TI comparáveis com os custos de outras organizações?	
O desempenho do CIO é mensurado por dados financeiros e não financeiros?	
Existem serviços de *outsourcing*? Se sim, eles são mensurados e monitorizados?	

Organização de TI e a gestão de risco

As questões seguintes permitem o auditor interno perceber o ambiente de governação de TI:

Tabela 4.5 - Organização de TI e a Gestão de Risco

Questões	**Avaliação / Comentários**
Até que ponto os processos montados pela organização são automatizados, formalizados, sistematizados e estáveis?	
Qual é o grau de complexidade da infraestrutura de TI e quantas aplicações/processos estão em uso?	
Os dados seguem um padrão e são facilmente partilhados entre aplicações e a infraestrutura de TI?	
Existem políticas, procedimentos e controlos padrão de *hardware, software* e aquisição de serviços?	
Qual é a maturidade dos processos de gestão de TI? Existem *frameworks* reconhecidas que servem de base de orientação (por exemplo, COBIT, ITIL, ISO)?	
Como funciona a gestão de risco em relação ao atendimento das necessidades de segurança e requisitos de conformidade da organização?	
Qual é a importância estratégica da função de TI?	

4.3. Análise e discussão de dados

Este capítulo examina e analisa os resultados dos dados recolhidos. Está dividido em três partes, conforme detalhado no Capítulo 3, em dois conjuntos de questões e uma discussão final.

Num primeiro conjunto, descreve as especificações dos respondentes (características da amostra) em termos de setor, cargo, dimensão e antiguidade da organização.

No segundo conjunto de questões, é pretendido conhecer o grau de presença de gestão e governação a nível organizacional e especificamente do departamento de TI.

Por último, através das respostas obtidas referentes às preocupações definidas numa lógica de prioridades, é feito o levantamento se existe (ou não) o alinhamento entre os gestores de topo e o departamento de TI.

Primeiro conjunto

Questões 1 a 4:

O maior número dos respondentes inquiridos (19 num total de 135) foi do setor de prestação de serviços que contempla a área da contabilidade, consultoria e auditoria, no entanto, também se pode verificar outros setores que são relevantes para a investigação em causa, conforme podemos ver na tabela seguinte:

Tabela 4.6 - Caraterização da Amostra

Setor	Cargo	Número médio de empregados	Ano de constituição	Número de respostas
Prestação de Serviços	Contabilistas, Consultores e Auditores	Mais de 250	Entre 1845 a 2011	9
Aeroportuário	Auditor Interno	Mais de 250	1999	2
Indústria	*IT Senior Manager*	Mais de 250	1882	2
Retalho	Auditor de SI	Mais de 250	1980	2
Saúde	*IT Operations Manager*	Mais de 250	1994	1
Público	*IT Manager*	Entre 10 e 50	2010	1
Bancário	Gerente	Mais de 250	1986	1
Trading	Contabilista	Entre 10 e 50	2010	1

Fonte: Autoria própria

Questão 5:

A maioria dos respondentes são responsáveis pelo departamento em que exercem funções com uma proximidade / envolvência da governação e gestão da organização, podendo contribuir assim para uma melhor recolha de respostas validadas. A tabela seguinte indica quais foram as principais preocupações consideradas pelas organizações inquiridas:

Tabela 4.7 - Preocupações Gerais da Organização

Preocupações	Importância
Valor de investimento da organização percebido pelas partes interessadas.	1º
Portfólio de produtos e serviços competitivos.	2º
Conformidade com as leis e regulamentos externos.	3º
Cultura de serviço orientada ao cliente.	4º
Gestão do risco do negócio (salvaguarda de ativos).	5º
Continuidade e disponibilidade do serviço de negócio.	6º
Transparência financeira.	7º
Respostas rápidas para um ambiente de negócio em mudança.	8º
Otimização dos custos de prestação de serviços.	9º
Tomada de decisão estratégica com base na informação.	10º
Otimização da funcionalidade do processo de negócio.	11º
Otimização dos custos do processo do negócio.	12º
Produtividade operacional e da equipa.	13º
Pessoas qualificadas e motivadas.	14º
Cultura de inovação de produtos e negócios.	15º
Gestão de programas de mudanças de negócios.	16º
Conformidade com as políticas internas.	17º

Fonte: Autoria própria

É importante relembrar que durante a análise da tabela anterior, foi solicitado que os respondentes dessem prioridade apenas a três preocupações, não obstante este critério, os respondentes priorizaram dezassete opções possíveis.

Aplicando a fórmula descrita no Capítulo 3 – Métodos e procedimentos, foi possível determinar as preocupações com maior importância.

Verificou-se que o valor de investimento da organização percebido pelas partes interessadas foi a primeira prioridade e aquela com maior importância.

No entanto, o portfólio de produtos e serviços competitivos e a conformidade com as leis e regulamentos externos foram a segunda e terceira prioridade, sendo as preocupações seguintes mais importantes.

Apesar de terem sido estas consideradas as mais importantes, deve-se referir que a cultura de serviço orientada ao cliente e a conformidade com as leis e regulamentos externos apresentam uma preocupação igualmente relevante da amostra considerada.

Quanto à lógica de prioridade, a terceira opção dos respondentes mais considerada foi gestão do risco do negócio (salvaguarda de ativos), ou seja, a ordem decrescente das preocupações no que corresponde à prioridade foram: 1º - Valor de investimentos da organização percebidos pelas partes interessadas; 2º - Portfólio de produtos e serviços competitivos; e, 3º - Gestão do risco do negócio (salvaguarda de ativos).

Segundo conjunto

Questão 6:

Os processos e as medidas (mais relevantes) que foram adotadas e consideradas para a mitigação das preocupações de acordo com o setor e principais preocupações organizacionais foram:

Tabela 4.8 - Processos e medidas de mitigação (Objetivos Gerais)

Setor		**Preocupações**	**Processos**
Prestação de Serviços	Recursos Humanos	• Conformidade com as leis e regulamentos; • Gestão do risco do negócio (salvaguarda de ativos); • Conformidade com as leis e regulamentos externos.	• Criar e implementar (automatização de processos): • Ciclos de aprovações; • Revisões de trabalho; • Auditorias internas; • Restrição de acessos.

	Distribuição Postal	• Continuidade e disponibilidade do serviço de negócio; • Respostas rápidas para um ambiente de negócio em mudança; • Otimização dos custos do processo do negócio.	• Aposta em novos produtos; • Processos de distribuição mais eficientes.
	Contabilidade, Consultoria	• Conformidade com as leis e regulamentos externos; • Portfólio de produtos e serviços competitivos; • Tomada de decisão estratégica com base na informação.	• Contratação de pessoal qualificado (formação contínua).
Aeroportuário		• Continuidade e disponibilidade do serviço de negócio; • Portfólio de produtos e serviços competitivos; • Gestão do risco do negócio (salvaguarda de ativos).	• SIG - Sistema de Informação Geográfica.
Indústria		• Valor de investimentos da organização percebidos pelas partes; • Transparência financeira; • Cultura de inovação de produtos e negócios.	• Processo de transferência de conhecimento.

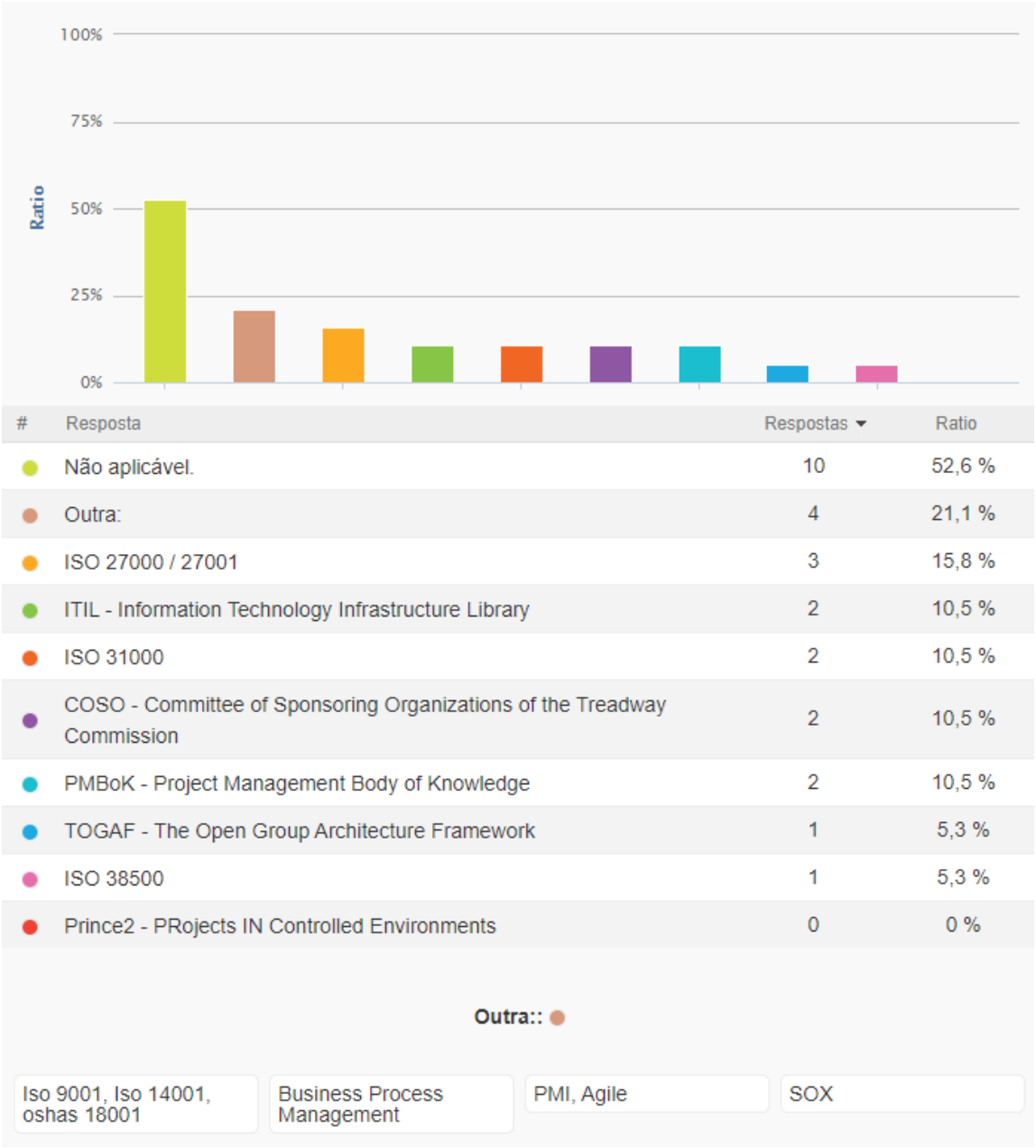
Retalho	• Cultura de serviço orientada ao cliente; • Respostas rápidas para um ambiente de negócio em mudança; • Cultura de inovação de produtos e negócios; • Continuidade e disponibilidade do serviço de negócio.	• Processos de suporte operacional e de gestão de projetos baseados em ITIL, PMI e Agile; • Identificação de necessidades de controlo através de auditorias aos processos de governação tendo por base a *framework* COBIT 5; • Controlo nas aprovações de serviços.
Bancário	• Cultura de serviço orientada ao cliente; • Tomada de decisão estratégica com base na informação; • Transparência financeira.	• Melhoramentos de *software* e *hardware*.

Fonte: Autoria própria

Durante a recolha de respostas, vários respondentes preferiram não responder à questão 6 (na sua totalidade ou parcialmente) por questões profissionais.

Questão 7:

Ainda no âmbito da gestão a nível organizacional, foi pedido aos respondentes que indicassem quais as metodologias que serviram de base para a execucação dos processos. Na questão, foram sugeridas algumas metodologias e *frameworks*, através das quais o COBIT 5 foi desenvolvido, no entanto, dando a hipótese de indicar outras que tivessem sido consideradas pela organização em causa. No gráfico seguinte, podemos identificar as respetivas opções selecionadas:



#	Resposta	Respostas	Ratio
	Não aplicável.	10	52,6 %
	Outra:	4	21,1 %
	ISO 27000 / 27001	3	15,8 %
	ITIL - Information Technology Infrastructure Library	2	10,5 %
	ISO 31000	2	10,5 %
	COSO - Committee of Sponsoring Organizations of the Treadway Commission	2	10,5 %
	PMBoK - Project Management Body of Knowledge	2	10,5 %
	TOGAF - The Open Group Architecture Framework	1	5,3 %
	ISO 38500	1	5,3 %
	Prince2 - PRojects IN Controlled Environments	0	0 %

Outra::

Iso 9001, Iso 14001, oshas 18001	Business Process Management	PMI, Agile	SOX

Figura 4.1 - Metodologias aplicadas nas organizações **Fonte**: Própria

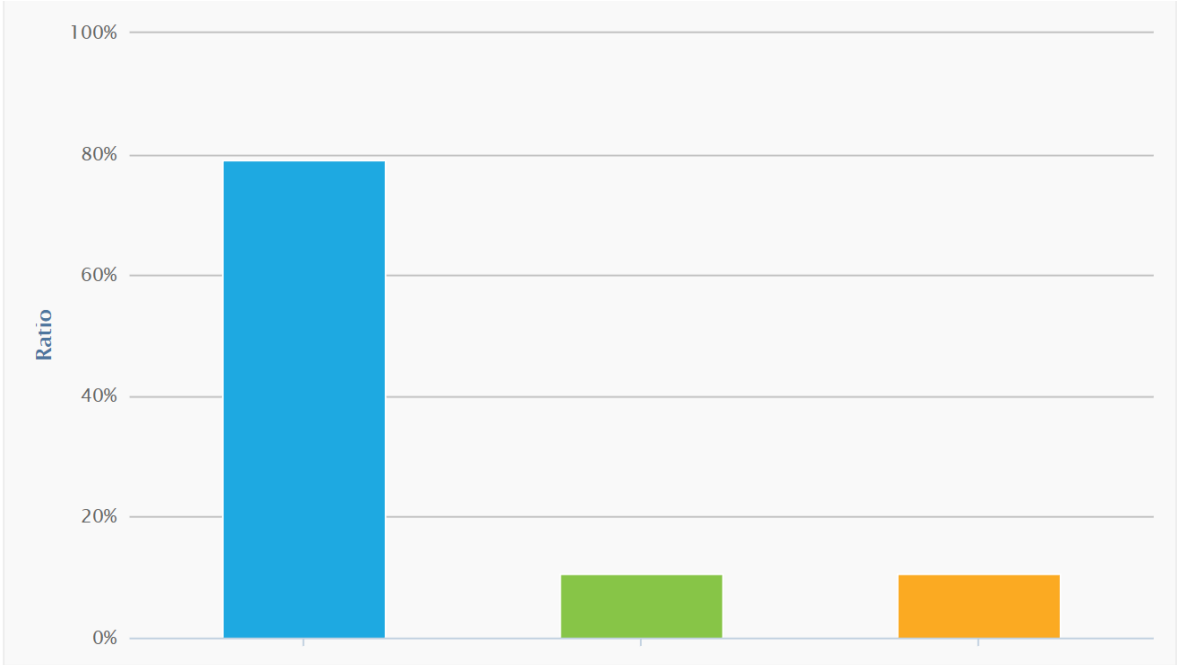
Das respostas obtidas, pode-se evidenciar que pelo menos uma das opções sugeridas foram selecionadas pelos respondentes (alguns selecionaram mais de que uma opção). Podendo assim, aproximar a organização a uma realidade onde o COBIT 5 seria um cenário possível.

Todavia, ainda se obtiveram respostas de carácter nulo, pelo que se verifica um alinhamento fraco entre a gestão organizacional e os respetivos respondentes, no entanto, por outro lado, deve-se pela inexistência da utilização de uma destas metodologias ou *frameworks.*

Contudo, foi possível obter algumas respostas fora das opções sugeridas, conforme se refere na opção “Outra”.

Questão 8:

Com vista a entender o grau ou a presença da governação na organização, o gráfico seguinte indica se existem responsáveis pelos processos implementados a nível organizacional:



#	Resposta	Respostas	Ratio
●	Sim.	15	78,9 %
●	Não.	2	10,5 %
●	Não sei.	2	10,5 %

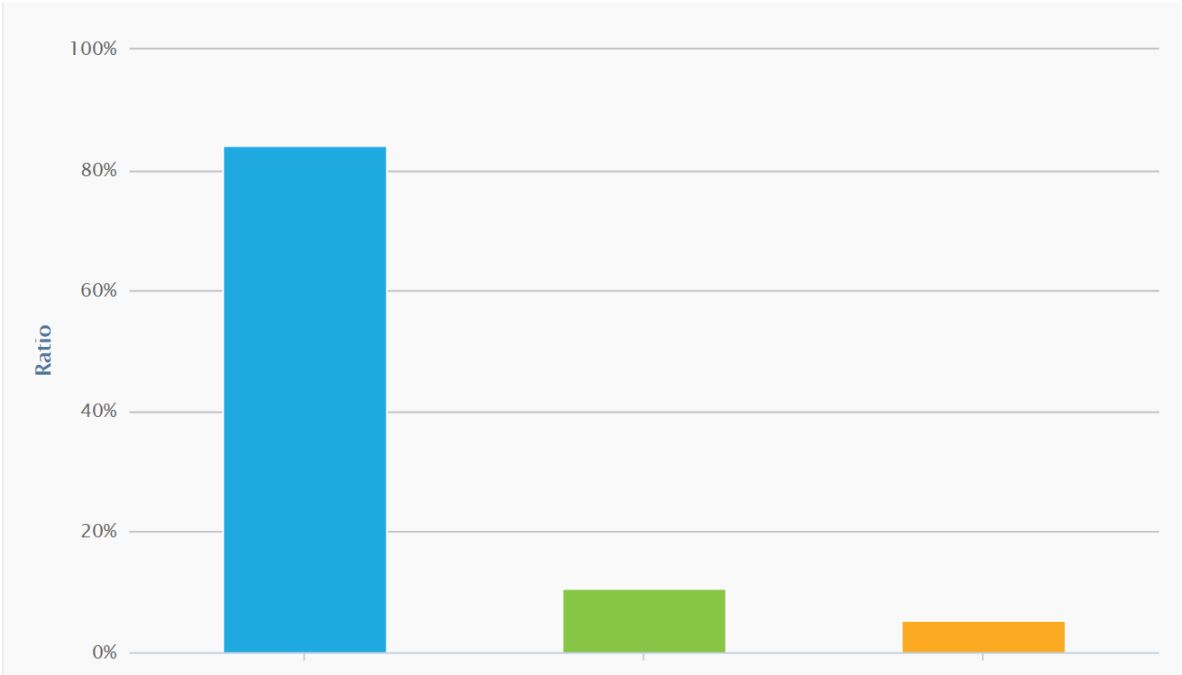
Figura 4.2 - Responsáveis dos processos (Objetivos Gerais) **Fonte:** Própria

Através das respostas obtidas nesta questão, apesar da maioria dos respondentes ser conhecedora dos responsáveis, os quatros respondentes em divergência evidenciam uma fraca presença de governação. Por outras palavras, para garantir a consistência em toda a organização, deve-se manter a um nível de comunicação efetiva e contínua em todas as áreas funcionais e responsabilidades exercidas.

Num cenário onde a comunicação é fraca entre os gestores de topo e as unidades organizacionais, consequentemente resultará num sistema ineficaz de planeamento e monitorização.

Questão 9:

A presente questão pretende evidenciar a existência de um departamento de SI ou TI organização, obtendo os seguintes valores nas respostas que se seguem:



#	Resposta	Respostas	Ratio
●	Sim.	16	84,2 %
●	Não.	2	10,5 %
●	Não sei.	1	5,3 %

Figura 4.3 - Existência de departamentos de TI / SI **Fonte:** Própria

Através das 16 respostas obtidas, foi possível avançar para uma investigação a nível de alinhamento entre a estrutura organizacional (com base nas preocupações da organização) e o departamento de TI (com base nas preocupações de TI).

Questão 10:

Foi solicitado aos 16 respondentes da questão anterior que dessem prioridade apenas a três preocupações, onde novamente, não obstante deste critério, os respondentes priorizaram as dezassete opções possíveis:

Tabela 4.9 - Preocupações de TI / SI

Preocupações	Importância
Alinhamento da estratégia de TI com as áreas de negócio.	1º
Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	2º
Compromisso do gestor executivo na tomada de decisões que envolve TI.	3º
Prestação de serviços de TI em consonância com os requisitos de negócio.	4º

Gestão do risco organizacional de TI.	5º
Benefícios obtidos pelo investimento de TI e portfólio de serviços.	6º
Transparência dos custos, benefícios e riscos de TI.	7º
Uso adequado de aplicações, informações e soluções tecnológicas.	8º
Segurança da informação, infraestrutura de processamento e aplicações.	9º
Agilidade de TI.	10º
Capacidade e apoio dos processos de negócio através da integração de aplicações e tecnologia presente nestes processos.	11º
Otimização de ativos, recursos e capacidades de TI.	12º
Criação de planos que resultam em benefícios, dentro do prazo, orçamento, e atendendo requisitos e padrões de qualidade.	13º
Disponibilidade de informações úteis e confiáveis para a tomada de decisão.	14º
Conformidade de TI com as políticas internas.	15º
Equipas de TI e de negócio motivadas e qualificadas.	16º
Conhecimento, especialidades e iniciativas para a inovação do negócio.	17º

Fonte: Autoria própria

Comparativamente à questão 5, para a análise da tabela anterior, foi solicitado que os respondentes dessem prioridade apenas a três preocupações, não obstante este critério, os respondentes priorizaram dezassete opções possíveis, desta vez, duas respostas não se enquadrarem no perfil indicado, por não existir departamento de TI.

Verificou-se que o "Alinhamento da estratégia de TI com as áreas de negócio" foi a primeira prioridade e aquela com maior importância. No entanto, a "Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos", foi a segunda prioridade. O "Compromisso do gestor executivo na tomada de decisões que envolve TI", foi a prioridade seguinte.

Apesar de terem sido estas consideradas as mais importantes, deve-se referir que a Prestação de serviços de TI em consonância com os requisitos de negócio apresentou uma preocupação igualmente relevante da amostra considerada.

Quanto à lógica de prioridade, as opções correspondem ao nível de importância supra referido.

Questão 11:

Os processos e as medidas (mais relevantes) que foram adotadas e consideradas para a mitigação das preocupações de acordo com o setor e principais preocupações do departamento de TI foram as seguintes:

Tabela 4.10 - Processos e medidas de mitigação (Objetivos de TI / SI)

Setor		**Preocupações**	**Processos**
Prestação de Serviços	Recursos Humanos	• Alinhamento da estratégia de TI e de negócios; • Prestação de serviços de TI em consonância com os requisitos de negócio; • Gestão do risco organizacional de TI.	• Implementação de Produtos Certificados em concordância com as políticas do grupo.
	Contabilidade, Consultoria	• Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos; • Compromisso do gestor executivo na tomada de decisões de TI; • Tomada de decisão estratégica com base na informação; • Capacidade e apoio dos processos de negócio através da integração de aplicações e tecnologia nos processos de negócio.	• Desenvolvimento interno de sistemas melhorados continuamente;
Aeroportuário		• Alinhamento da estratégia de TI e de negócios; • Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos; • Prestação de serviços de TI em consonância com os requisitos de negócio.	• SIG - Sistema de Informação Geográfica. • Gestão de processos (avalição de riscos); • Auditoria.
Indústria		• Alinhamento da estratégia de TI e de negócios;	• Processo de comunicação e

	• Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos; • Segurança da informação, infraestrutura de processamento e aplicações.	alinhamento com a estratégia do negócio. • Criação de plataformas com acesso direto *(IT Steering Committee)* • Restrição de acessos (acessos personalizados).
Retalho	• Alinhamento da estratégia de TI e de negócios; • Prestação de serviços de TI em consonância com os requisitos de negócio; • Agilidade de TI.	• Elaboração de PAR alinhado com as iniciativas e programas estratégicos da organização; • SAP – *System Application Products*.
Bancário	• Alinhamento da estratégia de TI e de negócios; • Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos; • Compromisso do gestor executivo na tomada de decisões de TI.	• Inovação (adoção de novas componentes tecnológicas).

Fonte: Autoria própria

O mesmo se aplica nesta questão durante a recolha de respostas, onde vários respondentes preferiram não responder a esta questão (na sua totalidade ou parcialmente) por questões profissionais.

Resultado da discussão

A *framework* COBIT 5, na perspetiva de uma organização não deve ter apenas uma abordagem financeira, mas também uma estrutura bem organizada para que os auditores mais facilmente entendam e comuniquem os resultados à gestão.

De acordo com o entrevistado designado de "Sujeito A", a base é entender na plenitude quais são os objetivos da organização. É muito difícil avaliar a eficácia do controlo, a menos que este seja claro com aquilo que se pretende alcançar.

No caso dos SI e TI, o controlo pode ser alvo de uma monitorização e auditoria eficiente quando o objetivo que implica o controlo é claro. A vantagem da *framework* COBIT 5 é que a mesma ajuda a evidenciar mais facilmente quais são esses objetivos. Portanto, deve partir da gestão e da governação, implementar os controlos e processos de um modelo com base nos objetivos da organização, permitindo executar autoavaliações, em que a própria gestão pode avaliar a eficiência da estrutura do controlo. A *framework* COBIT 5 acaba por ter apenas um controlo genérico: ajudar a que os objetivos da organização sejam atingidos.

Segundo o inquirido - Sujeito A-, o Modelo de Capacidade dos Processos (Anexo 4) presente no COBIT 5, surge como uma ferramenta útil para os auditores, não só oferece mais confiança durante a execução de auditoria, como também aumenta a frequência com que os processos são avaliados pelo auditor de acordo com o nível de maturidade definido pela organização.

Este modelo resulta numa base sólida para a realização de avaliações mais rigorosas, além de reduzir as divergências entre as partes interessadas sobre os resultados da avaliação.

Com base nas respostas obtidas, foi possível fazer um mapeamento entre os objetivos das organizações e os objetivos de TI (através das questões 5 e 10), cuja aferição resultou no Apêndice A e nos seguintes valores:

Tabela 4.11 - Alinhamento entre objetivos gerais e de TI

Grau de alinhamento entre objetivos gerais e de TI	**Número de organizações**
Alinhamento forte	7
Alinhamento médio	6
Alinhamento fraco	4
Não aplicável / Sem departamento	2

Fonte: Autoria própria

A tabela 4.11 foi criada com base nas informações do Apêndice B (Anexo 2 - ver 2º Princípio da *framework* COBIT), o que permitiu identifcar com facilidade quais os objetivos organizacionais que estão a ser apoiados pelos objetivos de TI.

No Apêndice B (Anexo 2), é detalhado, quais são os objetivos de TI que devem ser considerados primários de modo a contribuir diretamente para a consecussão dos objetivos organizacionais.

Em resumo:

- Duas organizações não se enquandraram na análise por não existir departamento de SI.
- Quatro organizações estão a disponibilizar e a utilizar inadequadamente os recursos de TI, não sendo capazes de prestar o apoio fundamental pretendido;
- Seis organizações, embora consigam cobrir todos os objetivos organizacionais através dos recursos de TI, estes não apresentam uma estrutura robusta e relação de causa e efeito importante;
- Sete organizações demonstraram ter os objetivos organizacionais cobertos por mais do que um objetivos de TI, apresentando uma boa estrutura de TI, capaz de prestar o apoio fundamental pretendido, no entanto, na tabela verifica-se que alguns objetivos de TI não estão devidamente alinhados, podendo resultar numa ineficiência de utilização de recursos.

No âmbito da auditoria, um auditor terá que considerar durante a execução do seu trabalho todos os processos e atividades que advém da Cascata de Objetivos, sendo que podem apresentar na área de controlo interno e com base na avaliação do risco, um nível de criticidade alto e com risco de não serem detetadas atividades que não foram alvo de uma auditoria.

Desta forma, pode dizer-se que o auditor pode beneficiar da *framework* COBIT para definir e priorizar objetivos da organização e de TI/SI, uma vez que a *framework* baseia-se no pressuposto de que as organizações existem para criar valor para os *Stakeholders*. Os auditores devem avaliar e relatar inequivocamente à gestão de topo das organizações se os benefícios são reais, se os riscos estão controlados e se os recursos se encontram otimizados.

5. Conclusões

5.1. Considerações gerais

Apesar da maior parte dos respondentes apresentar um perfil capaz de cobrir e apoiar os objetivos mais importantes da organização através dos recursos de TI/SI, deve-se dar ênfase à importância de uma boa estrutura de TI/SI. No entanto, percebe-se que as organizações ainda se deparam com problemas diferenciados, nomeadamente, como processar e melhorar a situação atual.

Por outro lado, os auditores devem adotar uma postura capaz de acompanhar a evolução neste âmbito, nomeadamente, a adesão de novas de tecnologias que fazem parte de qualquer estrutura organizacional nos dias de hoje e que estão relacionadas com TI/SI.

Conforme os resultados anteriormente apresentados, a principal preocupação do TI foi o "alinhamento da estratégia de TI e de negócio", pelo que se pode considerar, que a TI/SI embora independente do negócio, o seu objetivo é prestar suporte ao negócio.

É necessário estabelecer e manter a principal posição de apoio e suporte de TI/SI, estabelecer os conceitos sobre a interação entre a estratégia organizacional e a estratégia de TI/SI e esclarecer o papel da TI/SI num ambiente orientado ao cliente.

Por último, cabe ao auditor aos SI atuar em conformidade com a realidade com SI respeitando os vários parâmetros definidos.

5.2. Limitações e implicações do Estudo

Este projeto de dissertação tem um foco na framework COBIT 5 em termos de governação e gestão de TI. Procura-se também entender se o COBIT 5 (com leve tendência para o COBIT 2019) é (ou não) adotado como framework nas organizações a nível nacional.

Com base em diversas abordagens a várias organizações dos vários setores, é pretendida a descrição da situação atual na adoção do COBIT.

Assim, as limitações e implicações encontradas durante a investigação para esta dissertação começaram com a falta de evidência da utilização da *framework* COBIT 5 pelas organizações a nível nacional, o que resultou numa necessidade de adotar um método de investigação diferente ao previsto inicialmente.

Por outro lado, a problemática também se refere ao número de entrevistas realizadas, bem como, o número de respondentes aos questionários. O tempo foi um fator crítico de sucesso durante a realização de entrevistas, dado não existir grande disponibilidade dos respondentes e, portanto, a enorme expetativa na realização de mais entrevistas presenciais, teria sido mais enriquecedora da realidade empresarial. Verificaram-se também limitações com a revisão da literatura, cuja informação não pôde ser mencionada na presente dissertação, uma vez que o acesso a alguns artigos tiveram que ser pagos ou disponibilizados confidencialmente.

O resultado da investigação poderá não estar alinhado com o inicialmente esperado e cobrir todos os aspetos da governação e gestão de TI. Em consciência, foi um grande desafio compreender a importância de ter uma boa governação e gestão de processos de negócio orientados a TI nas organizações e de que forma acrescentam valor ao trabalho dos auditores.

5.3. Conclusão e Linhas de Investigação Futura

A presente investigação considera que é possível derivar de um subconjunto otimizado de processos e atividades definidos pela *framework* COBIT 5, onde, através da sua estrutura planear e executar uma auditoria aos SI com carácter relevante em contextos organizacionais, permitindo o auditor focar-se em processos que assegurem a finalidade e resultados exigidos.

O mercado prepara-se para um ambiente de várias tecnologias emergentes, incluindo, a realidade já presente de computação em nuvem, *Big Data*, inteligência artificial, a informação e a TI. A tecnologia permite que grandes volumes de informação sejam facilmente suportados e geridos. Talvez esta realidade aumente a taxa de sucesso das empresas, mas, ao mesmo tempo, levanta outras questões desafiadoras e complexas de gestão e governança para os profissionais de segurança, gestores e especialistas em governação.

Novos negócios exigem que os cenários de risco sejam bem avaliados e tratados com o poder da informação gerado. Neste sentido, o COBIT 5 é uma solução completa que as organizações modernas procuram, no entanto, fica desde já uma advertência: devemos ter em mente que só porque existe capacidade de adotar tais metodologias e ferramentas, isto não significa que devamos implementar, correndo sérios riscos.

Em primeiro lugar, é necessário priorizar a ética digital, onde este será o ponto de partida para qualquer gestor, auditor ou parte interessada para que o seu envolvimento com às áreas de TI e SI seja de real valor acrescentado.

Como linhas de investigação futura, é pretendido desenvolver ou adotar medidas de auditoria aos SI com base no subconjunto otimizado e testar se essas medidas nas organizações resultam num impacto positivo.

Referências Bibliográficas

AL OMARI, L., Barnes, P. H., & Pitman, G. - An *Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach.* Documento apresentado no *Symposium on IT Governance, Management & Audit (SIGMA2012),* Kuala Lumpur, Malaysia. [em linha] 2012. [Consult. em 10/11/2018], também disponível em: https://eprints.qut.edu.au/53110/

BAPTISTA DA COSTA, Carlos - Auditoria Financeira – Teoria e Prática. 9ª edição. Lisboa: Rei dos Livros, 2010. ISBN 978-989-8305-11-4.7084-1

DE HAES, S., & Van Grembergen, W. - *IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group, p.* 1-3. Documento apresentado no 38º *Annual Hawaii Internaional Conference on System Sciences,* Big Island, Hawai. [em linha] 2005. [Consult. em 12/11/2018], também disponível em: https://www.researchgate.net/publication/221178165_IT_Governance_Structures_Processes_and_Relational_Mechanisms_Achieving_ITBusiness_Alignment_in_a_Major_Belgian_Financial_Group

ISACA NEWS. (20 de Agosto de 2015). *How COBIT 5 can help internal audit be "the new pillar of senior management*. [em linha]. 2015. [Consult. em 15/11/2018], disponível em: https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=534.

ISACA (2007). *COBIT 4.1*. USA: ISACA. ISBN: 1-933284-37-4 (Consultado em 24/09/2018) disponível em: https://www.isaca.org/knowledge-center/cobit/pages/downloads.aspx.

ISACA (2012). *O Modelo Corporativo para Governança e Gestão de TI da Organização*. USA: ISACA. ISBN: 978-1-60420-284-7 [Consult. em 24/09/2018] disponível em: https://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx.

ISACA (2018). *COBIT® 2019 Framework: Introduction and Methodology*. USA: ISACA. ISBN: 978-1-60420-763-7 [Consult. em 30/11/2018] disponível em: https://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx.

ISACA (2018). *COBIT® 2019 Framework: Governance and Management Objectives*. USA: ISACA. ISBN: 978-1-60420-764-4 [Consult. em 05/12/2018] disponível em: https://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx.

SANTOS ALVES, Joaquim José dos – Princípios e Práticas de Auditoria e Revisão de Contas. 1º Edição – Lisboa: Edições Sílabo, Lda., 2015 ISBN: 978-972-618-821-6

LEITE, J. (2010). *Auditoria Interna-Auditoria Operacional-Manual Prático para Auditores Internos*. Lisboa: Rei dos Livros. ISBN: 978-989-8305-07-7.

MARQUES, A.M., & Anjos, M., & Vaz, S. Q. (2002). *101 Perguntas e Repostas do Direito da Internet e da Informática*. Lisboa: Centro Atlântico, Lda. ISBN: 972-8426-50-X

OLIVER, D., & Lainhart, J. (2012). *COBIT 5: Adding Value Through Effective Geit*. *EDPACS, 46*(3), 1-12. DOI: 10.1080/07366981.2012.706472

RADOVANOVIC D., Radojevic T., Lucic D. & Sarac M., *IT audit in accordance with Cobit standard*. Belgrade, Sérvia. [em linha]. 2010. [Consult. em 13/10/2018] disponível em: https://www.researchgate.net/publication/224162993 .

WEILL, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press, 20.

YOUTUBE. [Isaca Astana]. (2018, Janeiro 01). ISACA Astana: Intersecting IT and Audit using COBIT5 [Arquivo de vídeo]. Retirado de https://www.youtube.com/watch?v=d3MHrzv-zu4

YOUTUBE. [Isaca HQ]. (2017, Julho 25). Internal Control Using COBIT 5 [Arquivo de vídeo]. Retirado de https://www.youtube.com/watch?v=m0xat_pyb-0

Apêndices e Anexos

Apêndice A

Mapeamento - Objetivos Gerais cobertos por objetivos de TI							
Estado	**Questão**	**Organização**	**Objetivos Gerais**	**Cobertura**	**Objetivos de TI**	**Alinhamento - Relação Direta**	**Alinhamento - Relação Geral**
Descartado	#1						
Descartado	#2						
Validada	#3	Setor Público					
Observações:			Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Forte
			Portfólio de produtos e serviços competetivos.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte	
			Gestão do risco do negócio (salvaguarda de ativos).	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Médio	
Validada	#4	Indústria & Comércio					
Observações: (IT Senior Manager) × Não existe qualquer apoio para o objetivo de Transparência financeira. ×Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional.			Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Fraco
			Transparência financeira.	☒	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Fraco	
			Cultura de inovação de produtos e negócios.	☑	Segurança da informação, infraestrutura de processamento e aplicações.	Médio	
Validada	#5	Retalho					
Observações: (CISA - COBIT) ✓ Os objetivos organizacionais são apoiados por todos objetivos de TI (Estrutura robusta)			Cultura de serviço orientada ao cliente.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Forte
			Respostas rápidas para um ambiente de negócios em mundança.	☑	Prestação de serviços de TI em consonância com os requisitos de negócio.	Forte	
			Cultura de inovação de produtos e negócios.	☑	Agilidade de TI.	Forte	
Validada	#6	Saúde					
Observações:			Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Forte
			Portfólio de produtos e serviços competetivos.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte	
			Gestão do risco do negócio (salvaguarda de ativos).	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Médio	

Validada	#7	Aeroportuário			
Observações:		Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte
		Gestão do risco do negócio (salvaguarda de ativos).	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte
		Conformidade com as leis e regulamentos externos.	☑	Prestação de serviços de TI em consonância com os requisitos de negócio.	Médio
Validada	#8	Bancária			
Observações: × Não existe qualquer apoio para o objetivo de Transparência financeira. ×Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional.		Cultura de serviço orientada ao cliente.	☑	Alinhamento da estratégia de TI e de negócios.	Médio
		Tomada de decisão estratégica com base na informação.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Médio
		Transparência financeira.	☒	Compromisso do gestor executivo na tomada de decisões de TI.	Fraco
Validada	#9	C&C			
Observações:		Conformidade com as leis e regulamentos externos.	☑	Alinhamento da estratégia de TI e de negócios.	Médio
		Portfólio de produtos e serviços competetivos.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Médio
		Tomada de decisão estratégica com base na informação.	☑	Gestão do risco organizacional de TI.	Médio
Validada	#10	Contabilidade			
Observações: Sem conhecimento dos Objetivos de SI / TI		Portfólio de produtos e serviços competetivos.			
		Respostas rápidas para um ambiente de negócios em mundança.			
		Conformidade com as leis e regulamentos externos.			
Validada	#11	Consultoria			
Observações: × Não existe qualquer apoio para o objetivo de Conformidade de Políticas Internas.		Respostas rápidas para um ambiente de negócios em mundança.	☑	Prestação de serviços de TI em consonância com os requisitos de negócio	Forte
		Cultura de serviço orientada ao cliente.	☑	Alinhamento da estratégia de TI e de negócios.	Médio
		Conformidade com as políticas internas	☒	Capacidade e apoio dos processos de negócio através da integração de aplicações e tecnologia nos processos de negócio.	Fraco

Validada	#12	Aeroportuário				
Observações:		Continuidade e disponibilidade do serviço de negócio	☑	Prestação de serviços de TI em consonância com os requisitos de negócio.	Forte	Forte
		Portfólio de produtos e serviços competetivos	☑	Segurança da informação, infraestrutura de processamento e aplicações	Forte	
		Gestão do risco do negócio (salvaguarda de ativos).	☑	Alinhamento da estratégia de TI e de negócios.	Forte	
Validada	#13	Recursos Humanos				
Observações: × Não existe qualquer apoio para o objetivo de Transparência financeira.		Conformidade com as leis e regulamentos externos	☑	Segurança da informação, infraestrutura de processamento e aplicações	Forte	Médio
		Gestão do risco do negócio (salvaguarda de ativos	☑	Prestação de serviços de TI em consonância com os requisitos de negócio	Forte	
		Transparência financeira.	☒	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Fraca	
Validada	#14	Distribuição Postal				
Observações: Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional.		Continuidade e disponibilidade do serviço de negócio	☑	Alinhamento da estratégia de TI e de negócios	Médio	Médio
		Respostas rápidas para um ambiente de negócios em mundança	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Médio	
		Otimização dos custos do processo do negócio.	☑	Uso adequado de aplicações, informações e soluções tecnológicas.	Médio	
Validada	#15	C&C				
Observações: Os objetivos de TI não têm como prioridade a consecussão dos objetivos organizacionais, embora estejam a cobrir os mesmos.		Conformidade com as leis e regulamentos externos.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos	Forte	Médio
		Cultura de serviço orientada ao cliente	☑	Segurança da informação, infraestrutura de processamento e aplicações	Fraco	
		Continuidade e disponibilidade do serviço de negócio	☑	Uso adequado de aplicações, informações e soluções tecnológicas	Médio	
Validada	#16	Indústria				
Observações: Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional.		Cultura de serviço orientada ao cliente.	☑	Alinhamento da estratégia de TI e de negócios	Fraca	Médio
		Valor de investimentos da organização percebidos pelas partes interessadas	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte	
		Respostas rápidas para um ambiente de negócios em mundança	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Forte	

Validada	#17	Contabilidade				
Observações: Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional.		Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Forte
		Continuidade e disponibilidade do serviço de negócio.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte	
		Otimização da funcionalidade do processo de negócio	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Médio	
Validada	#18	Retalho				
Observações: Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos não presta apoio a nenhum objetivo organizacional, estando os objetivos dependentes dos processo de alinhamento da estratégia de TI e de negócios.		Continuidade e disponibilidade do serviço de negócio	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Média
		Cultura de inovação de produtos e negócios	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Média	
		Cultura de serviço orientada ao cliente.	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Fraca	
Validada	#19	Trading (Importações e Exportações)				
Observações:		Valor de investimentos da organização percebidos pelas partes interessadas.	☑	Alinhamento da estratégia de TI e de negócios.	Forte	Forte
		Portfólio de produtos e serviços competetivos.	☑	Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos.	Forte	
		Gestão do risco do negócio (salvaguarda de ativos).	☑	Compromisso do gestor executivo na tomada de decisões de TI.	Forte	
Validada	#20	Contabilidade				
Observações: Não existe Departamento de SI		Conformidade com as leis e regulamentos				
		Pessoas qualificadas e motivadas				
		Cultura de serviço orientada ao cliente.				
Validada	#21	C&C				
Observações: Não existe Departamento de SI		Cultura de serviço orientada ao cliente				
		Portfólio de produtos e serviços competetivos				
		Produtividade operacional e da equipa.				

Apêndice A - Cobertura dos Objetivos Gerais por Objetivos de T

Anexo 1 - Apêndice D – Necessidades das Partes Interessadas e os Objetivos Organizacionais

Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI?	■	■				■	■						■			■	■
Como posso gerenciar o desempenho de TI?		■			■				■	■	■	■		■			
Como posso explorar melhor as novas tecnologias para novas oportunidades estratégicas?	■	■						■					■			■	■
Como faço para criar e estruturar da melhor forma o meu departamento de TI?								■		■	■	■		■	■	■	
Qual é a minha dependência de fornecedores externos? Quão bem os contratos de terceirização de TI estão sendo gerenciados? Como faço para obter garantia dos fornecedores externos?			■	■						■							

(Continuação da tabela anterior)

Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Quais são os requisitos (de controle) da informação?				■					■						■		
Considerei todos os riscos de TI?			■				■		■						■		
Estou conduzindo uma resiliente e eficiente operação de TI?					■		■										
Como posso controlar o custo de TI? Como utilizar os recursos de TI de forma mais eficaz e eficiente? Quais são as opções de terceirização mais efetivas e eficientes?										■		■		■			
Tenho pessoal suficiente para TI? Como faço para desenvolver e manter sua capacitação, e como controlo seu desempenho?										■		■		■			
Como faço para obter garantia do funcionamento de TI?				■											■		
As informações que estou processando estão bem protegidas?				■			■								■		
Como posso melhorar a agilidade dos negócios com um ambiente de TI mais flexível?	■							■								■	■
Os projetos de TI falham para entregar o que prometeram – e caso afirmativo, por quê? TI está atrapalhando a execução da estratégia de negócios?	■	■	■					■			■	■	■				
Quão crítica é TI para a sustentação da organização? O que fazer se ela não estiver disponível?	■	■					■										
Quais processos de negócios críticos dependem de TI, e quais são os requisitos dos processos de negócios?	■	■									■	■					

(Continuação da tabela anterior)

Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Qual tem sido o custo adicional médio dos orçamentos operacionais de TI? Com que frequência e em que medida os projetos de TI estouram o orçamento?					■					■		■		■			
Quanto do esforço de TI é dedicado para apagar incêndios em vez de facilitar a melhoria do negócio?		■	■									■					
Foram disponibilizados infraestruturas e recursos de TI suficientes para alcançar os objetivos estratégicos da organização?		■			■					■		■					
Quanto tempo é necessário para a tomada de decisões importantes de TI?	■	■			■			■									
O esforço total de TI e seus investimentos são transparentes?		■		■	■										■		
A TI apoia a organização no cumprimento dos regulamentos e níveis de serviço? Como faço para saber se estou em conformidade com todos os regulamentos aplicáveis?				■											■		

Anexo 1 - As Necessidades das Partes Interessadas e os Objetivos Organizacionais **Fonte:** ISACA, COBIT® 5, 2012

Anexo 2 - Apêndice B – Mapeamento dos Objetivos Organizacionais em Objetivos de TI

		Objetivo Corporativo																
		Valor dos investimentos em negócio para as partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência financeira	Cultura de serviço orientada ao cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica baseada na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócio	Otimização dos custos do processo de negócio	Programa de gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com as políticas internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Objetivo de TI	Financeira					Cliente					Interna					A&C	
Financeira	01 Alinhamento da estratégia de TI e de negócios	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos			S	P											P		
	03 Compromisso da gerência executiva com a tomada de decisões de TI	P	S	S					S	S		S		P			S	S
	04 Gestão do risco organizacional de TI			P	S			P	S		P			S		S	S	
	05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	P	P				S		S		S	S	P		S			S
	06 Transparência dos custos, benefícios e riscos de TI	S		S		P				S	P		P					
Cliente	07 Prestação de serviços de TI em consonância com os requisitos de negócio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adequado de aplicativos, informações e soluções tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09 Agilidade de TI	S	P	S			S		P			P		S	S		S	P
	10 Segurança da informação, infraestrutura de processamento e aplicativos			P	P			P								P		
	11 Otimização de ativos, recursos e capacidades de TI	P	S						S		P	S	P	S	S			S
	12 Capacitação e apoio dos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	S	P	S			S		S		S	P	S	S	S			S
	13 Entregas de programas fornecendo benefícios, dentro do prazo, orçamento, e atendendo requisitos e padrões de qualidade	P	S	S			S				S		S	P				
	14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	S	S	S	S			P		P		S						
	15 Conformidade de TI com as políticas internas			S	S											P		
A&C	16 Equipes de TI e de negócios motivadas e qualificadas	S	S	P			S		S						P		P	S
	17 Conhecimento, expertise e iniciativas para a inovação dos negócios	S	P				S		P	S		S		S			S	P

Anexo 2 - Desdobramento dos Objetivos Organizacionais em Objetivos de TI, **Fonte:** ISACA, COBIT® 5, 2012

Anexo 3 - Apêndice C – Mapeamento dos Objetivos de TI em Processos de TI

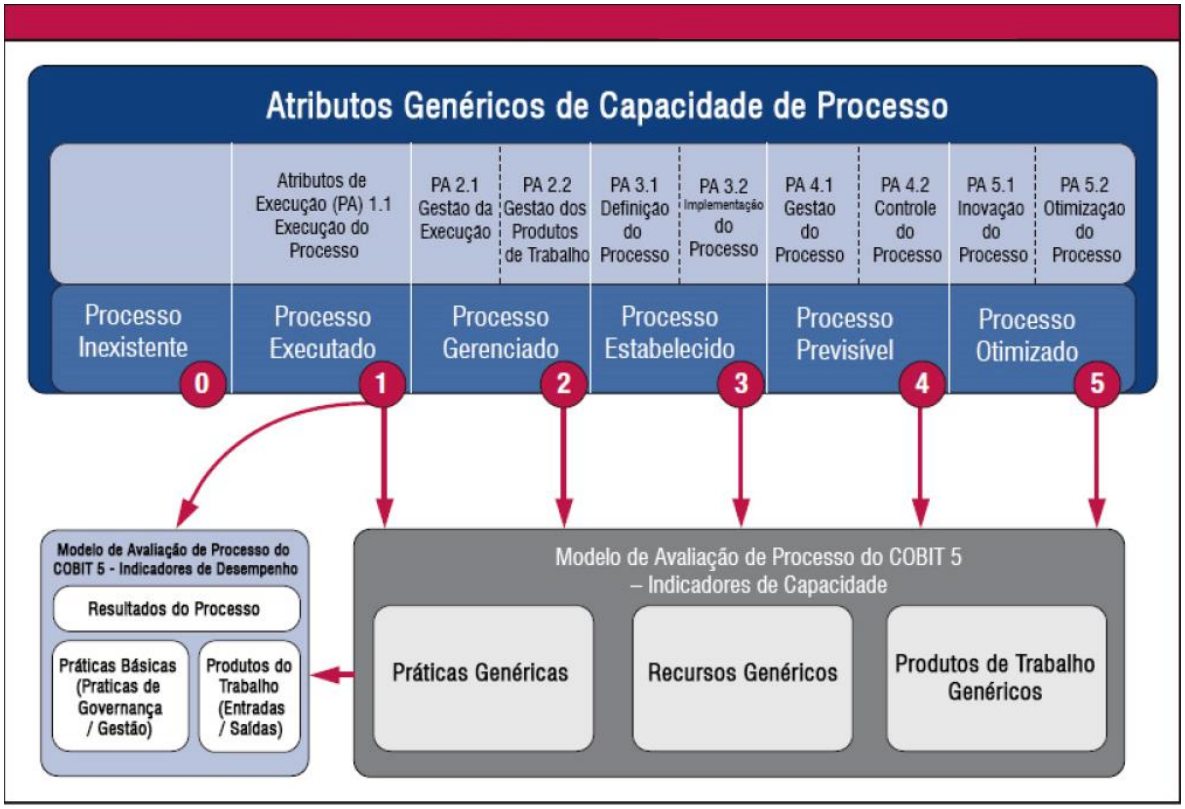
			Objetivos de TI																
			Alinhamento da estratégia de TI e de negócios	Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos	Compromisso da gerência executiva com a tomada de decisões de TI	Gestão do risco organizacional de TI	Benefícios obtidos pelo investimento de TI e portfólio de serviços	Transparência dos custos, benefícios e riscos de TI	Prestação de serviços de TI em consonância com os requisitos de negócio	Uso adequado de aplicativos, informações e soluções tecnológicas	Agilidade de TI	Segurança da informação, infraestrutura de processamento e aplicativos	Otimização de ativos, recursos e capacidades de TI	Capacitação e apoio aos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	Disponibilidade de informações úteis e confiáveis para tomada de decisão	Conformidade de TI com as políticas internas	Equipes de TI e de negócios motivadas e qualificadas	Conhecimento, expertise e iniciativas para inovação dos negócios
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processo do COBIT 5			Financeira						Cliente		Interna							A&C	
Avaliar, Dirigir e Monitorar	EDM01	Garantir a Definição e Manutenção do Modelo de Governança	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Garantir a Realização de Benefícios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Garantir a Otimização do Risco	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Garantir a Otimização de Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Garantir a Transparência às Partes Interessadas	S	S	P			P	P						S	S	S		S
Alinhar, Planejar e Organizar	APO01	Gerenciar a Estrutura de Gestão de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gerenciar a Estratégia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gerenciar Arquitetura da Organização	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gerenciar Inovação	S			S	P			P	P		P	S		S			P
	APO05	Gerenciar Portfólio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gerenciar Orçamento e Custos	S		S	S	P	P	S	S			S		S				
	APO07	Gerenciar Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gerenciar Relacionamentos	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gerenciar Contratos de Prestação de Serviços	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gerenciar Fornecedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gerenciar Qualidade	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gerenciar Riscos		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gerenciar Segurança		P		P		P	S	S		P				P			

(Continuação da tabela anterior)

			Objetivos de TI																
			Alinhamento da estratégia de TI e de negócios	Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos	Compromisso da gerência executiva com a tomada de decisões de TI	Gestão do risco organizacional de TI	Benefícios obtidos pelo investimento de TI e portfólio de serviços	Transparência dos custos, benefícios e riscos de TI	Prestação de serviços de TI em consonância com os requisitos de negócio	Uso adequado de aplicativos, informações e soluções tecnológicas	Agilidade de TI	Segurança da informação, infraestrutura de processamento e aplicativos	Otimização de ativos, recursos e capacidades de TI	Capacitação e apoio aos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	Disponibilidade de informações úteis e confiáveis para tomada de decisão	Conformidade de TI com as políticas internas	Equipes de TI e de negócios motivadas e	Conhecimento, expertise e iniciativas para inovação dos negócios
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processo do COBIT 5			Financeira						Cliente		Interna							A&D	
Construir, Adquirir e Implementar	BAI01	Gerenciar Programas e Projetos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gerenciar Definição de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gerenciar Identificação e	S			S	S		P	S			S	S	S	S			S
	BAI04	Gerenciar Disponibilidade e				S	S		P	S	S		P		S	P			S
	BAI05	Gerenciar Capacidade de Mudança	S		S		S		S	P	S		S	S	P				P
	BAI06	Gerenciar Mudanças			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gerenciar Aceitação e Transição da Mudança				S	S		S	P	S			P	S	S	S		S
	BAI08	Gerenciar	S				S		S	S	P	S	S			S		S	P
	BAI09	Gerenciar Ativos		S		S		P	S		S	S	P			S	S		
	BAI10	Gerenciar Configuração		P		S		S		S	S	S	P			P	S		
Entregar, Atender e Apoiar	DSS01	Gerenciar Operações		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gerenciar Solicitações e Incidentes de Serviços				P			P	S		S				S	S		S
	DSS03	Gerenciar Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gerenciar Continuidade	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gerenciar Serviços de Segurança	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gerenciar Controles do Processo de Negócio		S		P			P	S		S	S	S		S	S	S	S
Monitorar, Avaliar e Analisar	MEA01	Monitorar, Avaliar e Analisar Desempenho e Conformidade	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitorar, Avaliar e Analisar o Sistema de Controle Interno		P		P		S	S	S		S				S	P		S
	MEA03	Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos		P		P	S		S			S					S		S

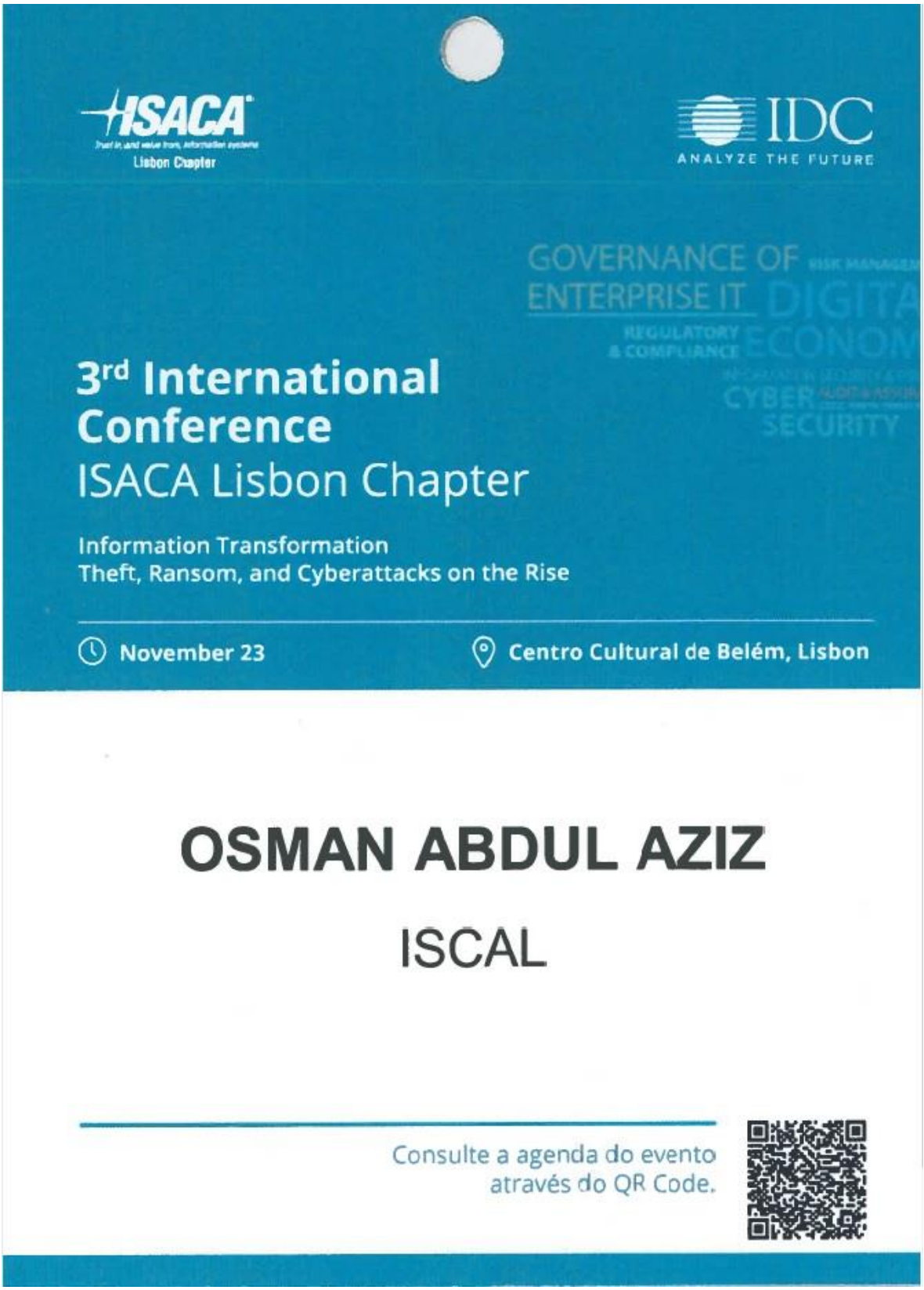
Anexo 3 - Desdobramento dos Objetivos de TI em Objetivos de Enablers, **Fonte:** ISACA, COBIT® 5, 2012

Anexo 4 - Modelo de Capacidade dos Processos



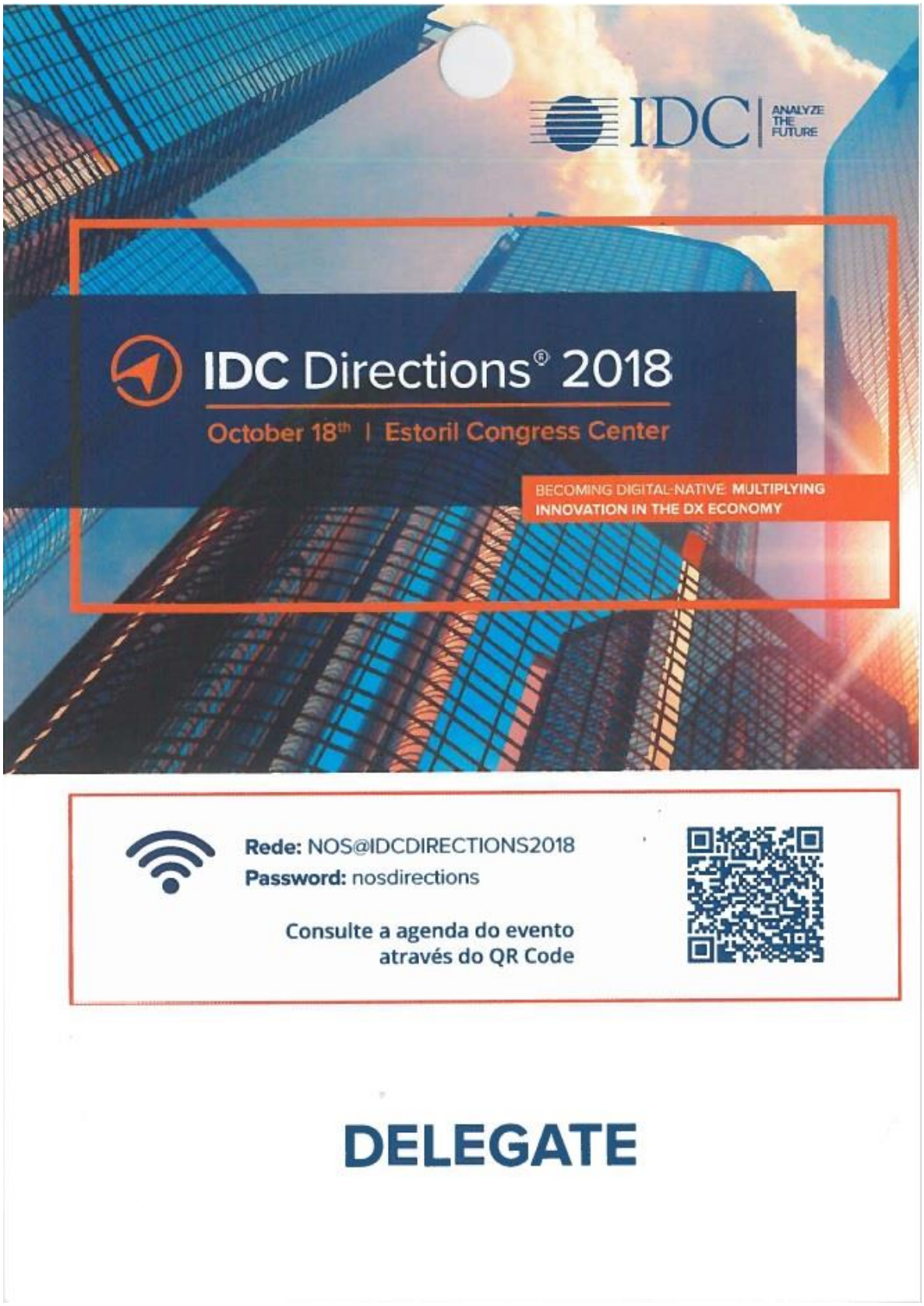
Anexo 4 - Modelo de Capacidade dos Processos, **Fonte**: ISACA, COBIT® 5, 2012

Anexo 5 - Identificação de Evento- 3ª Conferência Internacional do ISACA Lisbon Chapter



Anexo 5 - Identificação de Evento: 3ª Conferência Internacional do ISACA Lisbon Chapter

Anexo 6- Identificação de Evento: IDC Directions 2018



Anexo 6 - Identificação de Evento: IDC Directions 2018