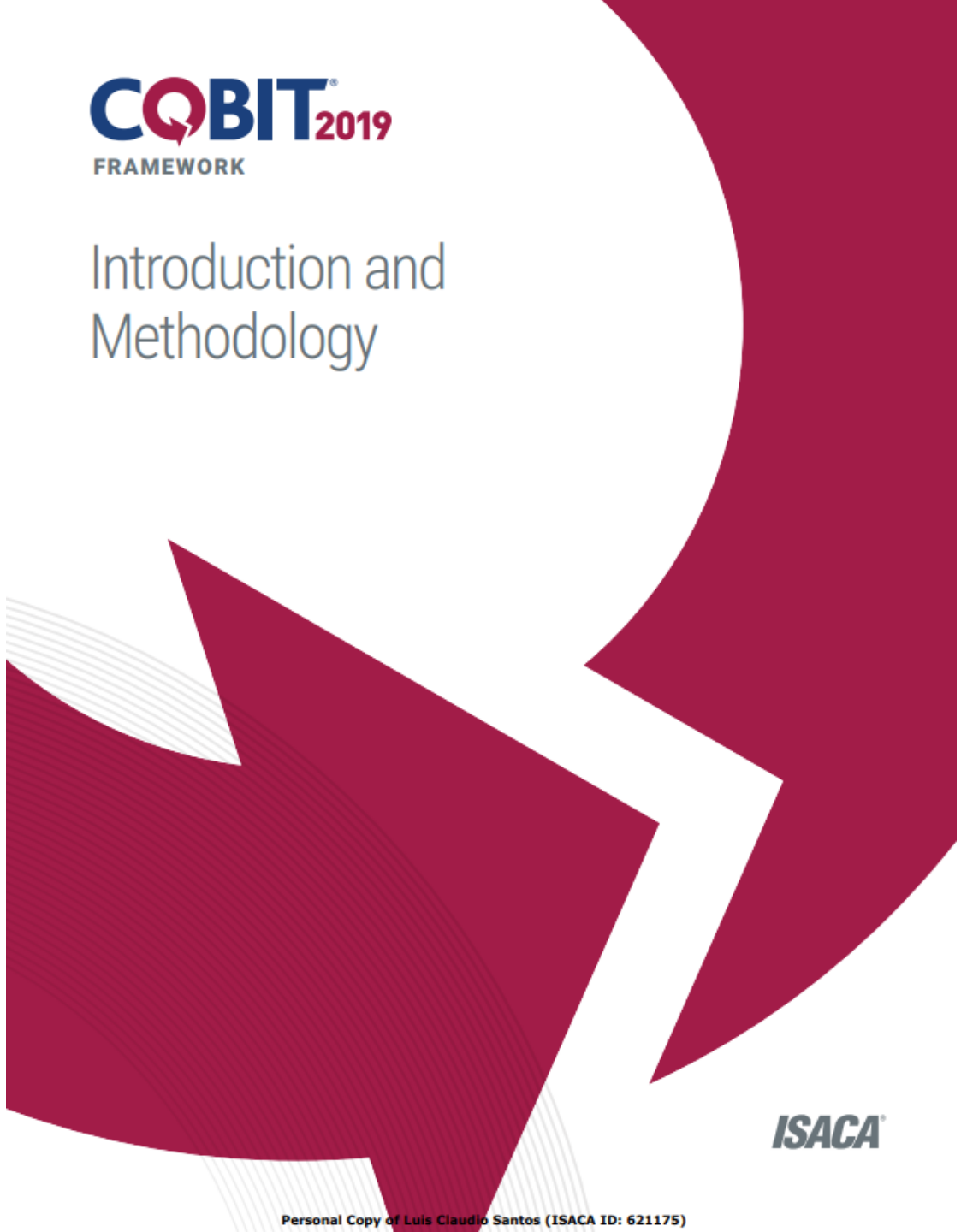
# COBIT 2019

Prof. Luis Claudio
ProvasdeTI.com.br



# O COBIT e a ISACA

COBIT nasceu em 1996 em um “white paper” ainda como uma sigla (“Control Objectives for Information and related Technology”).

Seu proprietário é a ISACA (Information Systems Audit and Control Association).

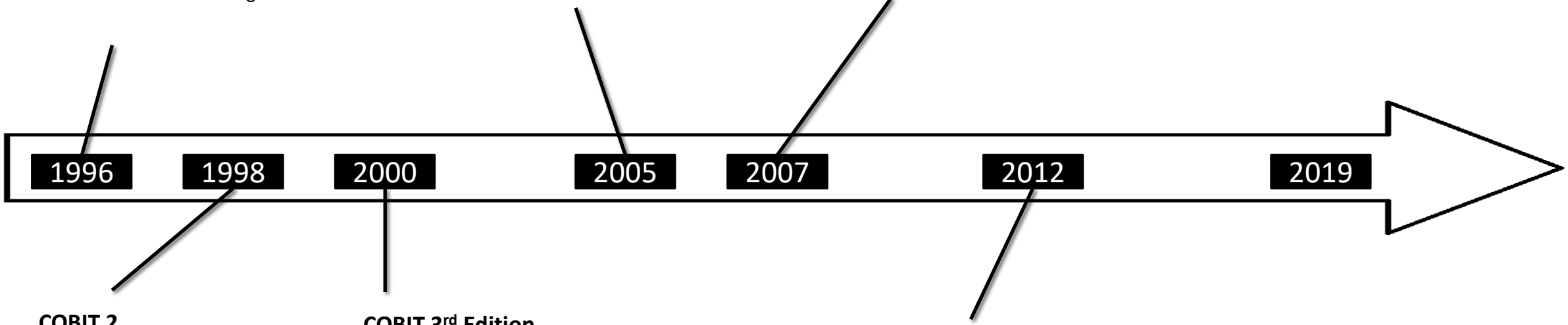
A ISACA possui programas cobiçados de certificação, tais como:

# COBIT - Histórico

**COBIT**
- Foco em **Auditoria**.
- Control Objectives for Information and Related Technologies.

**COBIT 4.0**
- Foco em **Controle** e **Auditoria**.
- Framework de **Gerenciamento de TI**.
- Framework de **Governança de TI**.

**COBIT 4.1**
- Market feedback indicated that the structure of the control objectives was more complicated than necessary, so two years later COBIT 4.1 was released with a reduced set of control objectives.

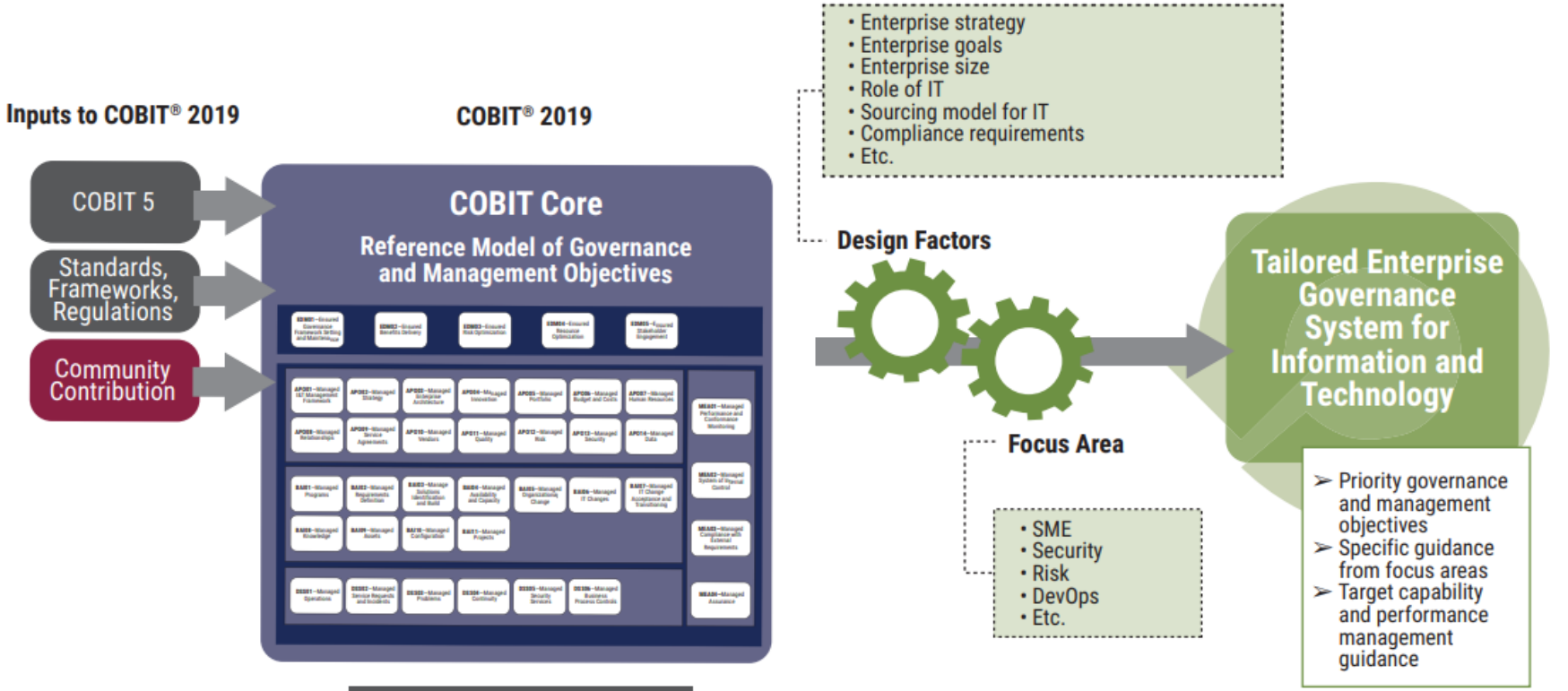



**COBIT 2**
- Maior visibilidade.
- Foco em **Controle** e **Auditoria**.

**COBIT 3rd Edition**
- Foco em **Controle** e **Auditoria**.
- Foco na **Função de TI**.
- Framework de **Gerenciamento de TI**.

**COBIT 5**
- Passou a ser uma "marca" (não mais um acrônimo).
- Framework de **Governança Empresarial de TI**.
- COBIT 5 presents a model for the **alignment** of **overall enterprise strategy with IT strategy**…
- Operates on a relatively simple foundation of **five principles** with **seven enablers**…
- Is aligned with several internationally recognized standards bodies, such as **ISO/IEC** and **ITIL**….
- More than 800 people provided input into the design of COBIT 5, which required nearly two years to develop and is now available in **16 languages**.

# COBIT 2019 – Visão Geral




***COBIT Core Publications***

**COBIT® 2019 Framework:** Introduction and Methodology

**COBIT® 2019 Framework:** Governance and Management Objectives

**COBIT® 2019 Design Guide:** Designing an Information and Technology Governance Solution

**COBIT® 2019 Implementation Guide:** Implementing and Optimizing an Information and Technology Governance Solution

# COBIT 2019 – Família


Framework – Introduction and Methodology

- Chapter 1 – Introdução.
- Chapter 2 – Público Alvo.
- Chapter 3 – Princípios.
- Chapter 4 – Conceitos Básicos e Terminologias.
- Chapter 5 – Objetivos de Governança e Gestão.
- Chapter 6 – Modelo de Desempenho Inspirado no CMM-I.

- Chapter 7 – Contém Visão Geral do COBIT® 2019 *Design Guide*.
- Chapter 8 – Contém Visão Geral do COBIT® 2019 *Implementation Guide*.
- Chapter 9 – Estudo de Caso da *Acme Corporation*.

- Chapter 10 – Padrões, Frameworks e Regulamentos.

# COBIT 2019 – Cap 10 - Lista Padrões etc.

Um dos princípios aplicados ao desenvolvimento do COBIT® 2019 foi o de manter seu posicionamento como um framework "**guarda-chuva**".

- CIS® Center for Internet Security®
  - The CIS Critical Security Controls for Effective Cyber Defense, Version 6.1, August 2016
- Cloud standards and good practices:
  - **Amazon Web Services** (AWS®)
  - Security Considerations for Cloud Computing, ISACA
  - Controls and Assurance in the Cloud: Using COBIT® 5, ISACA
- **CMMI®** Cybermaturity Platform, 2018
- **CMMI®** Data Management Maturity (DMM) SM model, 2014
- **CMMI®** Development V2.0, CMMI Institute, USA, 2018
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Framework, June 2017

# COBIT 2019 – Cap 10 - Lista Padrões etc.

Um dos princípios aplicados ao desenvolvimento do COBIT® 2019 foi o de manter seu posicionamento como um framework "**guarda-chuva**".

- European Committee for Standardization (CEN), e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, EN 16234-1:2016
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), The Standard of Good Practice for Information Security 2016
- **International Organization for Standardization** / International Electrotechnical Commission (ISO/IEC) standards
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- **Information Technology Infrastructure Library** (ITIL®) v3, 2011

# COBIT 2019 – Cap 10 - Lista Padrões etc.

Um dos princípios aplicados ao desenvolvimento do COBIT® 2019 foi o de manter seu posicionamento como um framework "**guarda-chuva**".

- **Institute of Internal Auditors**® (IIA® ), "Core Principles for the Professional Practice of Internal Auditing"
- King IV Report on Corporate Governance™, 2016
- US National Institute of Standards and Technology (NIST) standards:
  - Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018
  - Special Publication 800-37, Revision 2 (Draft), May 2018
  - Special Publication 800-53, Revision 5 (Draft), August 2017
- "Options for Transforming the IT Function Using Bimodal IT," MIS Quarterly Executive (white paper)
- A Guide to the Project Management Body of Knowledge: **PMBOK**® Guide, **Sixth Edition**, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled **Agile Framework** for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT™ Reference Architecture, version 2.0
- The Open Group Standard **TOGAF**® version 9.2, 2018
- The TBM Taxonomy, The TBM Council

# COBIT 2019 Framework

## Cap. 01
## Introdução

# 1. Introdução

**EGIT - Enterprise Governance of Information and Technology**

- Atualmente, os controladores e gestores de uma organização não podem mais delegar, ignorar ou evitar decisões relativas à I&T.
- EGIT é parte integral da Governança Corporativa.
- **Enterprise I&T** envolve toda a tecnologia e todo o processamento de informação que a organização utiliza para atingir metas, onde quer que isso ocorra na organização.

*"COBIT guidance uses the terms 'governance of enterprise information and technology', 'enterprise governance of information and technology', 'governance of IT' and 'IT governance' interchangeably."*

# 1. Introdução

**Resultados esperados da EGIT**

Três resultados (*outcomes*) são esperados da adoção bem sucedida da EGIT:

- **Benefits realization** — Criar valor para a organização através da I&T, mantendo ou aumentando investimentos atuais em I&T e eliminando iniciativas e ativos que não criam valor suficiente.

- **Risk optimization** — Otimizar o risco de negócio associado ao uso, propriedade, operação, envolvimento, influência e adoção de I&T na organização. Enquanto a entrega de valor foca na sua criação, *risk management* foca na preservação deste valor.

- **Resource optimization** — Assegurar que as capacidade apropriadas estão disponíveis para executar o plano estratégico e que são fornecidos recursos suficientes, apropriados e efetivos para implementar estratégias. Assegurar que novas tecnologias são introduzidas conforme necessário e sistemas obsoletos são atualizados ou substituídos.

# 1. Introdução

**COBIT – I&T Governance Framework**

**O que é?**

- O COBIT é uma estrutura (*framework*) para Governança e Gerenciamento da Informação e Tecnologia Organizacional (Enterprise I&T), focada na organização como um todo.

# 1. Introdução

**COBIT – I&T Governance Framework**

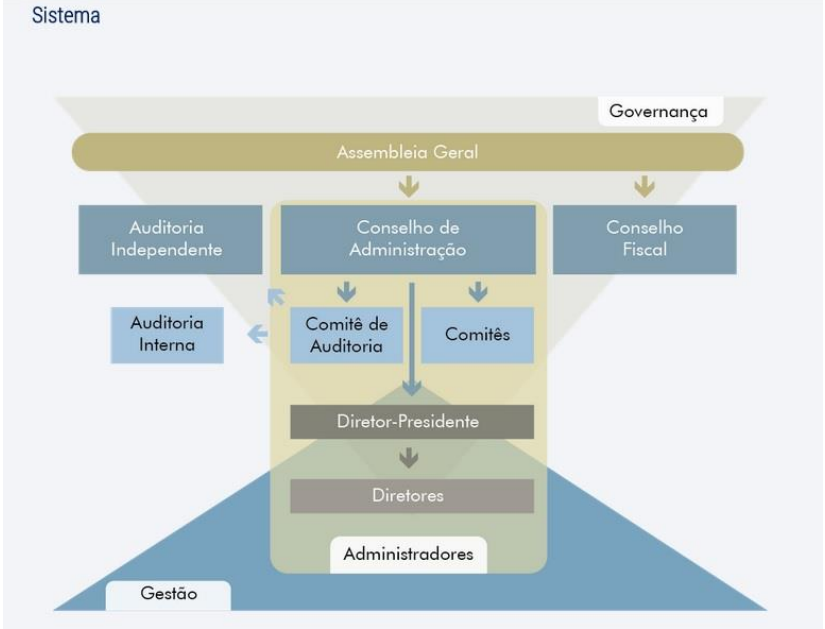
- O que o COBIT NÃO é:
  - COBIT is not a full description of the whole **IT environment** of an enterprise.
  - COBIT is not a framework to **organize** business processes.
  - COBIT is not an (IT-)**technical** framework to manage all technology.
  - COBIT does not **make** or **prescribe** any IT-related **decisions**.

*It will not decide what the best IT strategy is, what the best architecture is, or how much IT can or should cost. Rather, COBIT defines all the components that describe which decisions should be taken, and how and by whom they should be taken.*

# 1. Introdução

**COBIT – I&T Governance Framework**

- O COBIT faz distinção entre Governança e Gerenciamento.
  - **Governança**:
    - **Avaliar** as necessidades dos Stakeholder para estabelecer os objetivos da organização de forma consensual e equilibrada.
    - **Dirigir** a organização através de tomada de decisão e priorização.
    - **Monitorar** o desempenho e comparar com a direção dada e com os objetivos estabelecidos.
  - **Gerenciamento:**
    - Planejar, construir, executar e monitorar atividades em alinhamento com a direção estabelecida pela Governança, a fim de atingir os objetivos da organização.




http://www.ibgc.org.br/

*In most enterprises, management is the responsibility of the executive management, under the leadership of the chief executive officer (CEO).*

# COBIT 2019 Framework

## Cap. 02
## **Público Alvo**

# 2. Publico Alvo

São os stakeholders da EGIT e, por extensão, os stakeholders da Governança Corporativa.

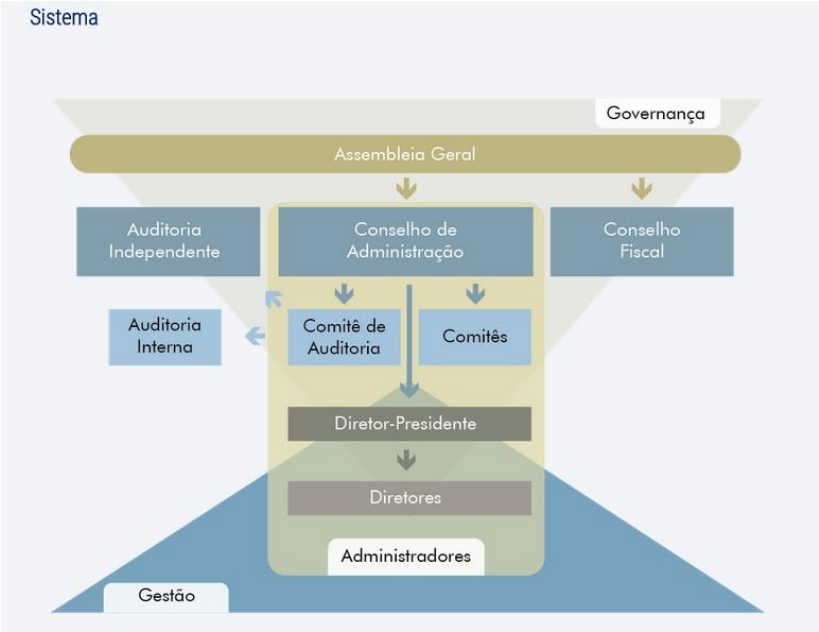
*A certain level of experience and a thorough understanding of the enterprise are required to benefit from the COBIT framework.*

**Internos**

- Boards
- Executive Management
- Business Managers
- IT Managers
- Assurance Providers
- Risk Management

**Externos**

- Regulators
- Business Partners
- IT Vendors



# COBIT 2019 Framework

## Cap. 03
## Princípios

# 3. Princípios

O COBIT® 2019 foi desenvolvido com base em dois conjuntos de princípios:

- *Principles that describe the core requirements of a governance system.*
- *Principles for a governance framework that can be used to build a governance system.*

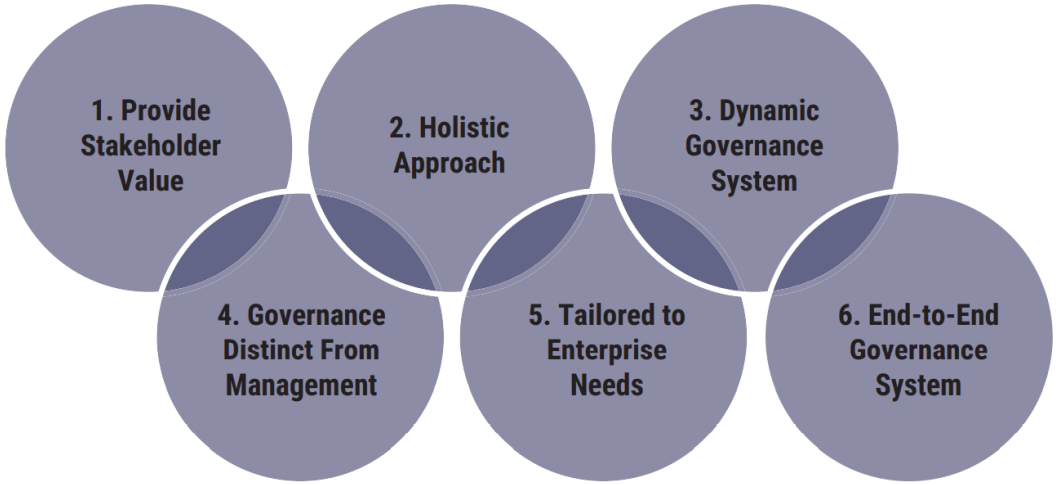



*Figure 3.1—Governance System Principles*

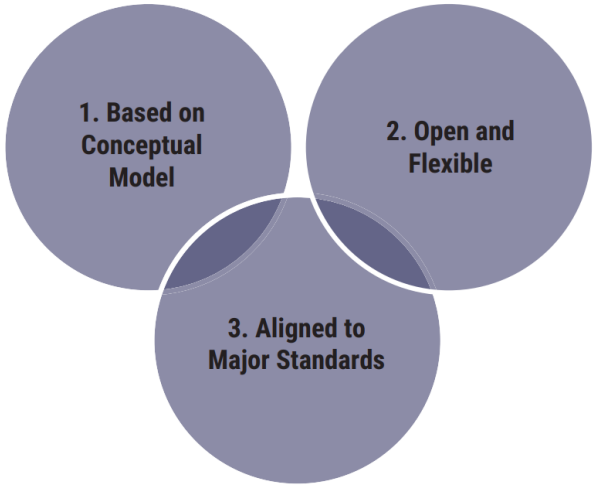



*Figure 3.2—Governance Framework Principles*

# 3. Princípios do Sistema

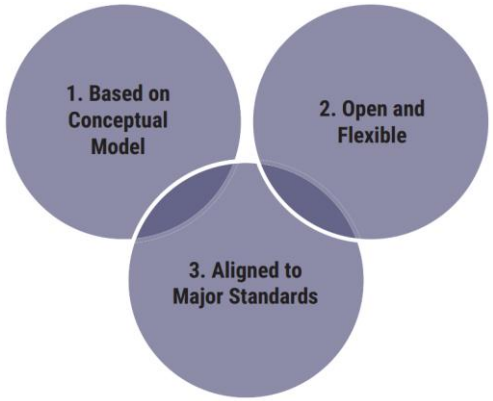



*Figure 3.2—Governance Framework Principles*

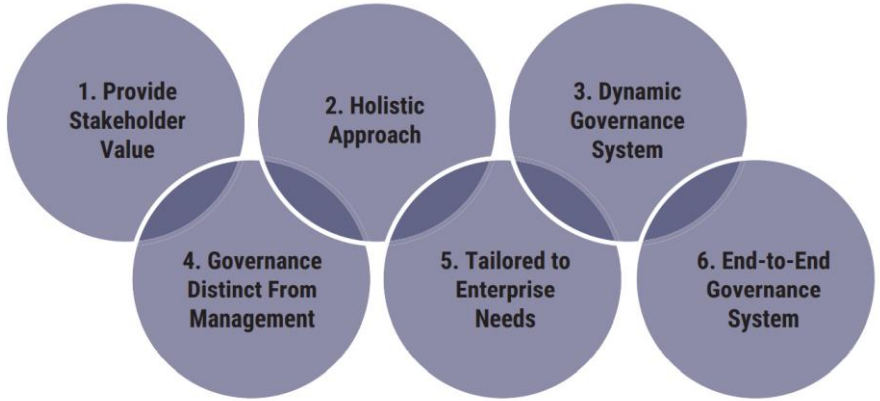



*Figure 3.1 - Governance System Principles*

# 3. Princípios do Sistema

## 1 - Valor para Stakeholders

Cada empresa precisa de um sistema de governança para atender às necessidades das partes interessadas e gerar **valor** a partir do uso da I&T.

*Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.*

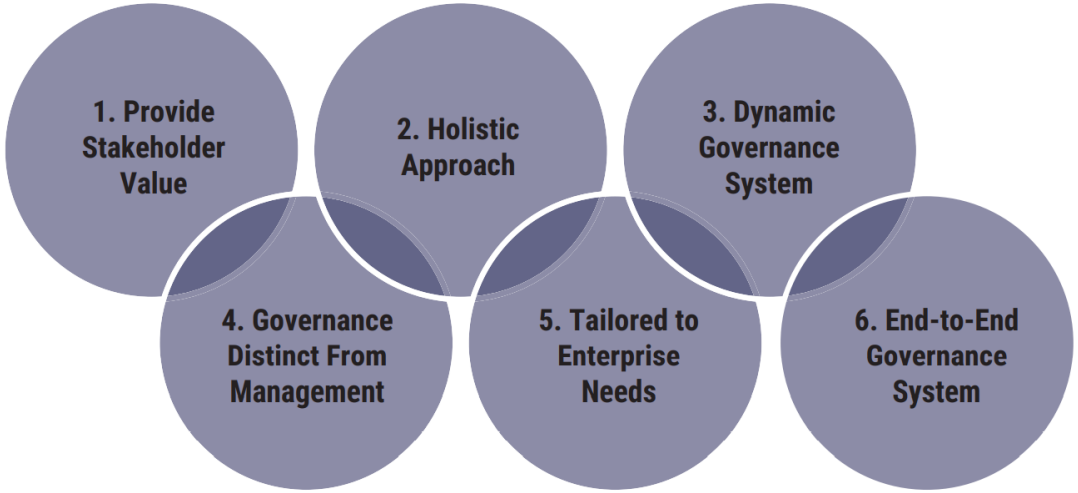



*Figure 3.1 - Governance System Principles*

# 3. Princípios do Sistema

## 2 - Abordagem Holística

Um sistema de governança para a I&T corporativa é construído a partir de um número de **componentes** que podem ser de diferentes tipos e que trabalham juntos de maneira **holística**.

*A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.*

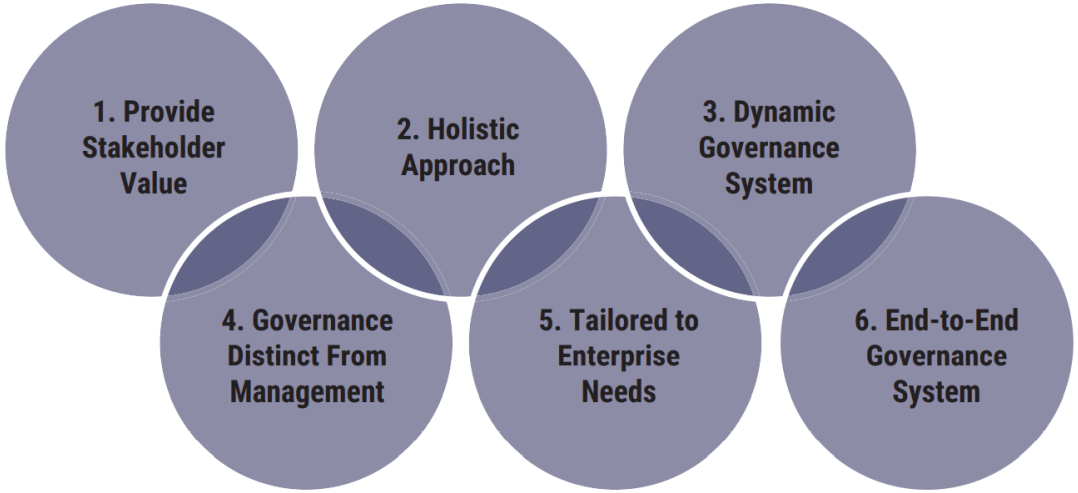



*Figure 3.1 - Governance System Principles*

# 3. Princípios do Sistema

## 4 - Governança *versus* Gestão

Um sistema de **governança** deve ter uma clara distinção entre as atividades e as estruturas de **governança** e de **gestão**.

A governance system should clearly distinguish between governance and management activities and structures.

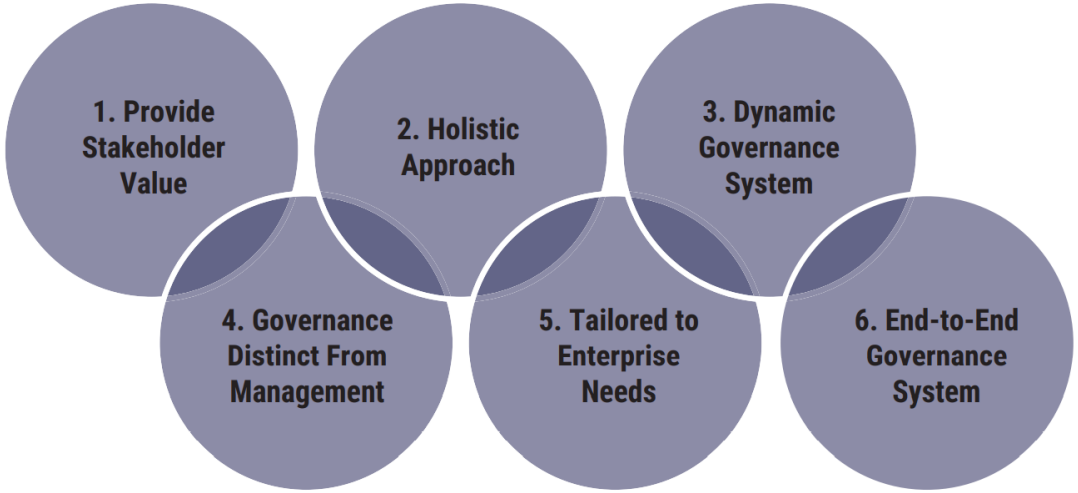



*Figure 3.1 - Governance System Principles*

# 3. Princípios do Sistema

## 6 – Ponta a Ponta

Um sistema de governança deve cobrir a organização de ponta a ponta, focando não somente na função de TI mas em toda a tecnologia e processamento de informação que a organização estabelece para atingir suas metas, a despeito de onde este processamento está localizado na empresa.

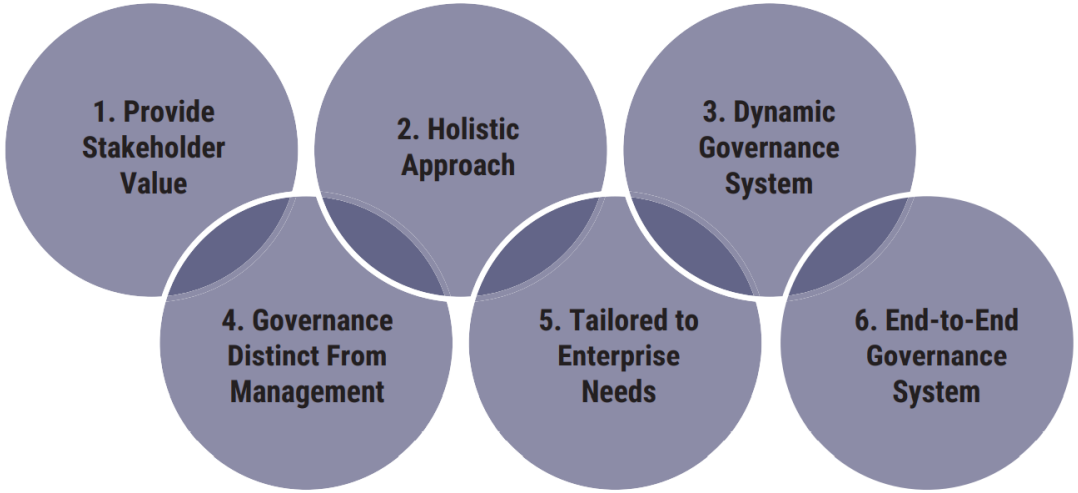



*Figure 3.1 - Governance System Principles*

A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise.

# 3. Princípios do Sistema

## 3 - Dinâmico

Um sistema de governança deve ser dinâmico. Isso significa que cada vez que um ou mais fatores de projeto mudam, o impacto desta mudança no EGIT System deve ser considerado.

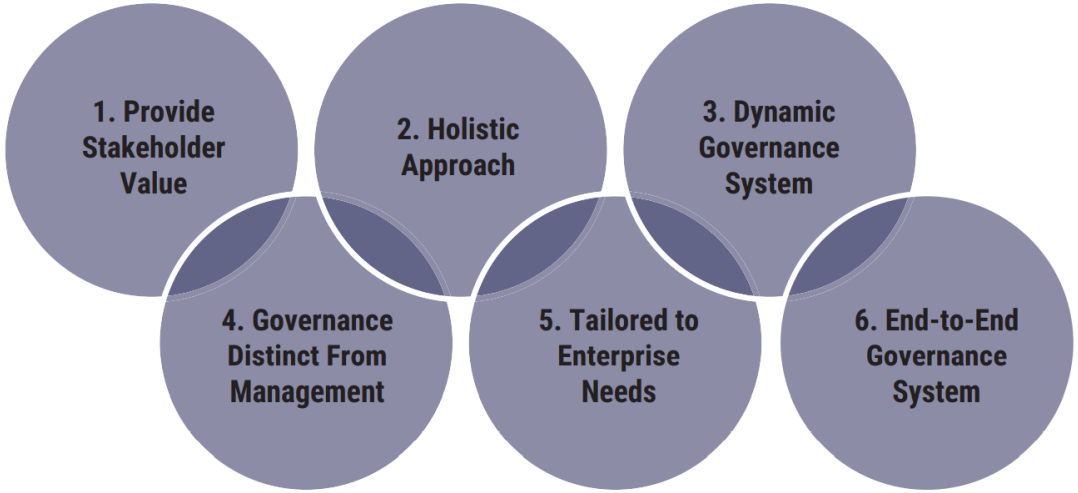



*Figure 3.1 - Governance System Principles*

A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.

# 3. Princípios do Sistema

## 5 - Adaptável

Um sistema de governança deve ser adaptado às necessidades da empresa, usando um conjunto de fatores de projeto como parâmetros para customizar e priorizar os componentes do sistema de governança.

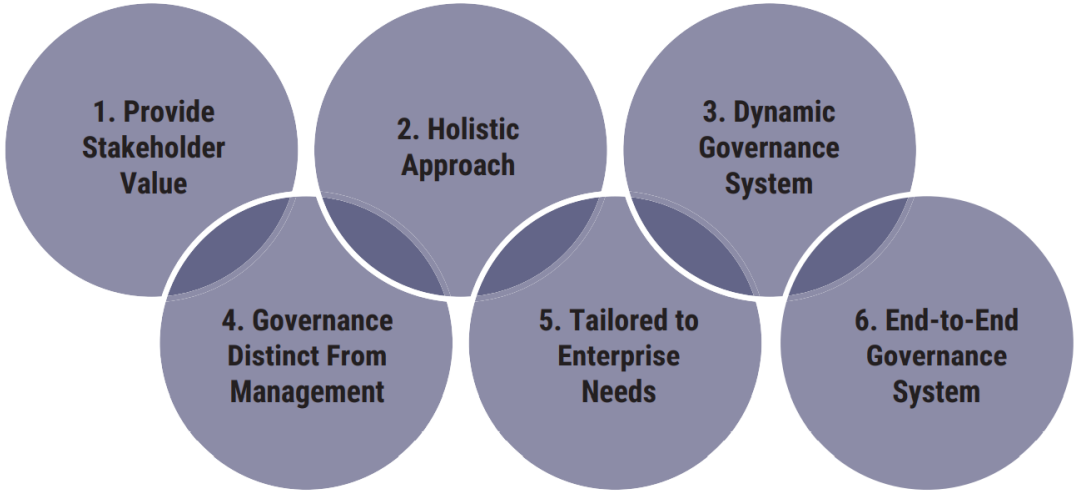



*Figure 3.1 - Governance System Principles*

*5. A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.*

# 3. Princípios do Framework

1. Um framework de governança deve ser baseado em um modelo conceitual, identificando os componentes-chave e os relacionamentos entre eles, a fim de maximizar a consistência e permitir automação.

*1. A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.*

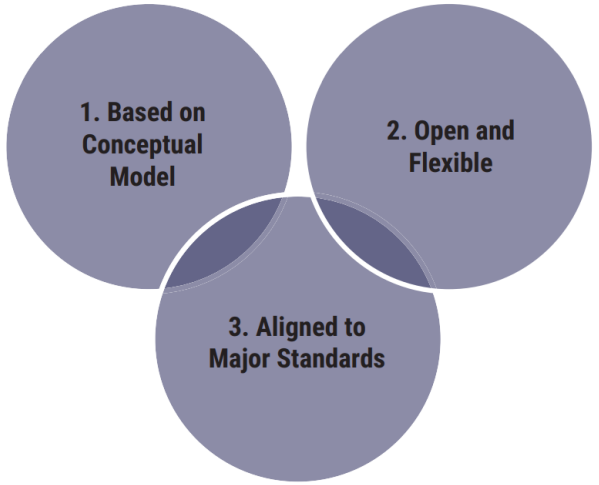



*Figure 3.2—Governance Framework Principles*

# 3. Princípios do Framework

2. Um framework de governança deve ser aberto e flexível. Ele deve permitir adição de novos conteúdos e ser capaz de tratar novas questões da maneira mais flexível possível, mantendo a integridade e a consistência.

*2. A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency*

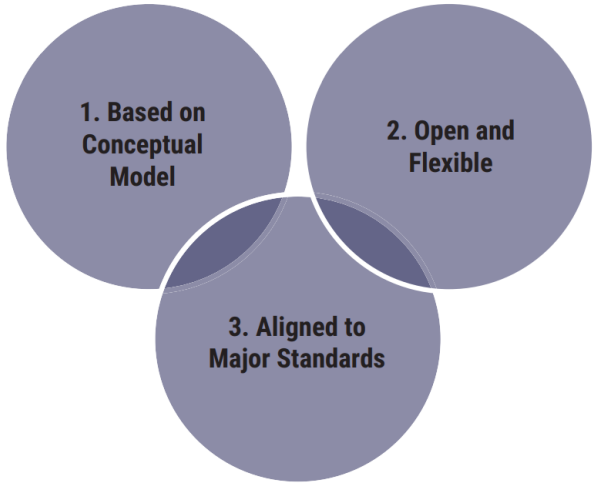



*Figure 3.2—Governance Framework Principles*

# 3. Princípios do Framework

3. Um framework de governança deve se alinhar aos padrões, frameworks e regulamentos relacionados relevantes.

*3. A governance framework should align to relevant major related standards, frameworks and regulations.*

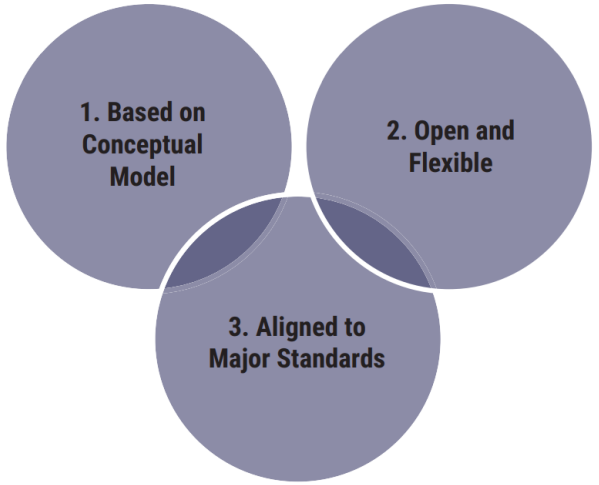
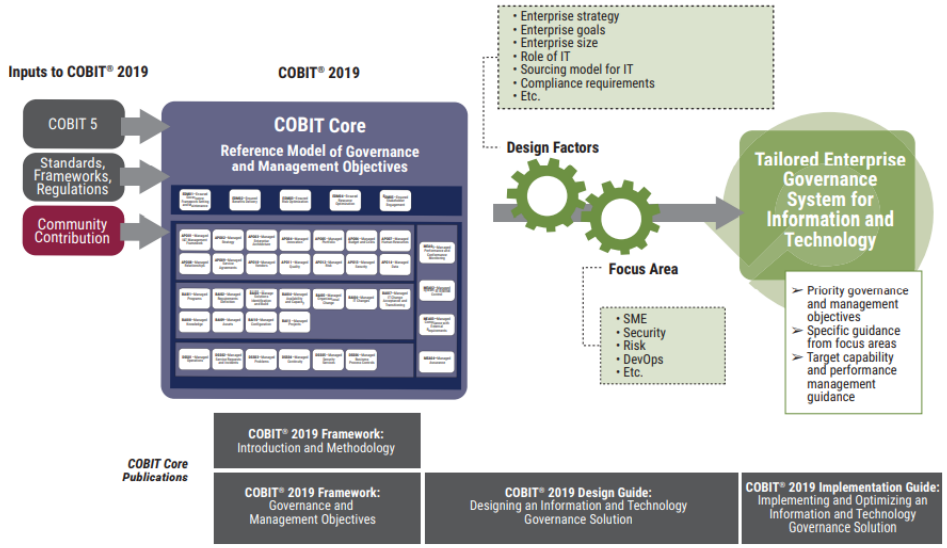



*Figure 3.2—Governance Framework Principles*

# COBIT 2019 Framework

## Cap. 04
## Conceitos Básicos

# 4.1 COBIT Overview




Atualmente, a família era composta por:

- ***COBIT®2019 Framework: Introduction and Methodology***
  Introduz conceitos-chave.

- ***COBIT®2019 Framework: Governance and Management Objectives***
  Descreve os 40 objetivos de governança e gestão, seus processos e outros components.

- **COBIT®2019 Design Guide: Designing an Information and Technology Governance Solution**
  Explora os fatores de desenho (*design factors*) que podem influenciar a governança e inclui um fluxo (*workflow*) para planejar um sistema de governança adaptado (*tailored*) à organização.

- ***COBIT®2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution***
  É uma evolução do COBIT® 5 Implementation Guide. Desenvolve um mapa (road map) para a melhoria contínua da governança. Pode ser combinado com o *COBIT® 2019 Design Guide*.

*"A number of these focus area content guides are already in preparation; others are planned. The set of focus area guides is open-ended and will continue to evolve."*
*COBIT 2019 Framework*

# 4.2 Governance and Management Objectives

Para que a I&T contribua para as metas da organização, alguns objetivos de governança e gestão devem ser atingidos…

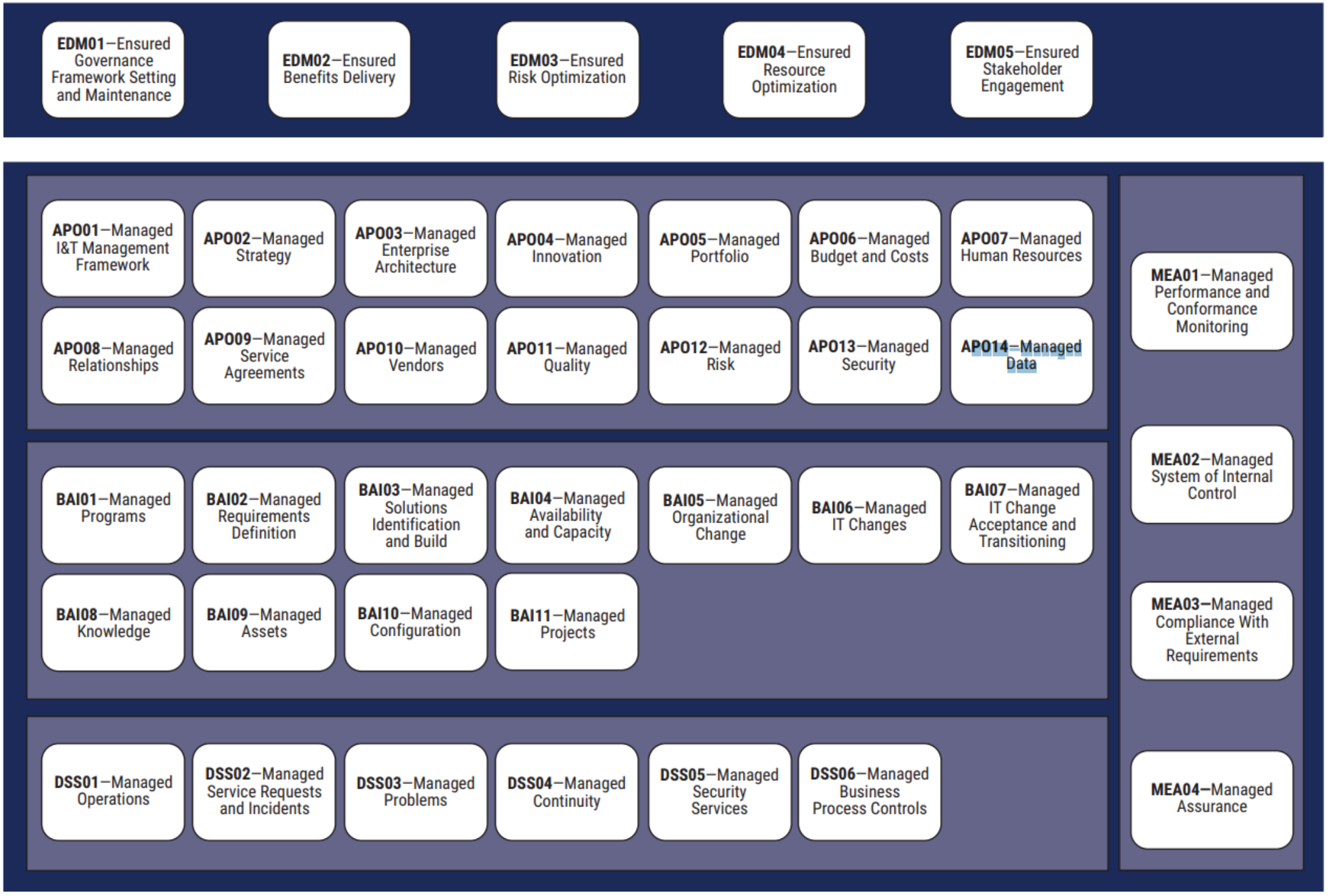
- Um objetivo de governança e gestão **sempre** está relacionado **a um processo** (com um nome idêntico ou similar) e a uma série de componentes relacionados que ajudam a atingir os objetivos.
- Objetivos de governança estão relacionados a processos de governança, enquanto objetivos de gestão estão relacionados a processos de gestão.

# 4.2 Governance and Management Objectives

Os objetivos são agrupados em cinco domínios.

- *Os **Objetivos de Governança** estão no domínio Evaluate, Direct and Monitor (**EDM**).*
  - *Neste domínio os responsáveis **avaliam** opções estratégicas, **direcionam** a gerência sênior com relação às opções estratégicas e **monitoram** o atingimento das estratégias.*

- *Os **Objetivos de Gerenciamento** estão agrupados em quatro domínios:*
  - *Align, Plan and Organize (**APO**) - coordenação geral sobre o alinhamento, planejamento, organização e estratégia das atividades de I&T.*
  - *Build, Acquire and Implement (**BAI**) - definição, aquisição e implementação das soluções de I&T e da sua integração nos processos de negócio.*
  - *Deliver, Service and Support (**DSS**) - cuida da entrega operacional e do suporte dos serviços de I&T.*
  - *Monitor, Evaluate and Assess (**MEA**) - monitoramento do desempenho e da conformidade da I&T com relação a objetivos de controle, metas de desempenho internos e requisitos externos.*


EDM01—Ensured Governance Framework Setting and Maintenance
EDM02—Ensured Benefits Delivery
EDM03—Ensured Risk Optimization
EDM04—Ensured Resource Optimization
EDM05—Ensured Stakeholder Engagement
APO01—Managed I&T Management Framework
APO02—Managed Strategy
APO03—Managed Enterprise Architecture
APO04—Managed Innovation
APO05—Managed Portfolio
APO06—Managed Budget and Costs
APO07—Managed Human Resources
APO08—Managed Relationships
APO09—Managed Service Agreements
APO10—Managed Vendors
APO11—Managed Quality
APO12—Managed Risk
APO13—Managed Security
APO14—Managed Data
BAI01—Managed Programs
BAI02—Managed Requirements Definition
BAI03—Managed Solutions Identification and Build
BAI04—Managed Availability and Capacity
BAI05—Managed Organizational Change
BAI06—Managed IT Changes
BAI07—Managed IT Change Acceptance and Transitioning
BAI08—Managed Knowledge
BAI09—Managed Assets
BAI10—Managed Configuration
BAI11—Managed Projects
DSS01—Managed Operations
DSS02—Managed Service Requests and Incidents
DSS03—Managed Problems
DSS04—Managed Continuity
DSS05—Managed Security Services
DSS06—Managed Business Process Controls
MEA01—Managed Performance and Conformance Monitoring
MEA02—Managed System of Internal Control
MEA03—Managed Compliance With External Requirements
MEA04—Managed Assurance

# 4.3 Components of the Governance System

**Componentes** são fatores que, individualmente ou de forma combinada, contribuem para a operação adequada do sistema de governança sobre a I&T.

componente

*adjetivo e substantivo de dois gêneros*

1. que ou o que compõe ou ajuda na composição de algo; que ou o que é parte constituinte de um sistema.
   "as (partes) c. de um sistema filosófico"
2. GRAMÁTICA GENERATIVA
   diz-se de ou cada uma das partes constituintes da gramática de uma língua.

- Eles interagem para criar um sistema holístico.
- Podem ser de diferentes tipos.
- Processos são os mais conhecidos dos componentes.


COBIT 2019


COBIT 5

# 4.3 Components of the Governance System

**Processes**

Descrevem um conjunto organizado de práticas e de atividades para produzir um conjunto de saídas (*outputs*) que sustentam as metas de I&T.

**Services, infrastructure and applications**

Incluem infraestrutura, tecnologia e aplicações necessários ao sistema de governança.

**Information**

É pervasiva e inclui toda a informação produzida e utilizada pela organização.

# 4.3 Components of the Governance System

**People, skills and competencies**

São necessárias para boas decisões, execução de ações corretivas e cumprimento bem sucedido de todas as atividades.

**Culture, ethics and behavior**

Tanto dos indivíduos quanto da empresa são frequentemente subestimados como fatores críticos de sucesso das atividades de governança e de gerenciamento.

**Organizational structures**

São as entidades-chave tomadoras de decisão na empresa.

**Principles, policies and frameworks**

Traduz comportamentos desejados em guias práticos para a gestão o dia a dia.

# 4.3 Components of the Governance System

Todos os componentes podem ser variantes ou genéricos.

**Genéricos**

São descritos no COBIT (*core model*) e se aplicam a qualquer situação.
**Contudo**, eles são genéricos e normalmente "*need customization before being practically implemented*".

**Variantes**

São baseados nos componentes genéricos, mas adaptados para um propósito específico ou para um contexto dentro de uma área foco (*e.g., for information security, DevOps, a particular regulation*).

# 4.4 Focus Area

Uma área foco descreve um determinado **tópico**, **domínio** ou **problema** (*issue*) que pode ser abordado por um conjunto de objetivos de governança e gestão e seus componentes.

*"The number of focus areas is virtually unlimited."*

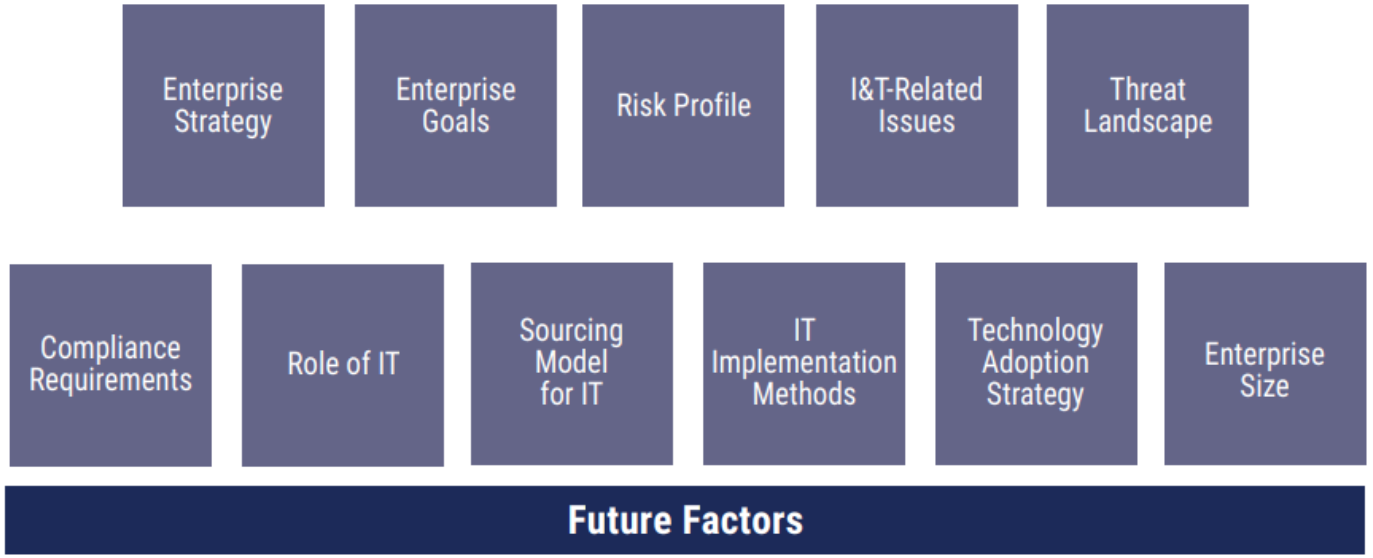
*"New focus areas can be added as required or as subject matter experts and practitioners contribute to the open-ended COBIT model."*

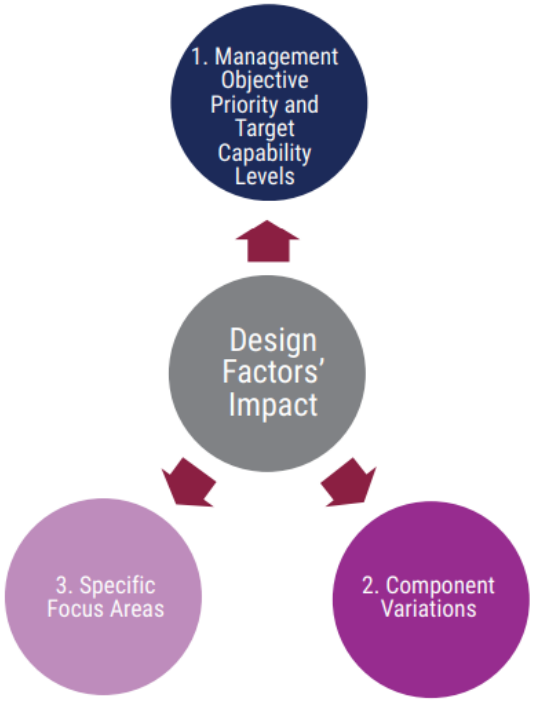
**ÁREAS FOCO**

- Uma Empresa
- A Segurança da Informação
- Transformação Digital
- Computação em Nuvem
- Gestão de Risco
- DevOps
- Etc.

# 4.5 Design Factors

São 11 ao todo os fatores de desenho descritos no COBIT 2019. Eles influenciam de diferentes maneiras a forma com que a adaptação se dará no sistema de governança na empresa.



# 4.5 Design Factors

**1. Enterprise Strategy (estratégia empresarial)**

Organizações podem adotar diferentes estratégias dentro dos quatro arquétipos abaixo.

Um organização pode ter uma estratégia primária e uma estratégia secundária.

| Figure 4.5—Enterprise Strategy Design Factor | |
|---|---|
| **Strategy Archetype** | **Explanation** |
| **Growth/Acquisition** | The enterprise has a focus on growing (revenues).[10] |
| **Innovation/Differentiation** | The enterprise has a focus on offering different and/or innovative products and services to their clients.[11] |
| **Cost Leadership** | The enterprise has a focus on short-term cost minimization.[12] |
| **Client Service/Stability** | The enterprise has a focus on providing stable and client-oriented service.[13] |

# 4.5 Design Factors

**2. Enterprise Goals (metas empresariais)**

A estratégia da empresa é percebida através de um conjunto de metas. O COBIT define 13 metas empresariais (EGs) estruturadas conforme as dimensões do *Balanced Scorecard* (BSc).

| Figure 4.6—Enterprise Goals Design Factor | | |
|---|---|---|
| **Reference** | **Balanced Scorecard (BSC) Dimension** | **Enterprise Goal** |
| **EG01** | Financial | Portfolio of competitive products and services |
| **EG02** | Financial | Managed business risk |
| **EG03** | Financial | Compliance with external laws and regulations |
| **EG04** | Financial | Quality of financial information |
| **EG05** | Customer | Customer-oriented service culture |
| **EG06** | Customer | Business-service continuity and availability |
| **EG07** | Customer | Quality of management information |
| **EG08** | Internal | Optimization of internal business process functionality |
| **EG09** | Internal | Optimization of business process costs |
| **EG10** | Internal | Staff skills, motivation and productivity |
| **EG11** | Internal | Compliance with internal policies |
| **EG12** | Growth | Managed digital transformation programs |
| **EG13** | Growth | Product and business innovation |

# 4.5 Design Factors

**3. Risk Profile (perfil de risco)**

O perfil de risco identifica os riscos relacionados a I&T aos quais a empresa está exposta e indica que áreas de risco estão excedendo o apetite ao risco da organização.

Seguem algumas categorias de risco que merecem consideração:

| Figure 4.7—Risk Profile Design Factor (IT Risk Categories) | | | |
|---|---|---|---|
| **Reference** | **Risk Category** | | |
| **1** | IT investment decision making, portfolio definition and maintenance | | |
| **2** | Program and projects lifecycle management | | |
| **3** | IT cost and oversight | | |
| **4** | IT expertise, skills and behavior | **12** | Third party/supplier incidents |
| **5** | Enterprise/IT architecture | **13** | Noncompliance |
| **6** | IT operational infrastructure incidents | **14** | Geopolitical issues |
| **7** | Unauthorized actions | **15** | Industrial action |
| **8** | Software adoption/usage problems | **16** | Acts of nature |
| **9** | Hardware incidents | **17** | Technology-based innovation |
| **10** | Software failures | **18** | Environmental |
| **11** | Logical attacks (hacking, malware, etc.) | **19** | Data and information management |

# 4.5 Design Factors

**4. I&T-related Issues (questões relacionadas a I&T)**

Um método para avaliar os riscos relacionados a I&T em uma organização é considerer quais riscos a organização está enfrentando, ou seja, quais riscos relacionados a I&T já se materializaram.

As mais comuns entre estas questões incluem:

| Figure 4.8—I&T-Related Issues Design Factor | |
|---|---|
| **Reference** | **Description** |
| **A** | Frustration between different IT entities across the organization because of a perception of low contribution to business value |
| **B** | Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value |
| **C** | Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT |
| **D** | Service delivery problems by the IT outsourcer(s) |
| **E** | Failures to meet IT-related regulatory or contractual requirements |
| **F** | Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems |
| **G** | Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets |
| **H** | Duplications or overlaps between various initiatives, or other forms of wasted resources |
| **I** | Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction |

# 4.5 Design Factors

**5. Threat Landscape (panorama de ameaças)**

O cenário sob o qual uma empresa opera pode ser classificado em “Normal” ou “Alto”:

| Figure 4.9—Threat Landscape Design Factor | |
|---|---|
| **Threat Landscape** | **Explanation** |
| **Normal** | The enterprise is operating under what are considered normal threat levels. |
| **High** | Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment. |

# 4.5 Design Factors

**6. Compliance Requirements (requisitos de conformidade)**

Os requisitos de conformidade ao qual a empresa está sujeita podem ser classificados de acordo com as categorias abaixo:

| Figure 4.10—Compliance Requirements Design Factor | |
|---|---|
| **Regulatory Environment** | **Explanation** |
| **Low compliance requirements** | The enterprise is subject to a minimal set of regular compliance requirements that are lower than average. |
| **Normal compliance requirements** | The enterprise is subject to a set of regular compliance requirements that are common across different industries. |
| **High compliance requirements** | The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions. |

# 4.5 Design Factors

**7. Role of IT (papel da TI)**

O papel da TI na empresa pode ser classificado como:

| IMPACTO PRESENTE | IMPACTO FUTURO: BAIXO | IMPACTO FUTURO: ALTO |
|---|---|---|
| ALTO | "FÁBRICA"<br>Ex.: companhias aéreas | ESTRATÉGICO<br>Ex.: bancos, seguradoras |
| BAIXO | SUPORTE<br>Ex.: indústrias | TRANSIÇÃO<br>Ex.: editoras, *e-commerce* |

**Figura 3 – "*Grid* Estratégico": impacto estratégico de aplicações de TI**
(Adaptado de MCFARLAN, 1984)

| Figure 4.11—Role of IT Design Factor | |
|---|---|
| **Role of IT**[17] | **Explanation** |
| **Support** | IT is not crucial for the running and continuity of the business process and services, nor for their innovation. |
| **Factory** | When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services. |
| **Turnaround** | IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services. |
| **Strategic** | IT is critical for both running and innovating the organization's business processes and services. |

# 4.5 Design Factors

**8. Sourcing model for IT (modelo de terceirização de TI)**

O modelo de terceirização que a empresa adota pode ser classificado como:

| Figure 4.12—Sourcing Model for IT Design Factor | |
|---|---|
| **Sourcing Model** | **Explanation** |
| **Outsourcing** | The enterprise calls upon the services of a third party to provide IT services. |
| **Cloud** | The enterprise maximizes the use of the cloud for providing IT services to its users. |
| **Insourced** | The enterprise provides for its own IT staff and services. |
| **Hybrid** | A mixed model is applied, combining the other three models in varying degrees. |

# 4.5 Design Factors

**9. IT implementation methods (métodos de implementação da TI)**

Os métodos que a empresa adota podem ser classificados como:

| Figure 4.13—IT Implementation Methods Design Factor | |
|---|---|
| **IT Implementation Method** | **Explanation** |
| **Agile** | The enterprise uses Agile development working methods for its software development. |
| **DevOps** | The enterprise uses DevOps working methods for software building, deployment and operations. |
| **Traditional** | The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations. |
| **Hybrid** | The enterprise uses a mix of traditional and modern IT implementation, often referred to as “bimodal IT.” |

# 4.5 Design Factors

**10. Technology Adoption Strategy (estratégia de adoção de tecnologia)**

A estratégia de adoção de tecnologia pode ser.

| Figure 4.14—Technology Adoption Strategy Design Factor | |
|---|---|
| **Technology Adoption Strategy** | **Explanation** |
| **First mover** | The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage. |
| **Follower** | The enterprise typically waits for new technologies to become mainstream and proven before adopting them. |
| **Slow adopter** | The enterprise is very late with adoption of new technologies. |

# 4.5 Design Factors

**11. Enterprise size (porte da empresa)**

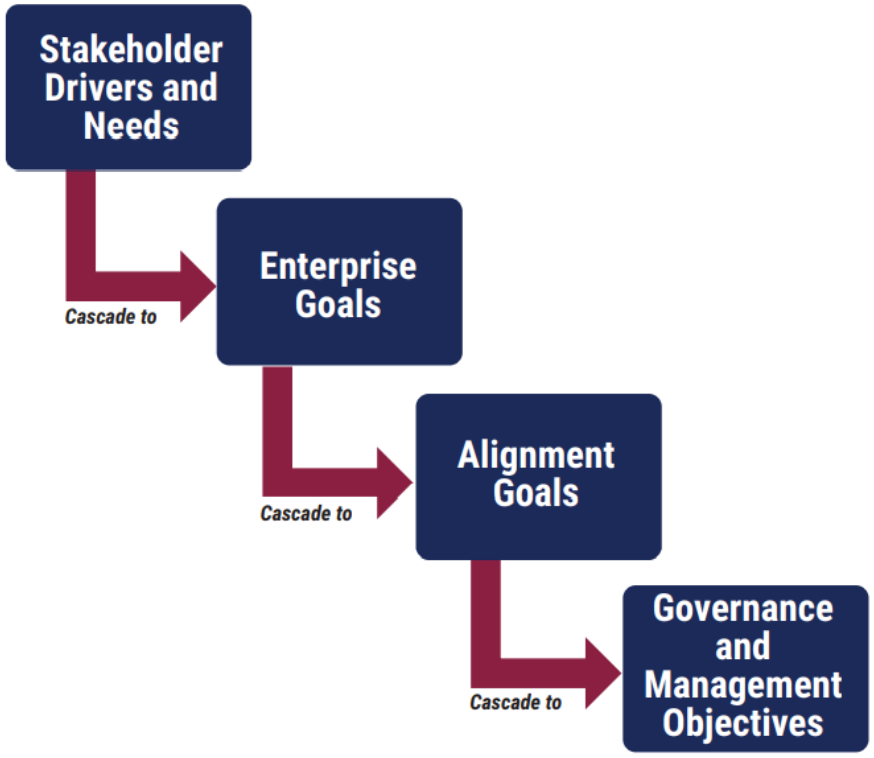
São identificadas duas categorias para o desenho (*design*) do sistema de governança empresarial.

| Figure 4.15—Enterprise Size Design Factor | |
|---|---|
| **Enterprise Size** | **Explanation** |
| **Large enterprise (Default)** | Enterprise with more than 250 full-time employees (FTEs) |
| **Small and medium enterprise** | Enterprise with 50 to 250 FTEs |

*"18 Micro-enterprises, i.e., enterprises with fewer than 50 staff members, are not considered in this publication."*
*COBIT 2019*

# 4.6 Goals Cascade

As necessidades das partes interessadas devem ser transformadas em estratégias executáveis.




COBIT 2019


COBIT 5

# 4.6 Goals Cascade

As metas empresariais são um dos fatores de desenho (*design*) do sistema de governança.

| | | ***Meta Empresarial*** | **Métrica** |
|---|---|---|---|
| **EG01** | Financial | Portfolio of competitive products and services | Time-to-market for new products and services |
| **EG02** | Financial | Managed business risk | Appropriate frequency of update of risk profile |
| **EG03** | Financial | Compliance with external laws and regulations | Cost of regulatory noncompliance, including settlements and fines |
| **EG04** | Financial | Quality of financial information | Cost of regulatory noncompliance with finance-related regulations |
| **EG05** | Customer | Customer-oriented service culture | Number of customer service disruptions |
| **EG06** | Customer | Business service continuity and availability | Percent of complaints as a function of committed serviceavailability targets |
| **EG07** | Customer | Quality of management information | Timeliness of management information |
| **EG08** | Internal | Optimization of internal business process functionality | Satisfaction levels of suppliers with supply chain capabilities |
| **EG09** | Internal | Optimization of business process costs | Ratio of cost vs. achieved service levels |
| **EG10** | Internal | Staff skills, motivation and productivity | Level of stakeholder satisfaction with staff expertise and skills |
| **EG11** | Internal | Compliance with internal policies | Percent of stakeholders who understand policies |
| **EG12** | Growth | Managed digital transformation programs | Number of programs on time and within budget |
| **EG13** | Growth | Product and business innovation | Level of awareness and understanding of business innovation opportunities |

# 4.6 Goals Cascade

*“This updated term also seeks to avoid the frequent misunderstanding that these goals indicate purely internal objectives of the IT department within an enterprise.”*

| | | Meta de Alinhamento |
|---|---|---|
| **AG01** | Financial | I&T compliance and support for business compliance with external laws and regulations |
| **AG02** | Financial | Managed I&T-related risk |
| **AG03** | Financial | Realized benefits from I&Tenabled investments and services portfolio |
| **AG04** | Financial | Quality of technology-related financial information |
| **AG05** | Customer | Delivery of I&T services in line with business requirements |
| **AG06** | Customer | Agility to turn business requirements into operational solutions |
| **AG07** | Internal | Security of information, processing infrastructure and applications, and privacy |
| **AG08** | Internal | Enabling and supporting business processes by integrating applications and technology |
| **AG09** | Internal | Delivery of programs on time, on budget and meeting requirements and quality standards |
| **AG10** | Internal | Quality of I&T management information |
| **AG11** | Internal | I&T compliance with internal policies |
| **AG12** | Learning and Growth | Competent and motivated staff with mutual understanding of technology and business |
| **AG13** | Learning and Growth | Knowledge, expertise and initiatives for business innovation |