

# IT Governance Framework with COBIT

1



**By,**

Mr. Kumar Pudashine (MEng, AIT, Bangkok)

CISA, CISM, CRISC, CDCP, CEH, CNDA, ITIL, COBIT 5, CCNP (Enterprise), ISO 27001:2013 LA, ISO 27001:2022 LA, JNCIA, AcitivIdentity Certified  
Cyber Security Consultant

December 2023

# Information

2

- Information is a key resource for all enterprises.
- Information is created, used, retained, disclosed and destroyed.
- Technology plays a key role in these actions.
- Technology is becoming pervasive in all aspects of business and personal life.

**What Benefits do Information and Technology Bring to Enterprises?**

# Enterprise Benefits : Enterprise and their Executives Strive to

3

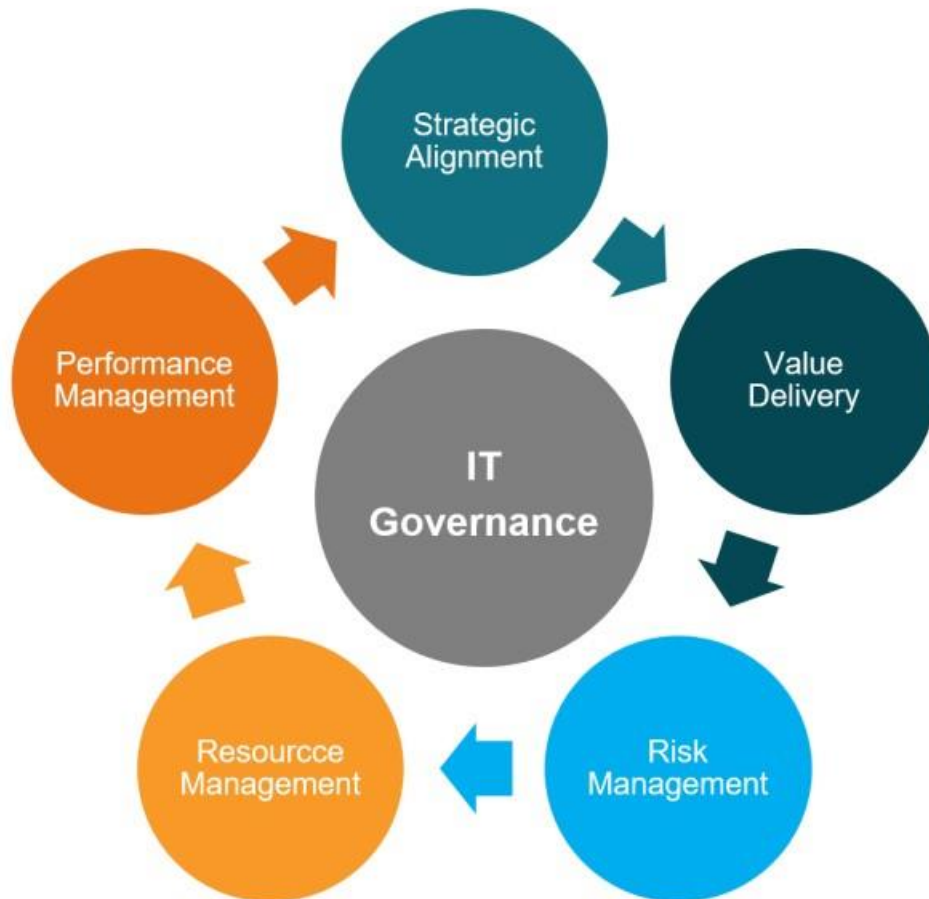
- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

**How can these benefits be realized to create enterprise stakeholder value?**

# Stakeholders Value: ??

4

- ✓ Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- ✓ Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- ✓ External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.



WHAT IS  
IT GOVERNANCE?



# COBIT : ??

6

Control Objectives for Information and Related  
Technologies

# NRB IT Guidelines 2012 : IT Governance

## 1. IT GOVERNANCE

IT has been adopted by most of the commercial banks to some degree from branch automation to providing alternate delivery channels<sup>i</sup>. This pervasive nature of IT has increased the challenge on governing it. Since IT is very critical in supporting and enabling business goals and is strategic for business growth, due diligence on its governance is essential. IT governance is a continuous process where IT strategy drives the process using necessary resources. In this context; NRB expects commercial banks to follow following guidelines

1. Bank<sup>1</sup> should have a board approved IT related strategy and policy and IT policy should be reviewed at least annually. IT strategy can be long term and short term and long term strategy should be mapped to short term strategy periodically. There should be detail operational procedures and guidelines to manage all IT operations.
2. Organizational structure for IT should be commensurate with the size, scale and nature of business activities carried out by the bank and may differ from bank to bank. Broadly the organization structure consists of Development, Technology, IT Operation and Information Assurance.
3. Bank should assess the requirement of expertise to successfully complete required IT functions. A periodic IT training requirement for IT personnel according to the IT functions of the bank should be assessed.
4. Bank should have performance monitoring and measuring system of IT functions and it should be reported to appropriate level of management.
5. IT related risk should also be considered in the risk management policy or operational risk policy of the bank and it should cover all e-banking activities and supplier activities as well. Periodic update of risk management is essential.
6. Banks are encouraged to implement international IT control framework such as COBIT<sup>ii</sup> as applicable to their IT environment.

# COBIT : What It is ??

8

COBIT provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.





# COBIT 2019 : New Concept ??

## INTRODUCTION

WHAT IS COBIT AND WHAT IT IS NOT: SETTING THE RIGHT EXPECTATIONS

### COBIT IS



- A framework for the governance and management of enterprise I&T
- COBIT defines the components to build and sustain a governance system
- COBIT defines the design factors that should be considered by the enterprise to build a best fit governance system
- COBIT is flexible and allows guidance on new topics to be added

### COBIT IS NOT



- A full description of the whole IT environment of an enterprise
- A framework to organize business processes
- An (IT-) technical framework to manage all technology
- COBIT does not make or prescribe any IT-related decisions

# COBIT5 : Framework

10

- ✓ COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
- ✓ COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- ✓ The COBIT 5 **Principles** and **Enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

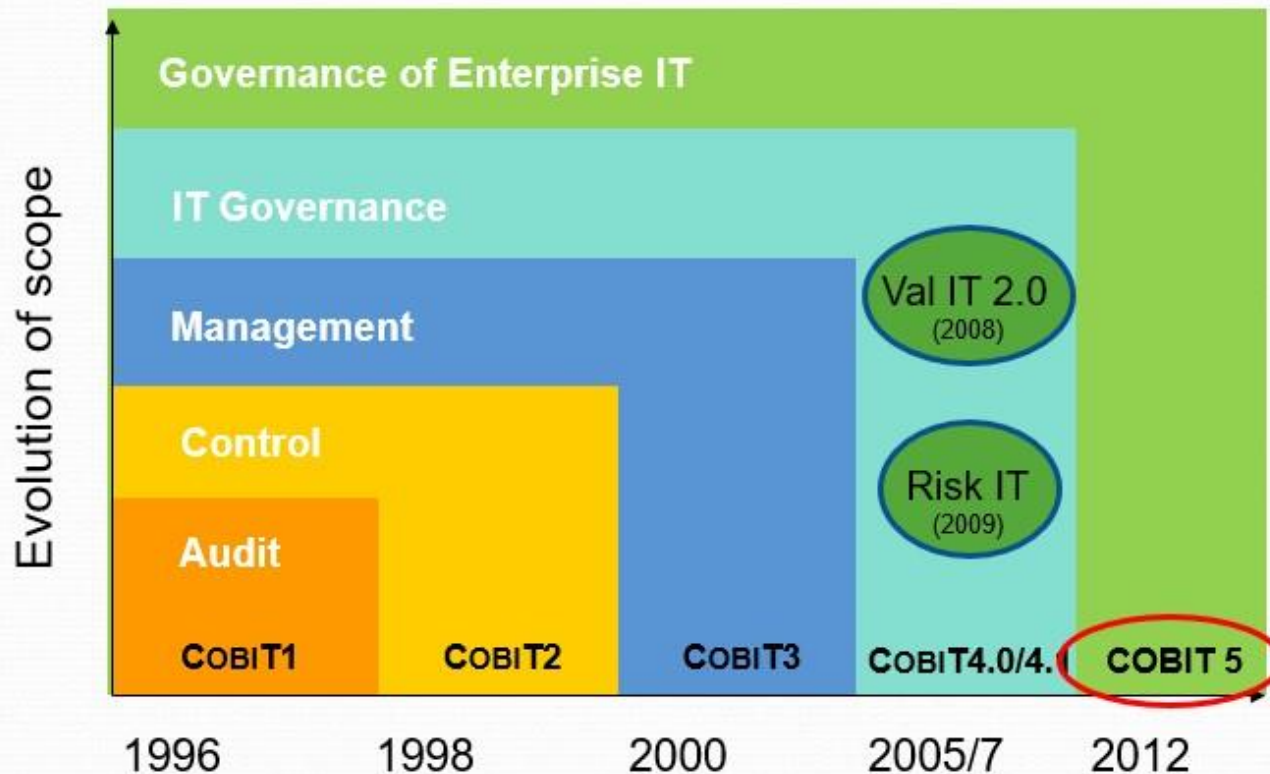
# COBIT5 : Governance and Management

11

- ✓ **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed-on direction and objectives (**EDM**).
- ✓ **Management** **plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**).

# COBIT : One Complete Business Framework (COBIT 1-COBIT 5)

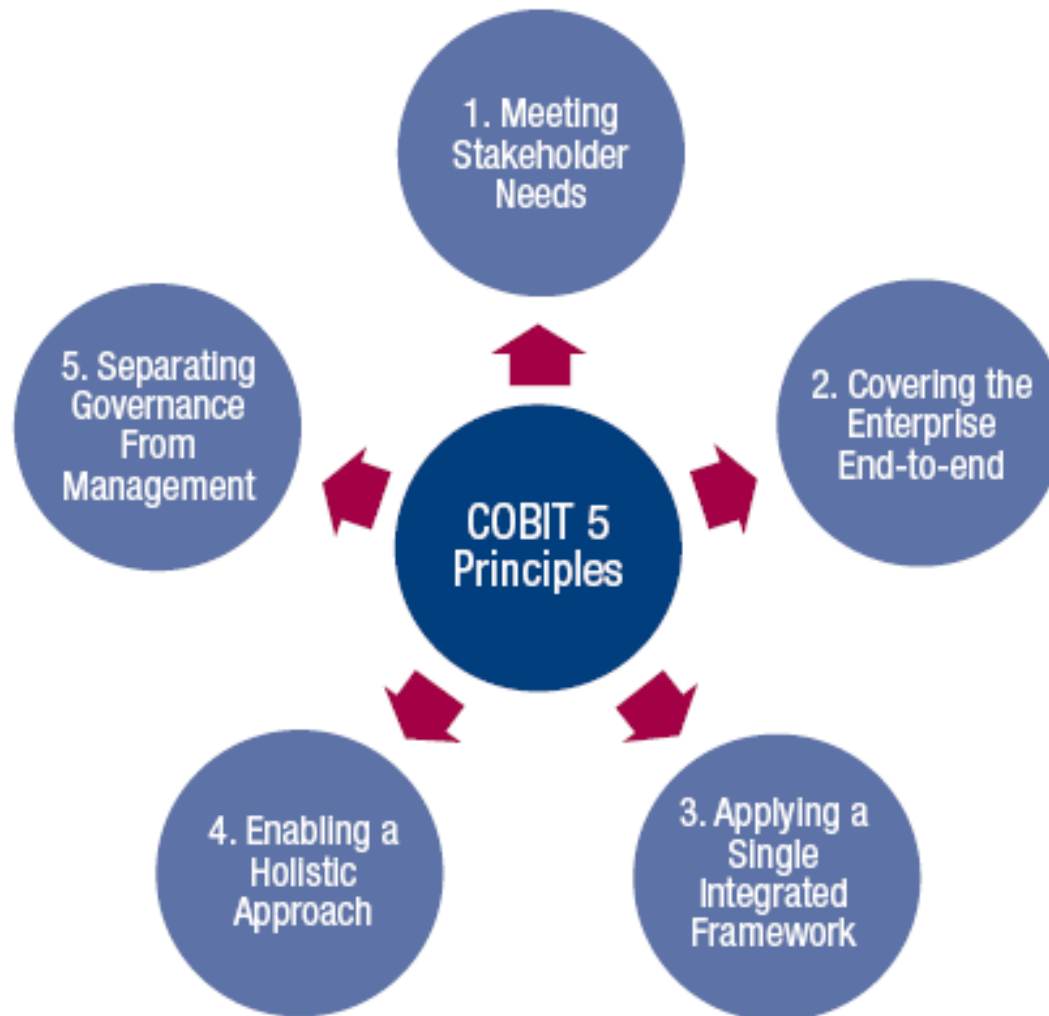
12



An business framework from ISACA, at [www.isaca.org/cobit](http://www.isaca.org/cobit)

# COBIT5 : Five Principles

13



# COBIT5 : Five Principles

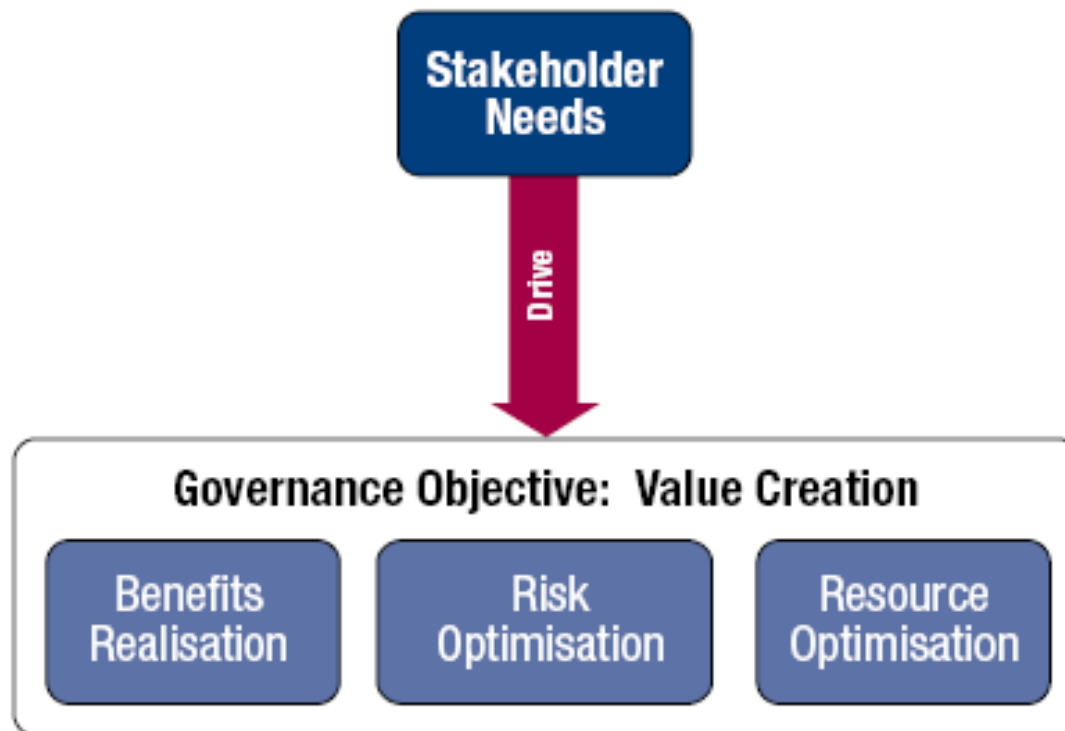
14

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

# Principle 1 : Meeting Stakeholders Need

15

Enterprises Exist to Create Value for their Stakeholders



# Principle 1 : Meeting Stakeholders Need

16

- ✓ Enterprises have **many** stakeholders, and ‘creating value’ means different—and sometimes conflicting—things to each of them.
- ✓ Governance is about negotiating and deciding amongst different stakeholders’ value interests.
- ✓ The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.
- ✓ For each decision, the following can and should be asked:
  - ✓ Who receives the benefits?
  - ✓ Who bears the risk?
  - ✓ What resources are required?



# Principle 1 : Meeting Stakeholders Need

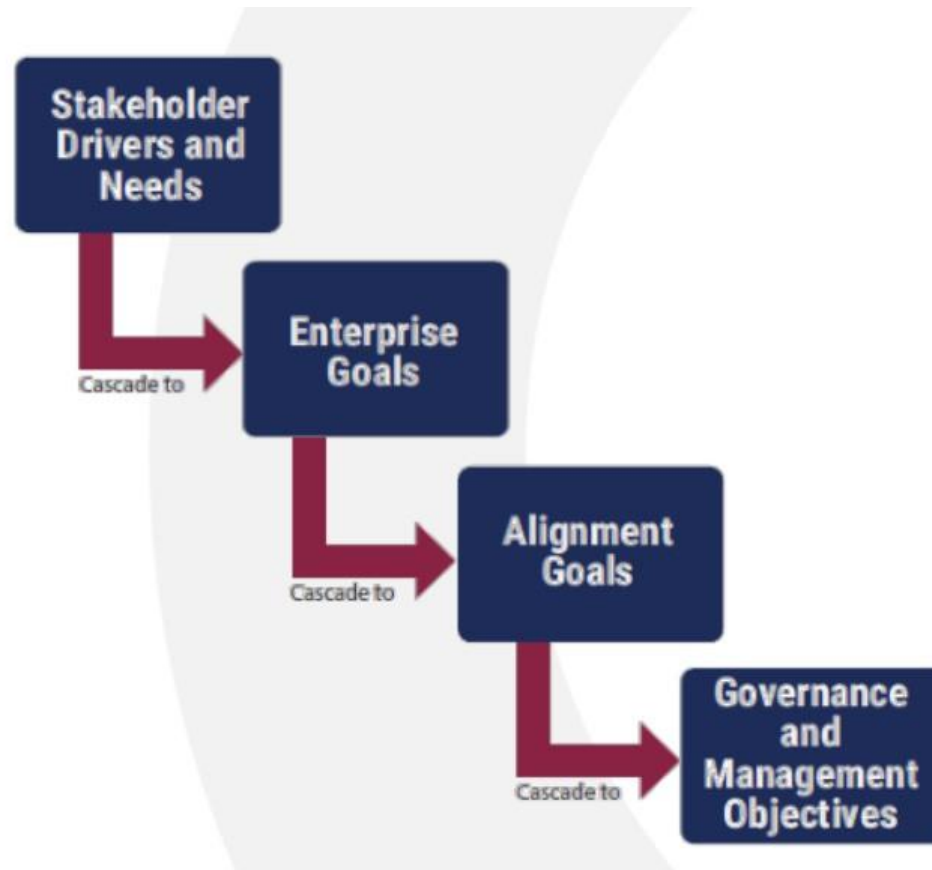
17

The COBIT 5 goals cascade translates stakeholder needs into specific, practical and customised goals within the context of the enterprise, IT-related goals and enabler goals.



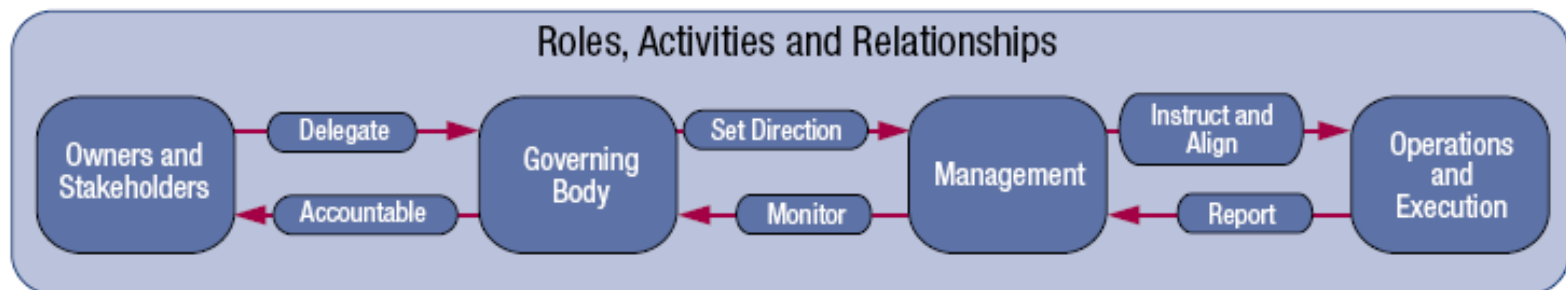
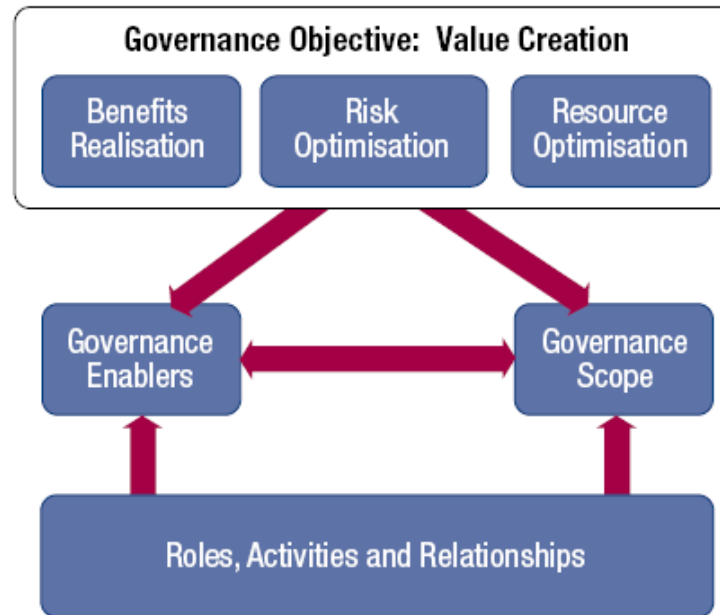
# COBIT 2019 : Goals Cascade

18



# Principle 2 : Covering the Enterprise End-to-End

19



# Principle 2 : Covering the Enterprise End-to-End

20

- Integrates Governance of Enterprise IT into Enterprise Governance
- COBIT 5 addresses the governance and management of information and related technology from an enterprise wide, end-to-end perspective.
- **COBIT 5 does not focus only on the 'IT function'**, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

# Principle 3 : Applying a Single Integrated Framework

21

- COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:
  - Enterprise: COSO, ISO/IEC 9000, ISO/IEC 31000
  - IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 Series, TOGAF, PMBOK/PRINCE2, CMMI
- This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

# Principle 3 : Applying a Single Integrated Framework

22

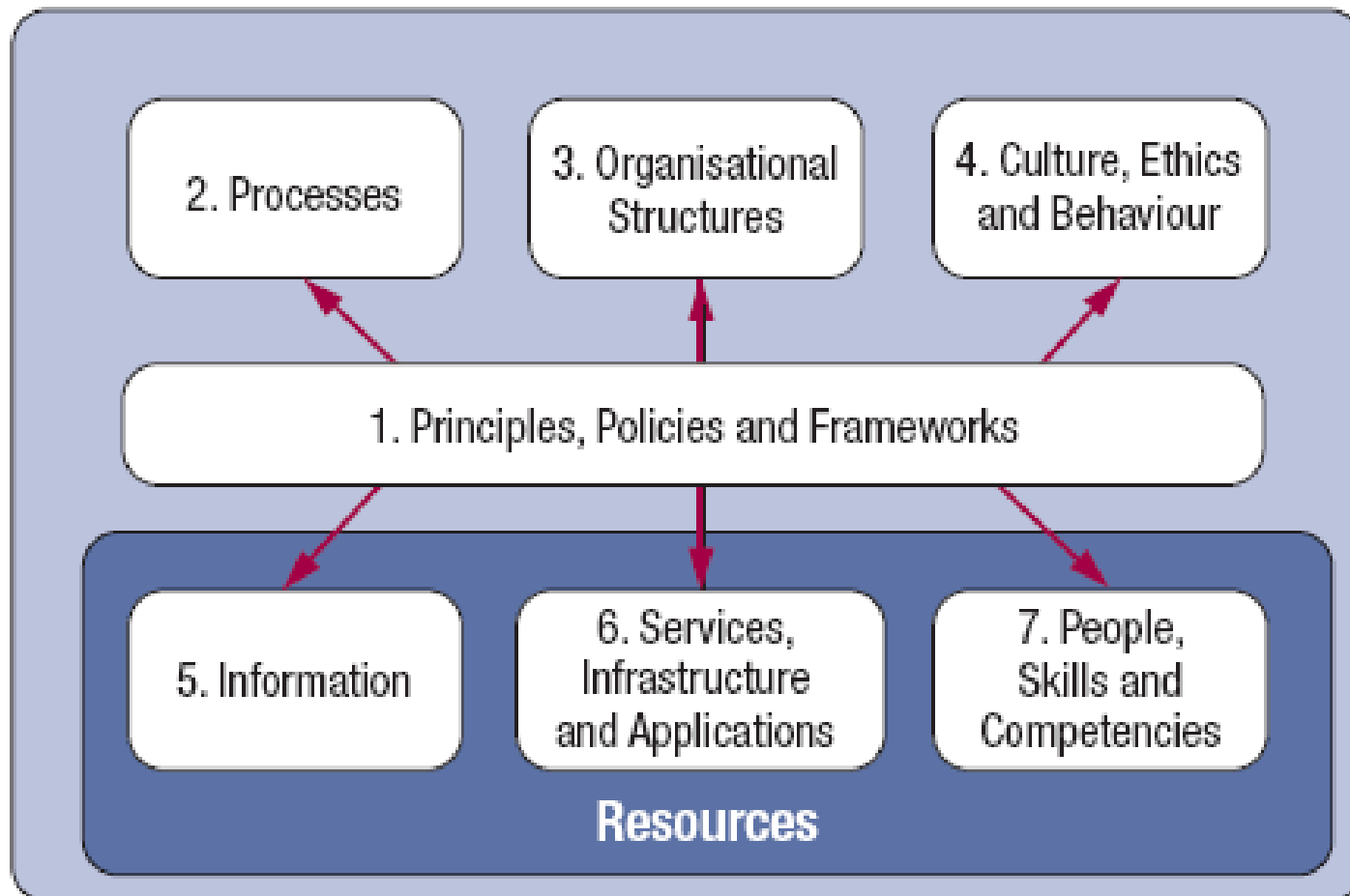


*TOGAF®*



# Principle 4 : Enabling a Holistic Approach

23



# Principle 5 : Separating Governance From Management

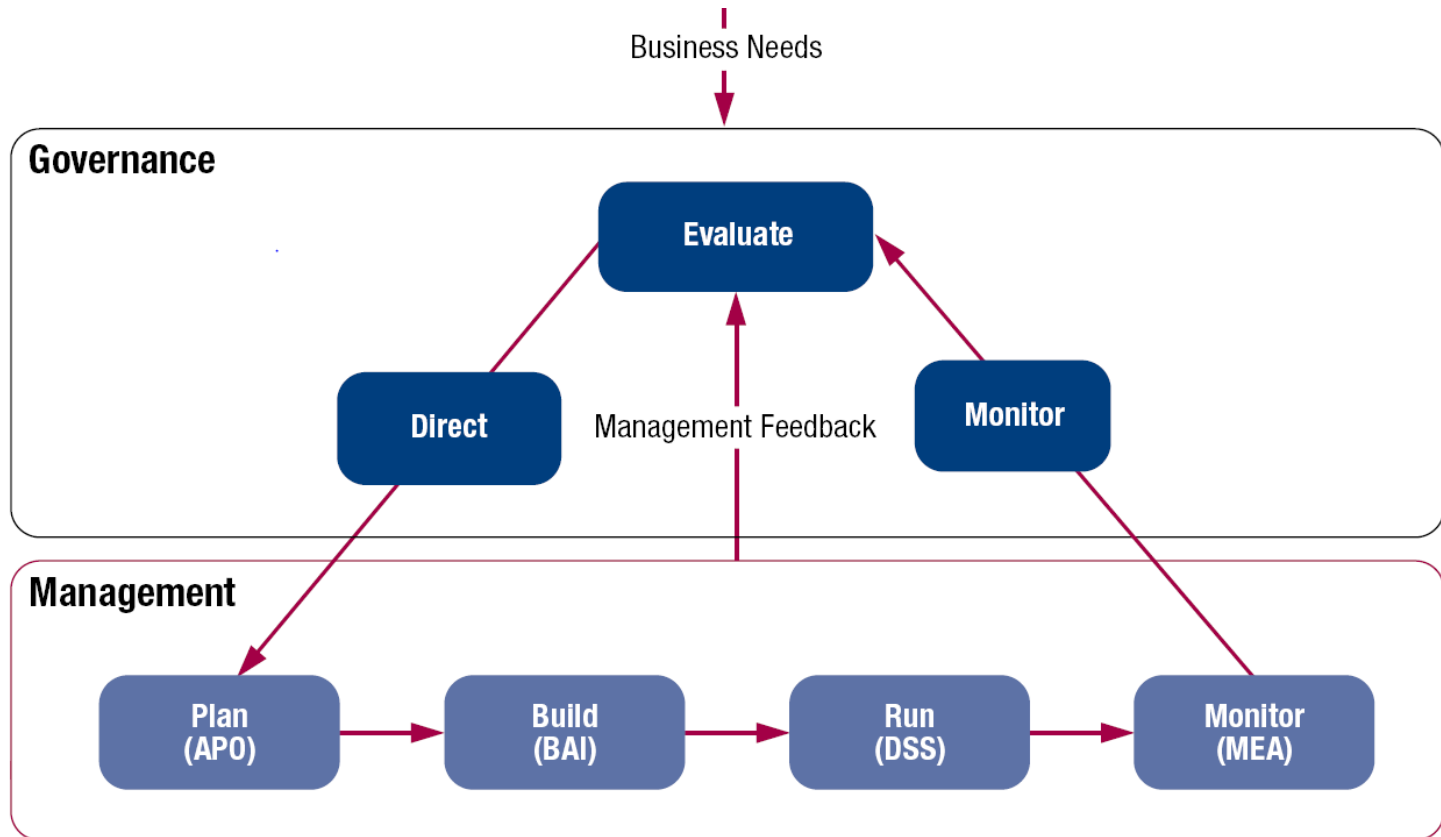
24

- The COBIT 5 framework makes a clear distinction between Governance and Management.
- **Governance**—In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
- **Management**—In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.



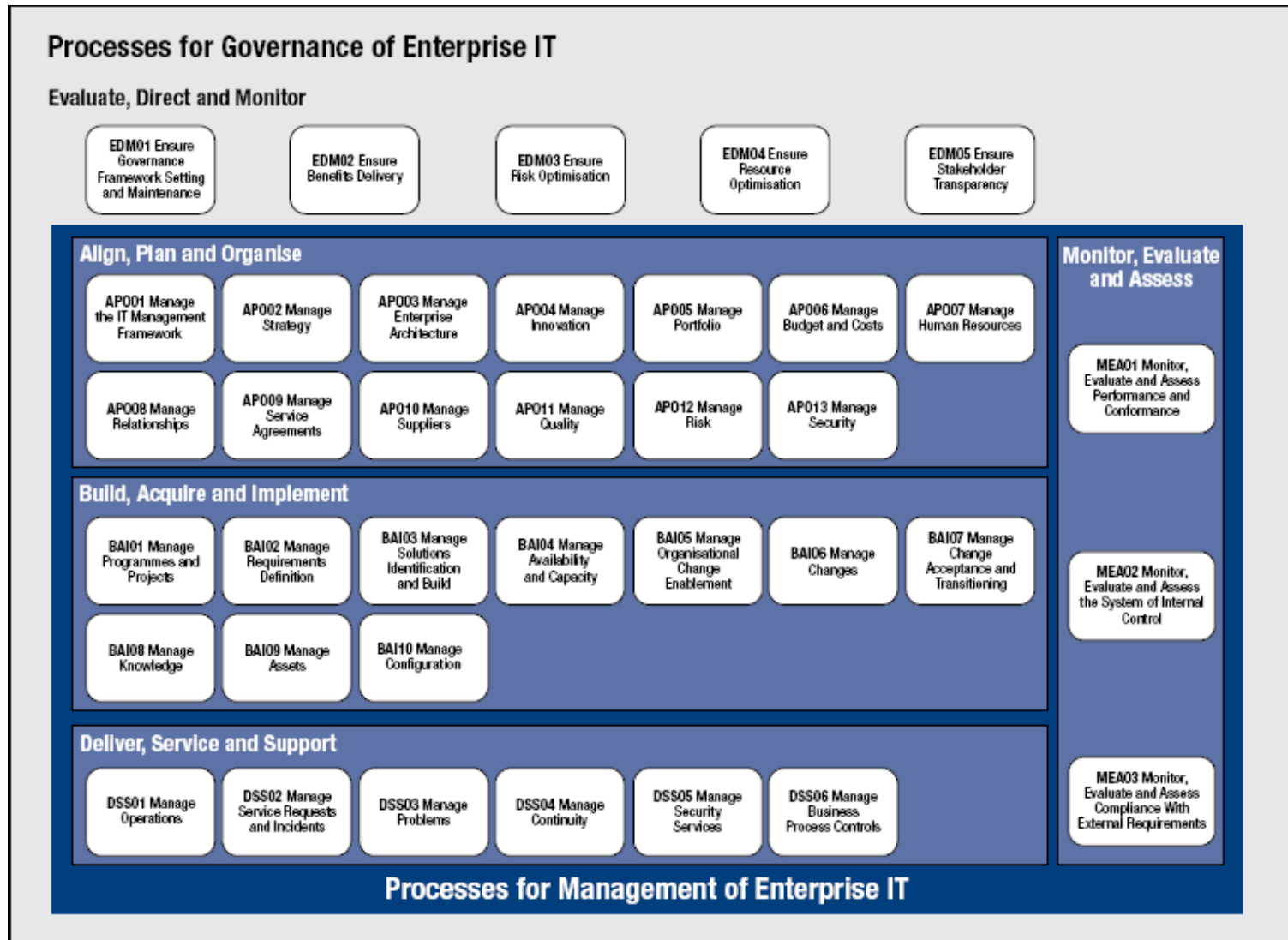
# Principle 5 : Separating Governance From Management

25



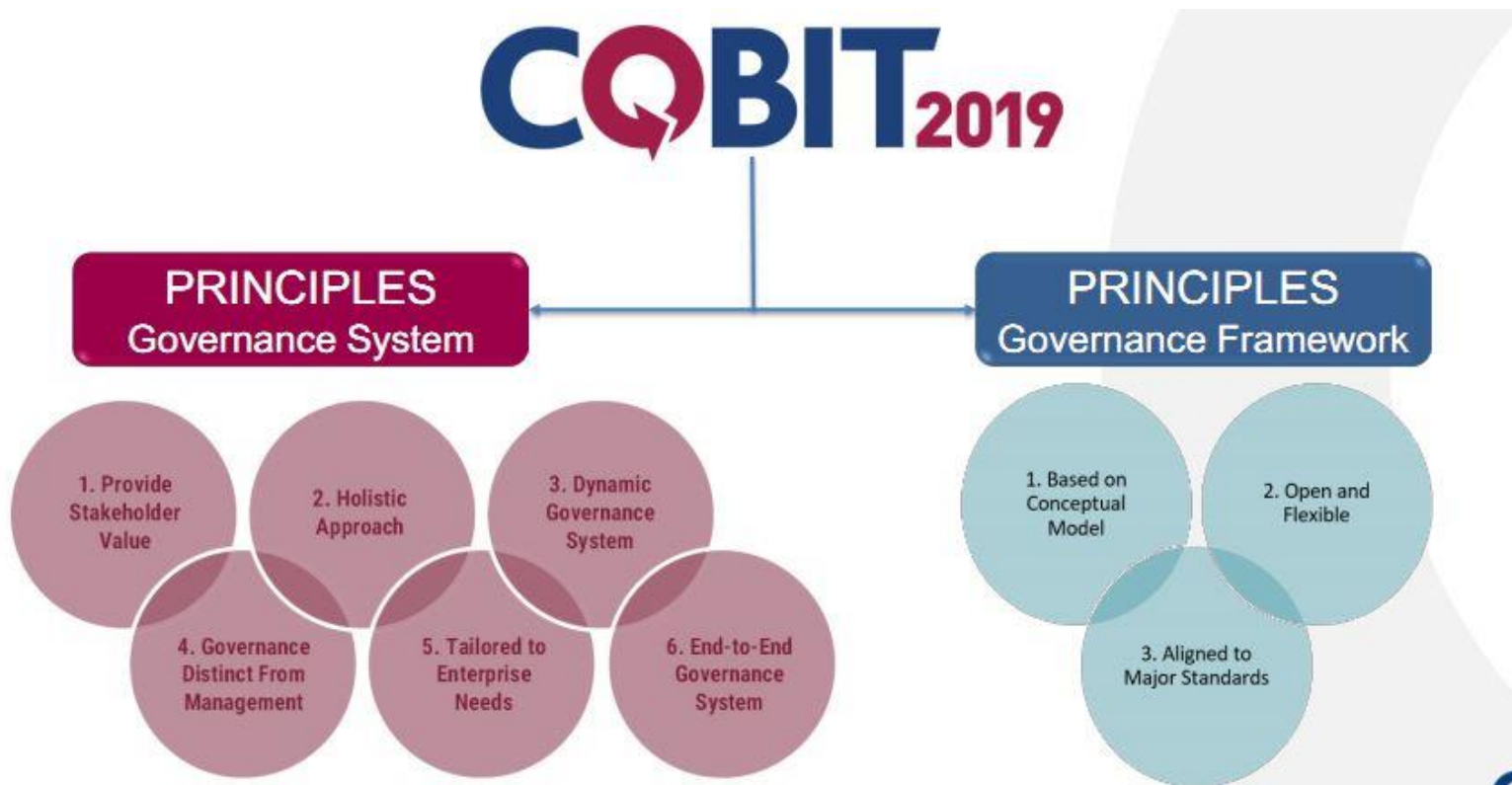
# COBIT 5: 37 Enabling Process

26



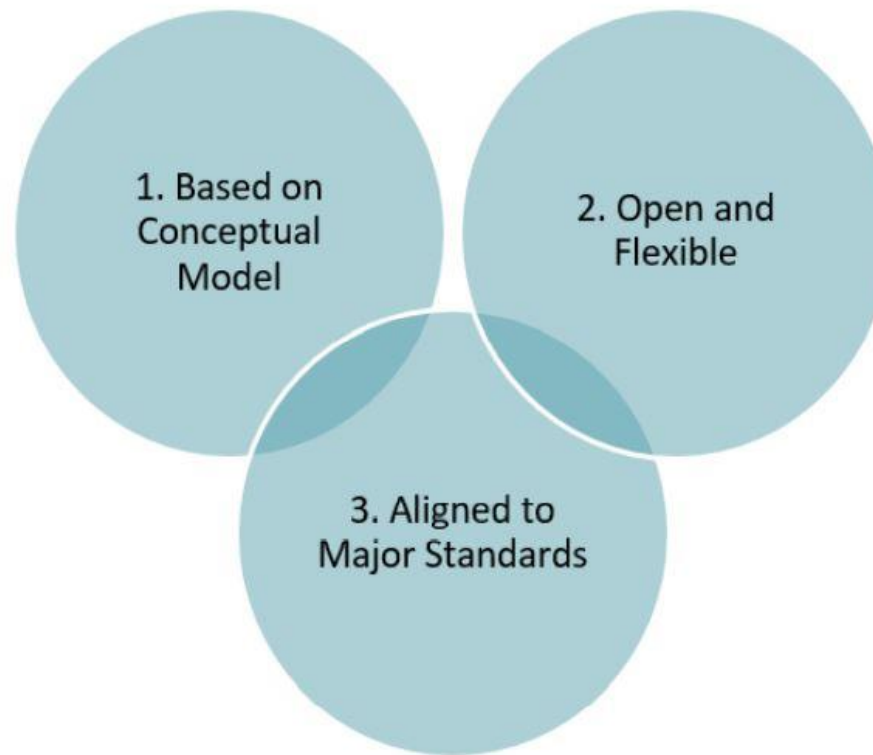
# COBIT 2019 : Principles

27



# Governance Framework Principles : 3 Principles ??

28



*Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 3 COBIT Principles, Figure 3.2*

# COBIT 2019: Governance Systems and Components

29

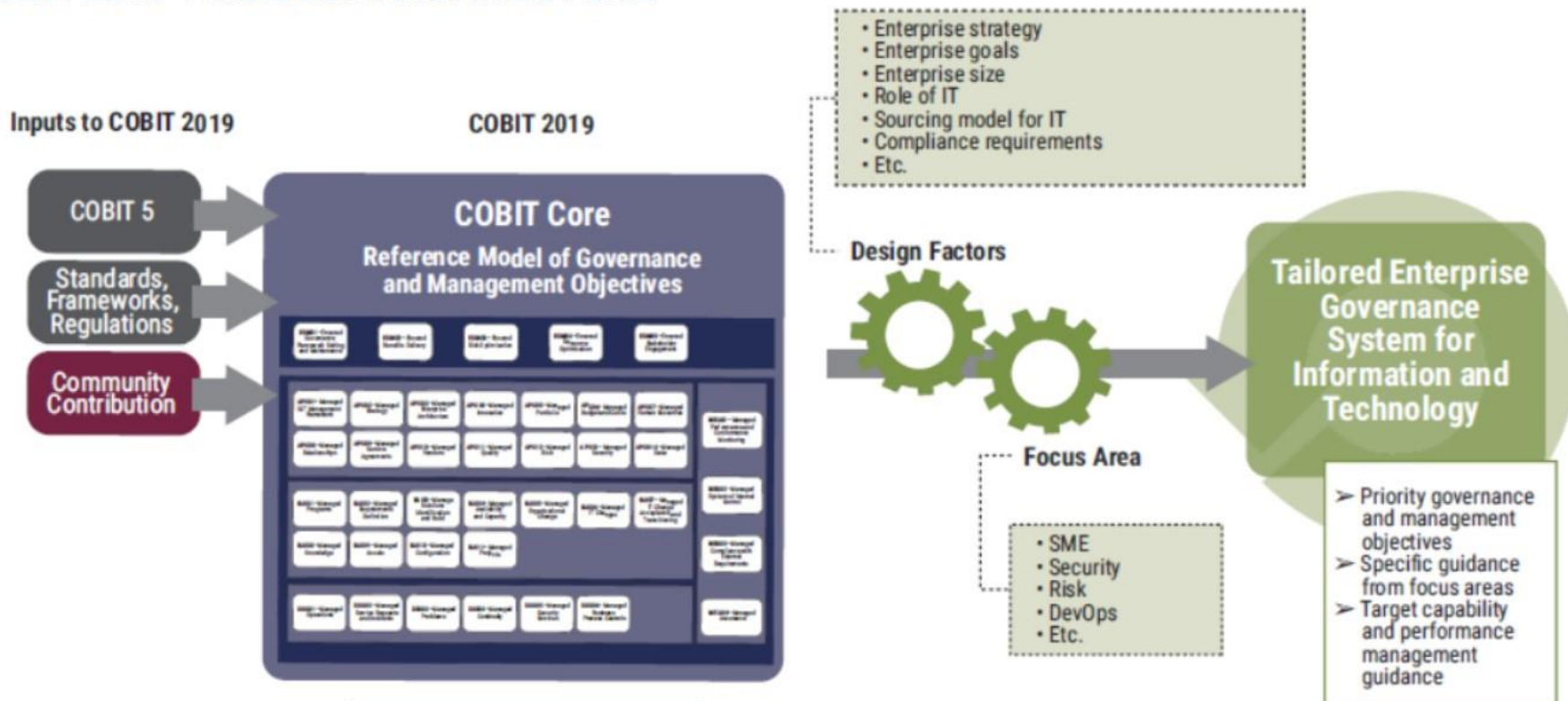


*Reference: COBIT® 2019 Framework: Basic Concepts: Governance Systems and Components, Figure 4.3*

# COBIT 2019 : Product Architecture

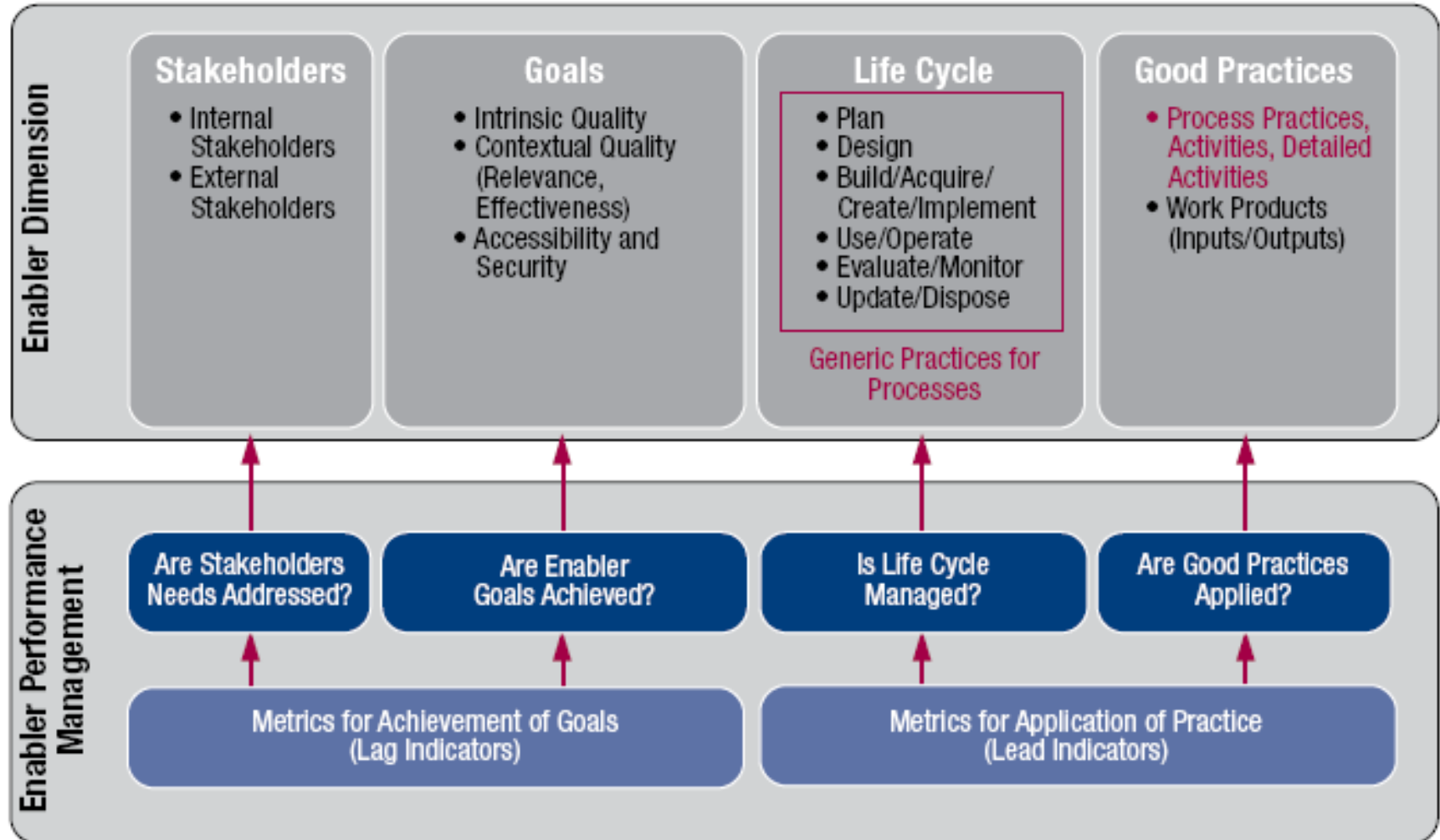
30

## COBIT 2019 PRODUCT ARCHITECTURE



# COBIT 5: Enabling Process

31



# COBIT 2019 : Governance and Management Objectives

32

Governance  
objectives

Management objectives

**EDM**  
Evaluate, Direct  
and Monitor

**APO**  
Align, Plan and  
Organize

**BAI**  
Build, Acquire and  
Implement

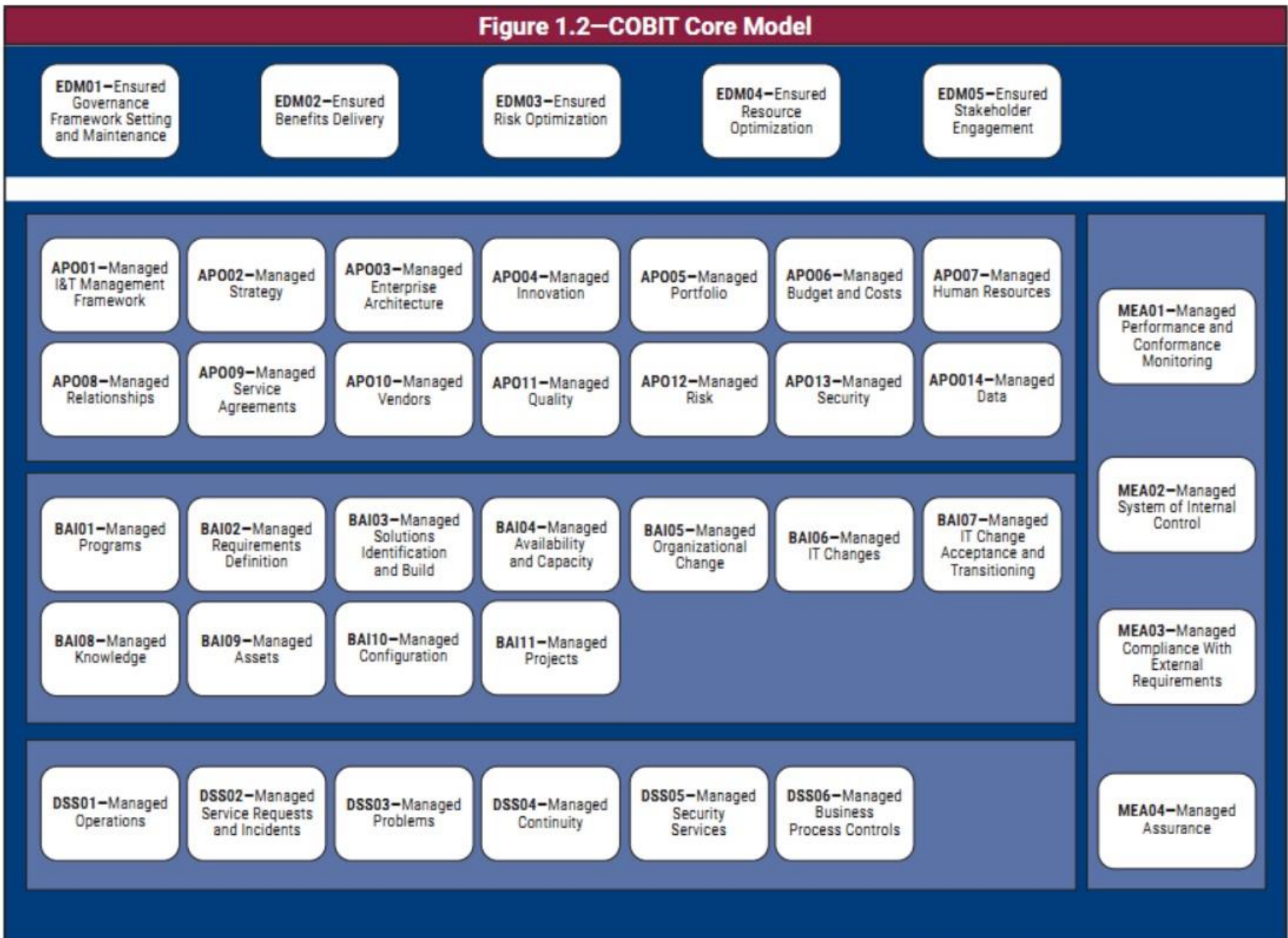
**DSS**  
Deliver, Service and  
Support

**MEA**  
Monitor, Evaluate  
and Assess

**COBIT** 2019

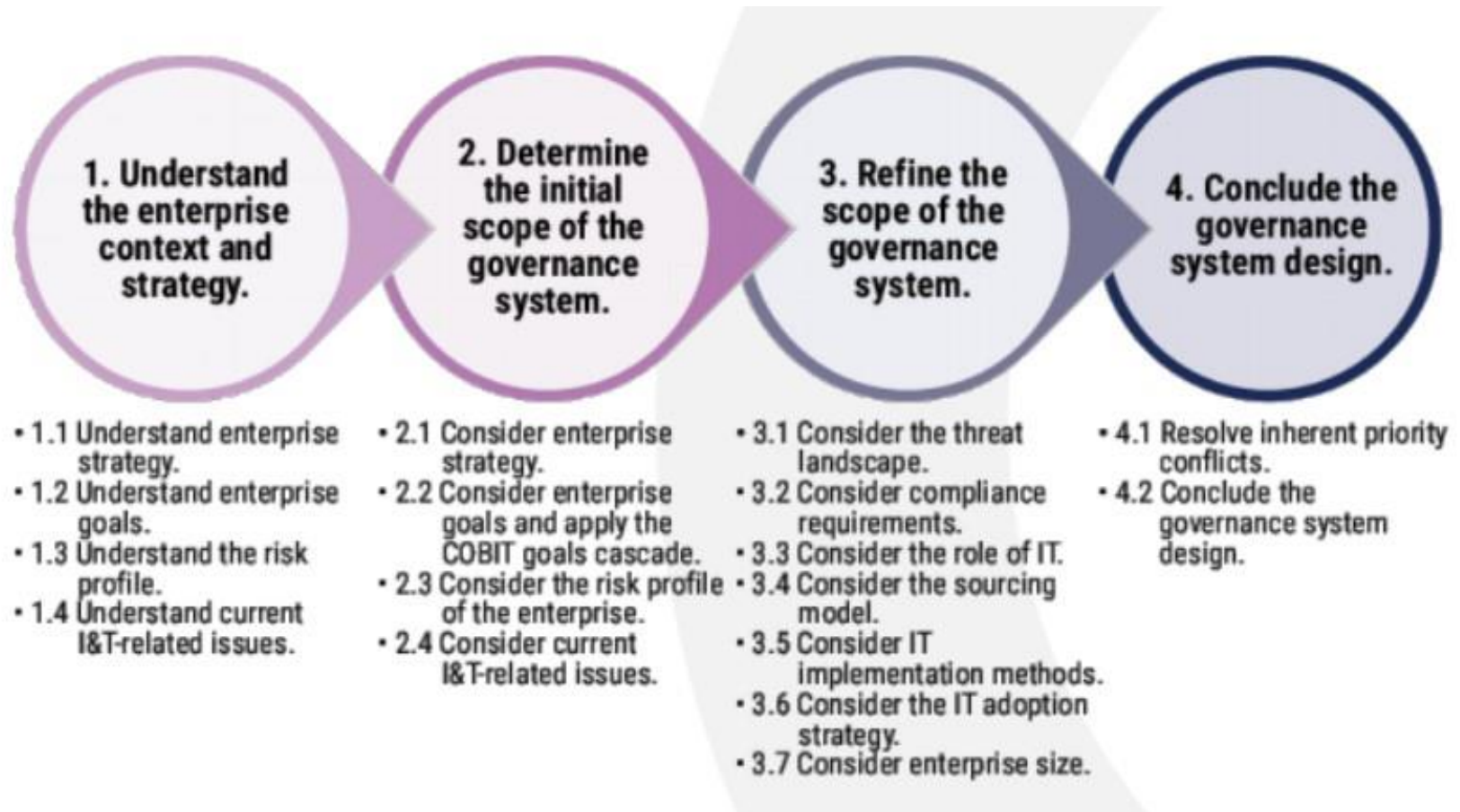


**Figure 1.2—COBIT Core Model**



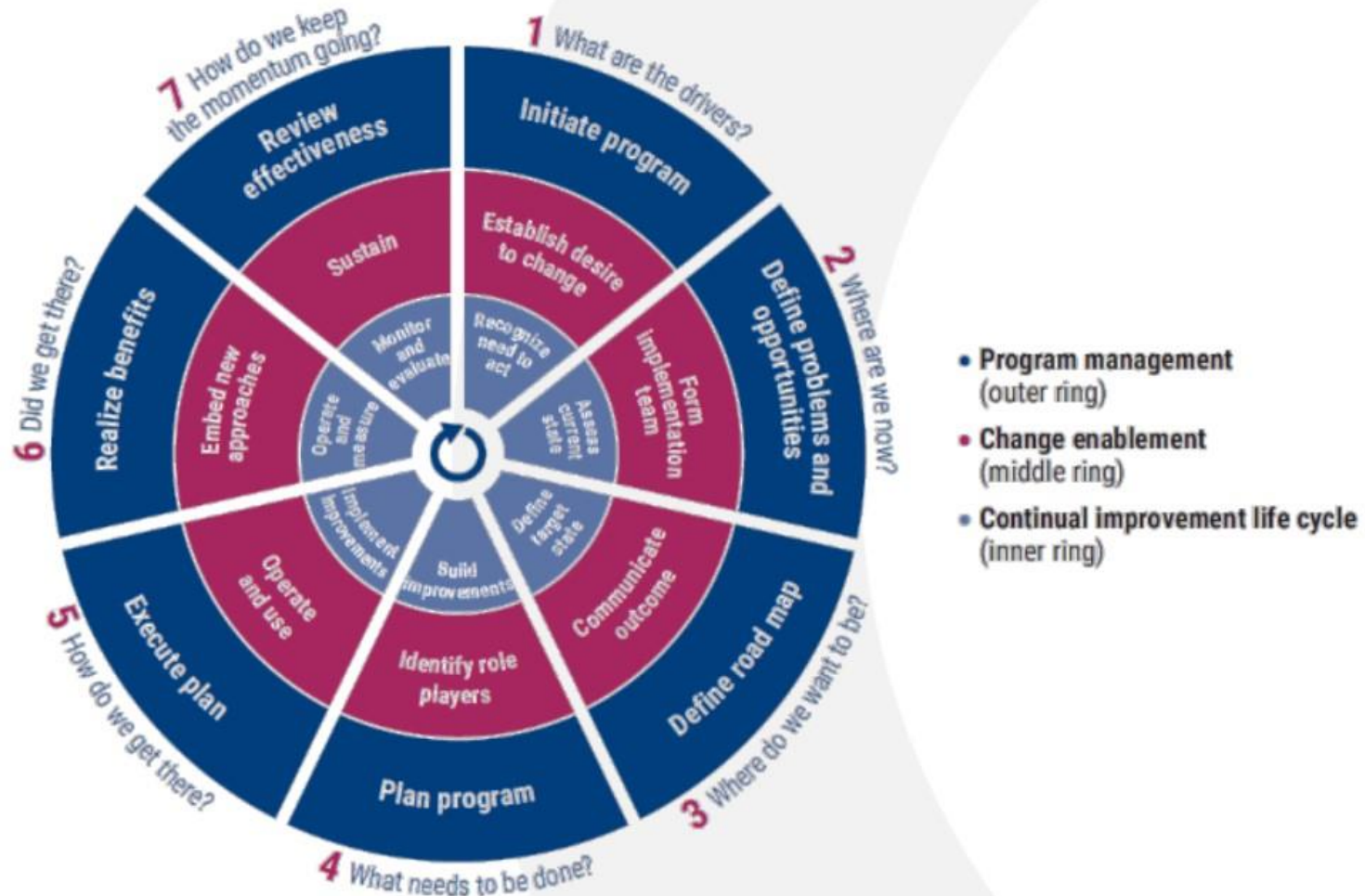
# Designing and Implementing: Tailored Governance System

34



# Designing and Implementing: Tailored Governance System

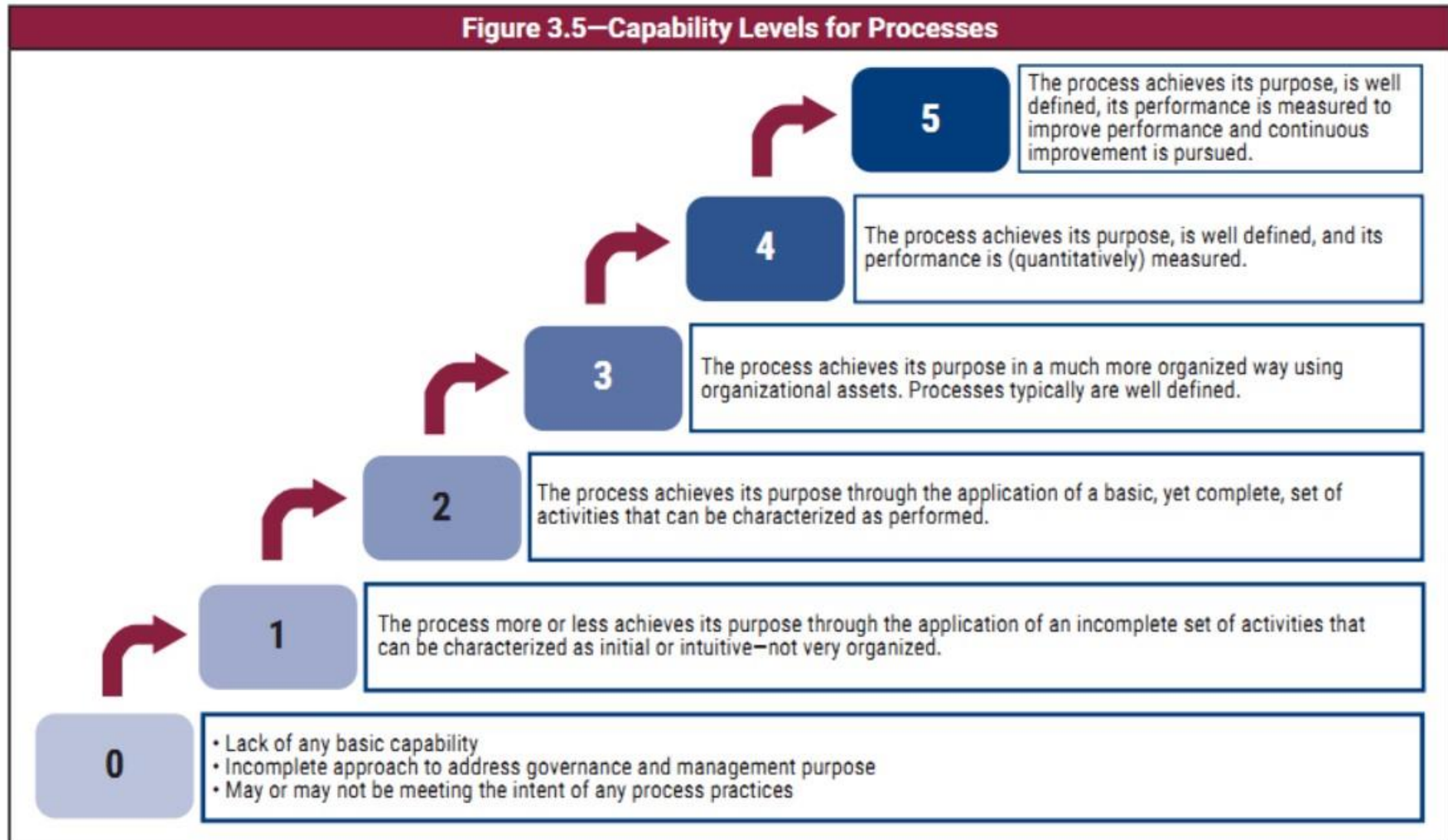
35



# Capability Levels of Process

36

Figure 3.5—Capability Levels for Processes

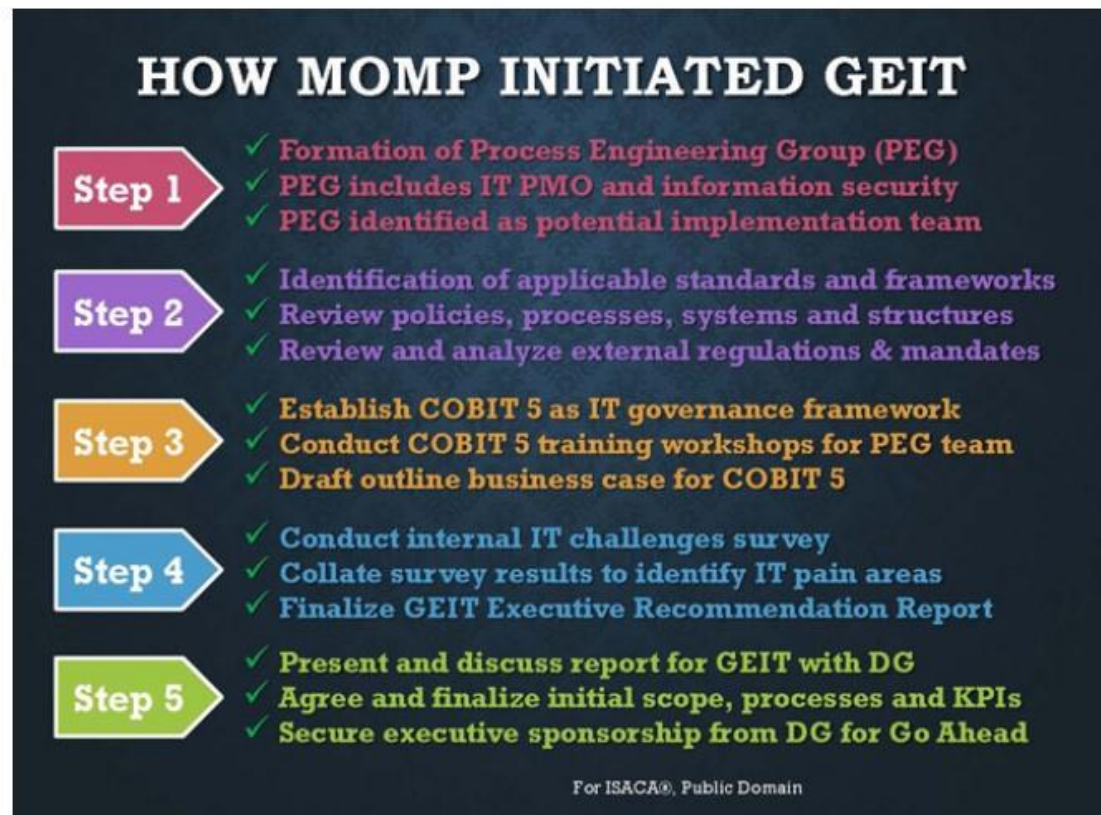




# Case 1 : Ministry of Manpower (MoMP), Sultanate of Oman

37

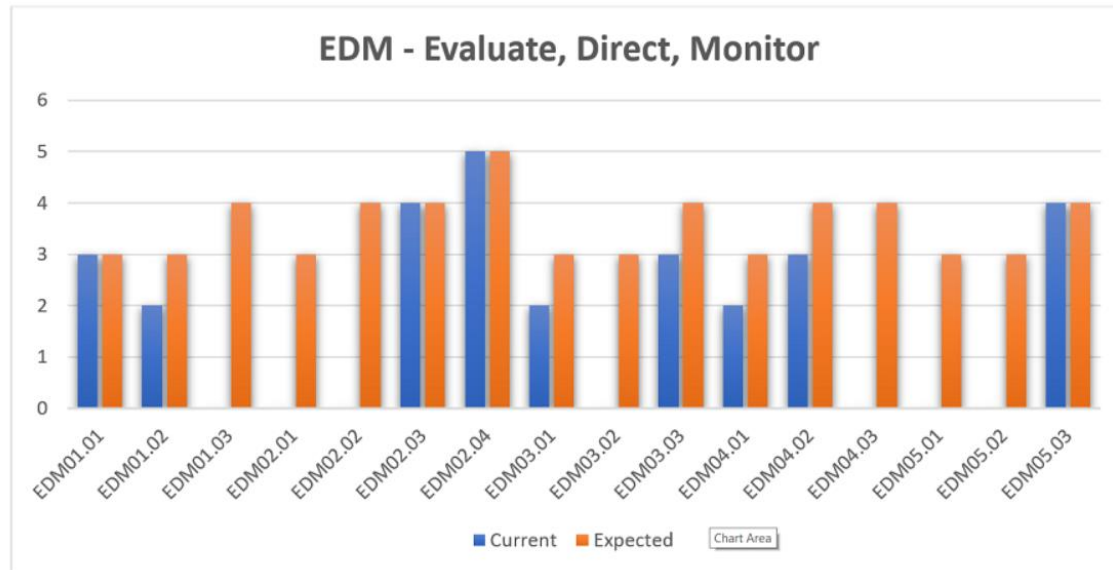
Figure 2—Steps to Initiate GEIT



Source: R. Banerjee, R. A. Al-Lawati and M. M. Al-Balushi. Reprinted with permission.

# Case 2 : A COBIT 2019 Use Case: Financial Institutions in Georgia

38



<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/a-cobit-2019-use-case-financial-institutions-in-georgia>

# Case 3: Implementing COBIT 5 in the Jordanian Banking System

39

## CENTRAL BANK REQUIREMENTS

The requirements for Jordanian banks, at first glance, appears very aggressive. However, once momentum gained, the results have been somewhat positive.

One requirement that has created much activity is that banks are required to implement all 37 Processes of the COBIT 5 framework targeting specific capability levels. As noted below, these processes are required to achieve a capability level 3 within 18 months of the publication of the regulation and achieve a capability level 5 within three years of the publication of the regulation.



Figure 3, Process Capability Requirements

*Thank  
you*

