# COBIT 5 Webinar -2

Nanda Mohan Shenoy D

CAIIB,DBM-Part I,CISA,NCFM in(Commodities, FNO, Currency Derivatives, AMFI , Depository) PG Diploma in IRPM, PG Diploma in EDP and Computer Management, DIM,LA ISO 9001,LA ISO 27001

President ISACA Mumbai Chapter(2010-2012)

# What is COBIT

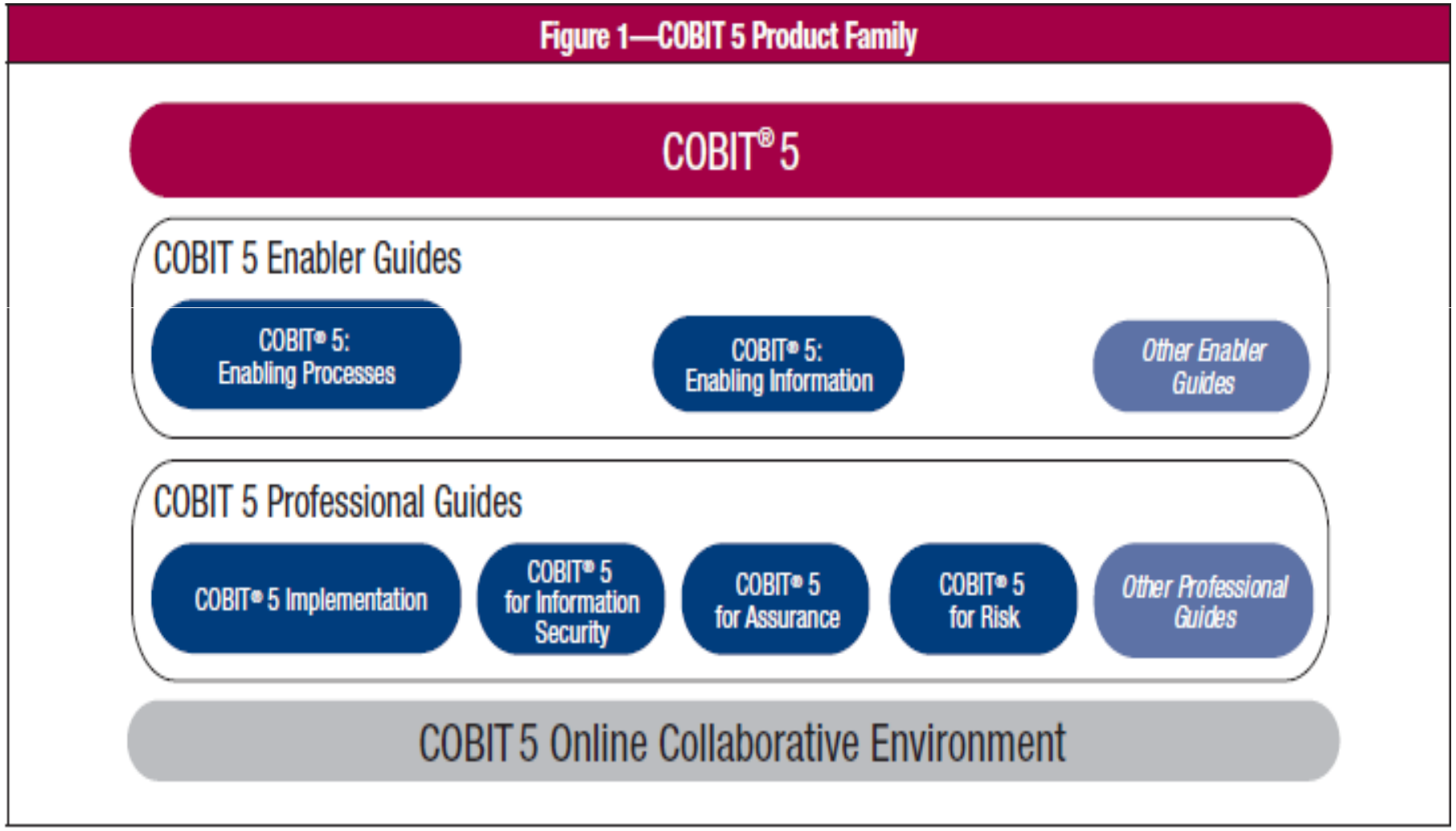
- It was an acronym for

**C OBIT** is a Framework by ISACA

- Latest Version 5.0 released on 10th April 2012

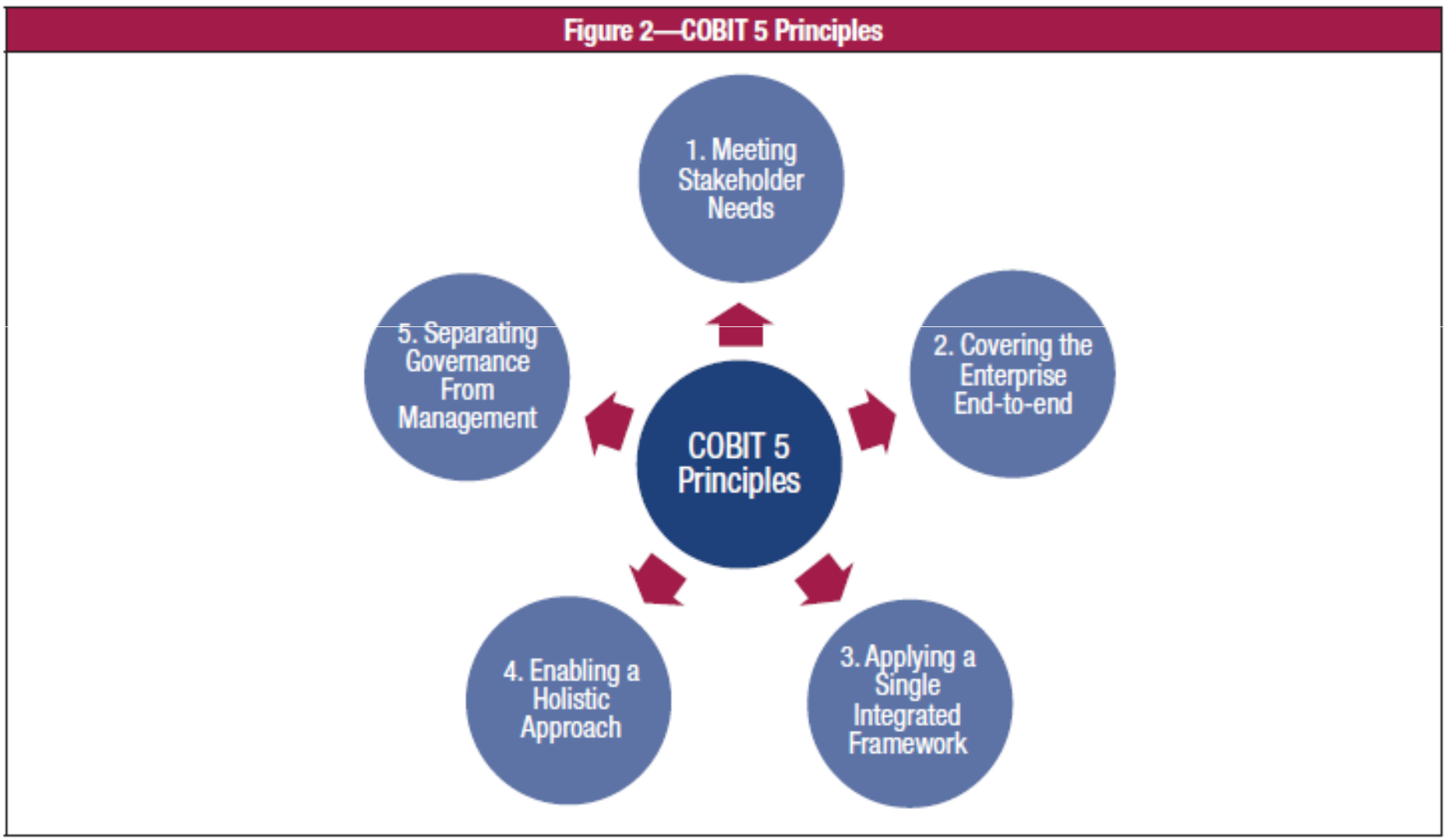
# Inputs?

# Product Family



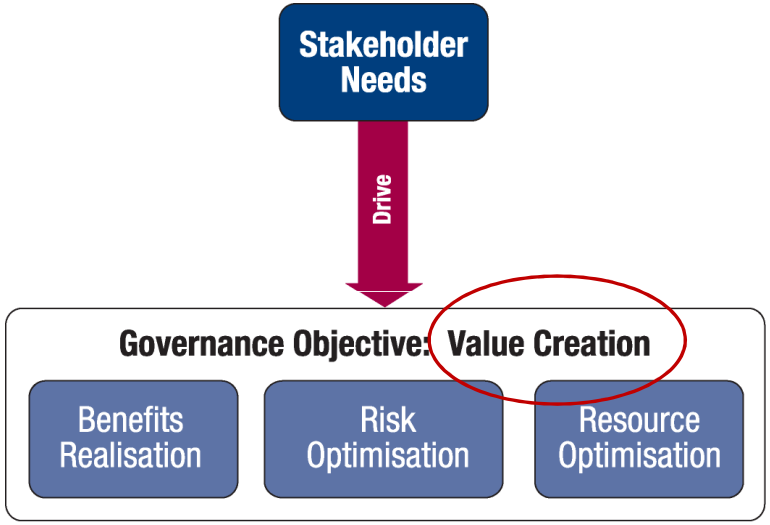
# 5 Principles

**Figure 2—COBIT 5 Principles**



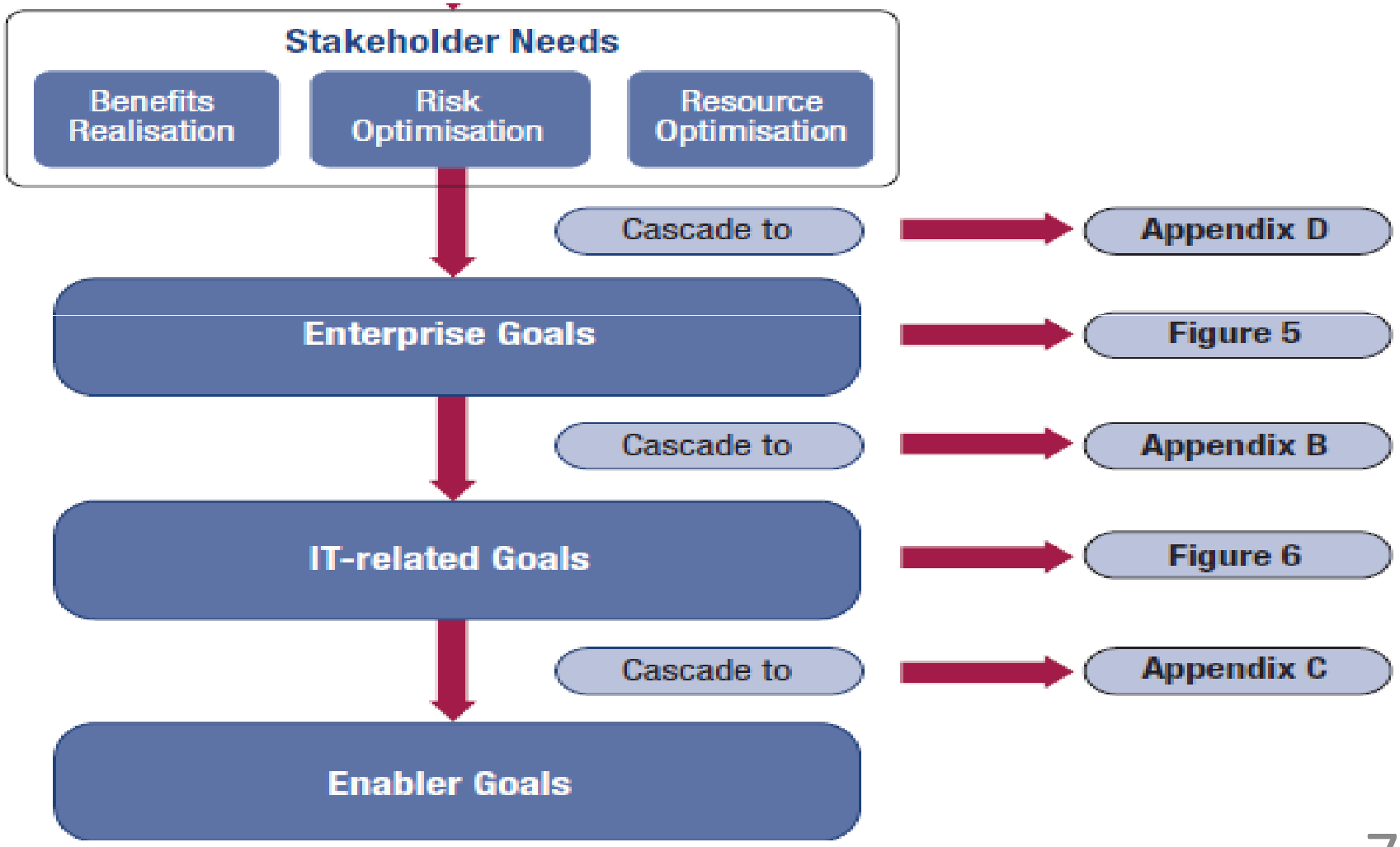
# Principle 1:
# Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders




- **Value creation:** realizing benefits at an optimal resource cost while optimizing risk.

# Principle-1


Stakeholder Needs
Benefits Realisation
Risk Optimisation
Resource Optimisation
Cascade to
Appendix D
Enterprise Goals
Figure 5
Cascade to
Appendix B
IT-related Goals
Figure 6
Cascade to
Appendix C
Enabler Goals

# Matrix

- Stakeholder needs  in the form of qustionnaires-24
  - Appendix D 24 by 17 Matrix
- Enterprise Goals-17
- IT Goals -17
  - Appendix  B 17 by 17 Matrix
- Enabler Goals-37
  - Appendix C 37 by 17 Matrix

# Principle 1 – Cascade Steps

**Step 3 - Enterprise Goals cascade to IT related Goals**

There are also 17 generic IT related goals as shown in Figure 6 (shown below) that are also categorised into the Balanced Score Card (BSC) categories. The relationship of enterprise goals to IT related Goals are shown in Appendix B Figure 22 page 50

**Figure 6—IT-related Goals**

| IT BSC Dimension | Information and Related Technology Goal | |
|---|---|---|
| Financial | 01 | Alignment of IT and business strategy |
| | 02 | IT compliance and support for business compliance with external laws and regulations |
| | 03 | Commitment of executive management for making IT-related decisions |
| | 04 | Managed IT-related business risk |
| | 05 | Realised benefits from IT-enabled investments and services portfolio |
| | 06 | Transparency of IT costs, benefits and risk |
| Customer | 07 | Delivery of IT services in line with business requirements |
| | 08 | Adequate use of applications, information and technology solutions |
| Internal | 09 | IT agility |
| | 10 | Security of information, processing infrastructure and applications |
| | 11 | Optimisation of IT assets, resources and capabilities |
| | 12 | Enablement and support of business processes by integrating applications and technology into business processes |
| | 13 | Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards |
| | 14 | Availability of reliable and useful information for decision making |
| | 15 | IT compliance with internal policies |
| Learning and Growth | 16 | Competent and motivated business and IT personnel |
| | 17 | Knowledge, expertise and initiatives for business innovation |

# Fig-5

| Figure 5—COBIT 5 Enterprise Goals | | | | |
|---|---|---|---|---|
| | | Relation to Governance Objectives | | |
| BSC Dimension | Enterprise Goal | Benefits Realisation | Risk Optimisation | Resource Optimisation |
| Financial | 1. Stakeholder value of business investments | P | | S |
| | 2. Portfolio of competitive products and services | P | P | S |
| | 3. Managed business risk (safeguarding of assets) | | P | S |
| | 4. Compliance with external laws and regulations | | P | |
| | 5. Financial transparency | P | S | S |
| Customer | 6. Customer-oriented service culture | P | | S |
| | 7. Business service continuity and availability | | P | |
| | 8. Agile responses to a changing business environment | P | | S |
| | 9. Information-based strategic decision making | P | P | P |
| | 10. Optimisation of service delivery costs | P | | P |
| Internal | 11. Optimisation of business process functionality | P | | P |
| | 12. Optimisation of business process costs | P | | P |
| | 13. Managed business change programmes | P | P | S |
| | 14. Operational and staff productivity | P | | P |
| | 15. Compliance with internal policies | | P | |
| Learning and Growth | 16. Skilled and motivated people | S | P | P |
| | 17. Product and business innovation culture | P | | |

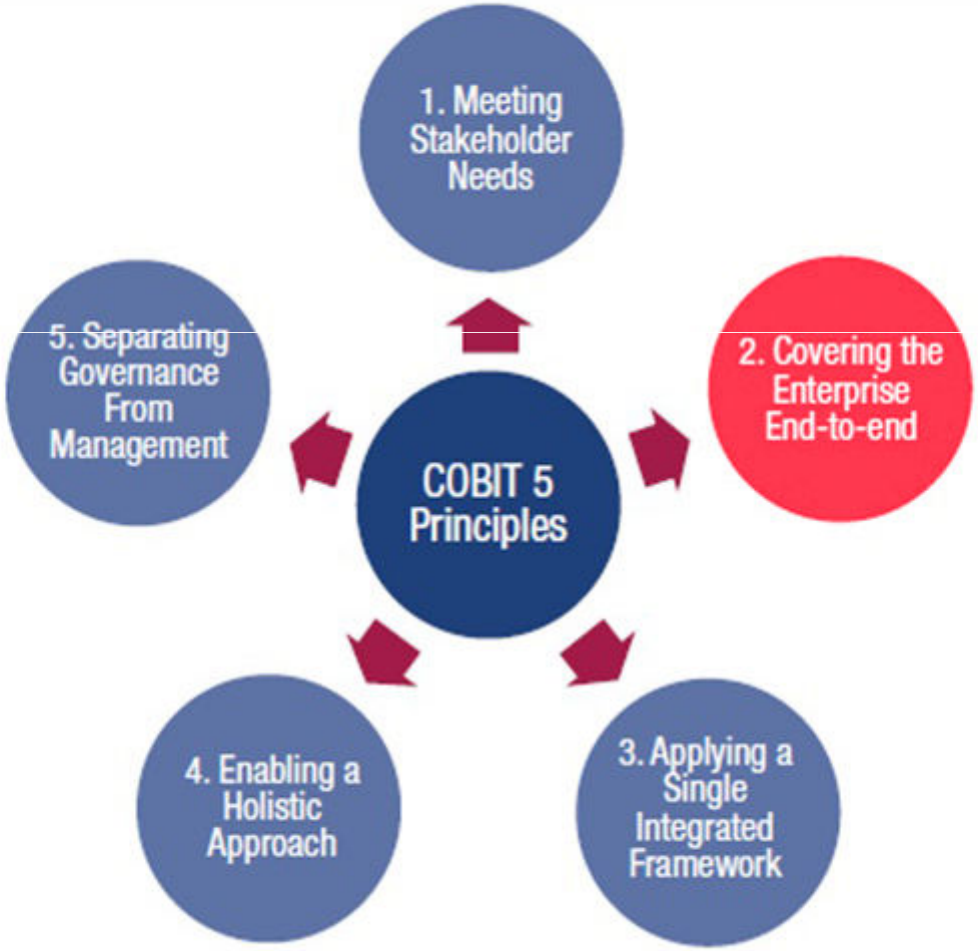
# Appendix C

**Figure 23—Mapping COBIT 5 IT-related Goals to Processes**

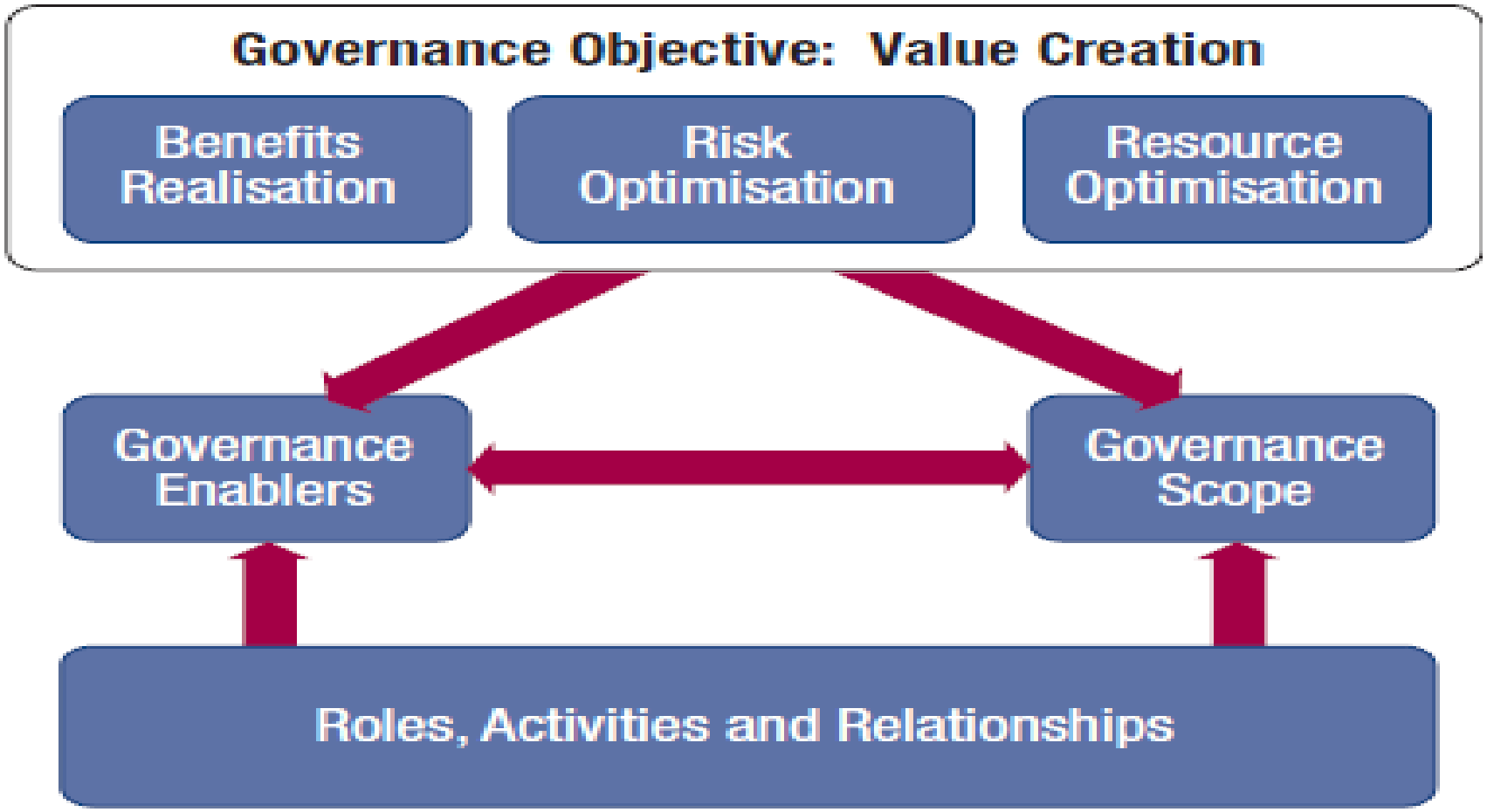
| | | | IT-related Goal | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Alignment of IT and business strategy | IT compliance and support for business compliance with external laws and regulations | Commitment of executive management for making IT-related decisions | Managed IT-related business risk | Realised benefits from IT-enabled investments and services portfolio | Transparency of IT costs, benefits and risk | Delivery of IT services in line with business requirements | Adequate use of applications, information and technology solutions | IT agility | Security of information, processing infrastructure and applications | Optimisation of IT assets, resources and capabilities | Enablement and support of business processes by integrating applications and technology into business processes | Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards | Availability of reliable and useful information for decision making | IT compliance with internal policies | Competent and motivated business and IT personnel | Knowledge, expertise and initiatives for business innovation |
| | | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| | COBIT 5 Process | | Financial | | | | | | Customer | | Internal | | | | | | | Learning and Growth | |
| Direct and Monitor | EDM01 | Ensure Governance Framework Setting and Maintenance | P | S | P | S | S | S | P | | S | S | S | S | S | S | S | S | S |
| | EDM02 | Ensure Benefits Delivery | P | | S | | P | P | P | S | | | S | S | S | S | | S | P |
| | EDM03 | Ensure Risk Optimisation | S | S | S | P | | P | S | S | | P | | | S | S | P | S | S |
| | EDM04 | Ensure Resource | | | | | | | | | | | | | | | | | |

# Prin-2

**Figure 2—COBIT 5 Principles**

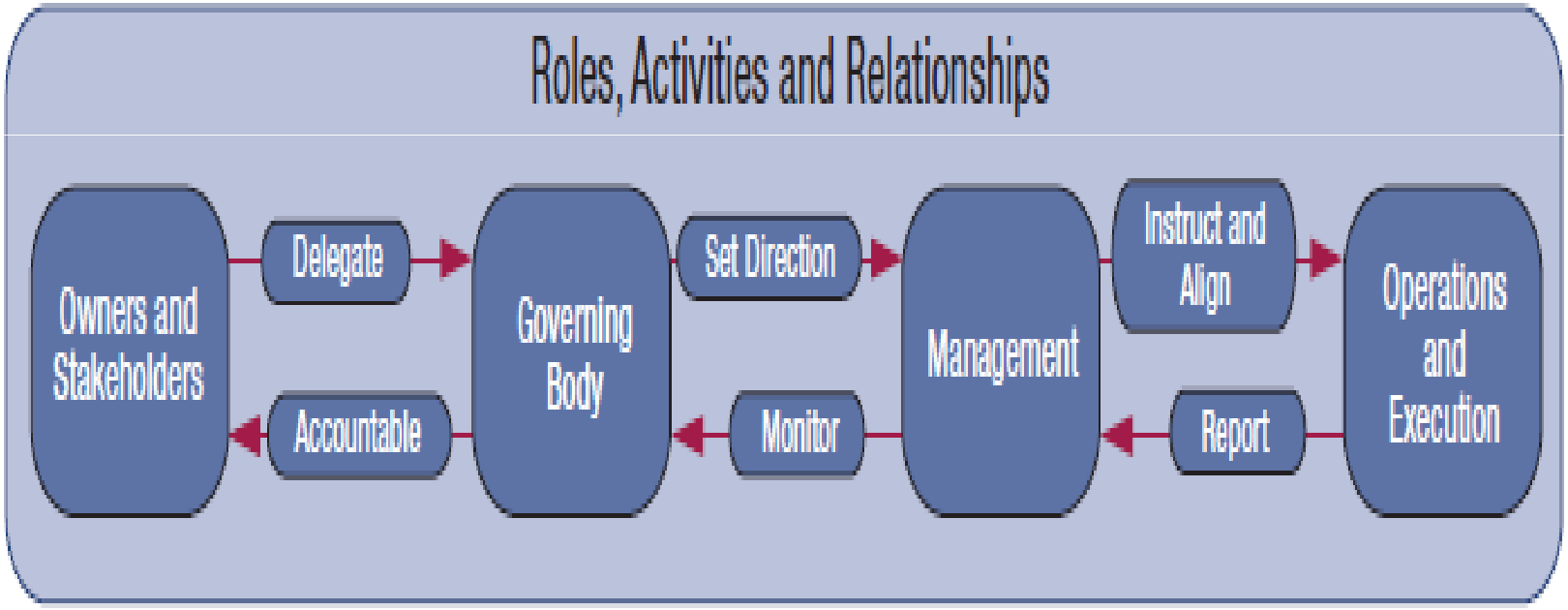


# Principle-2


Governance Objective: Value Creation
Benefits Realisation
Risk Optimisation
Resource Optimisation
Governance Enablers
Governance Scope
Roles, Activities and Relationships

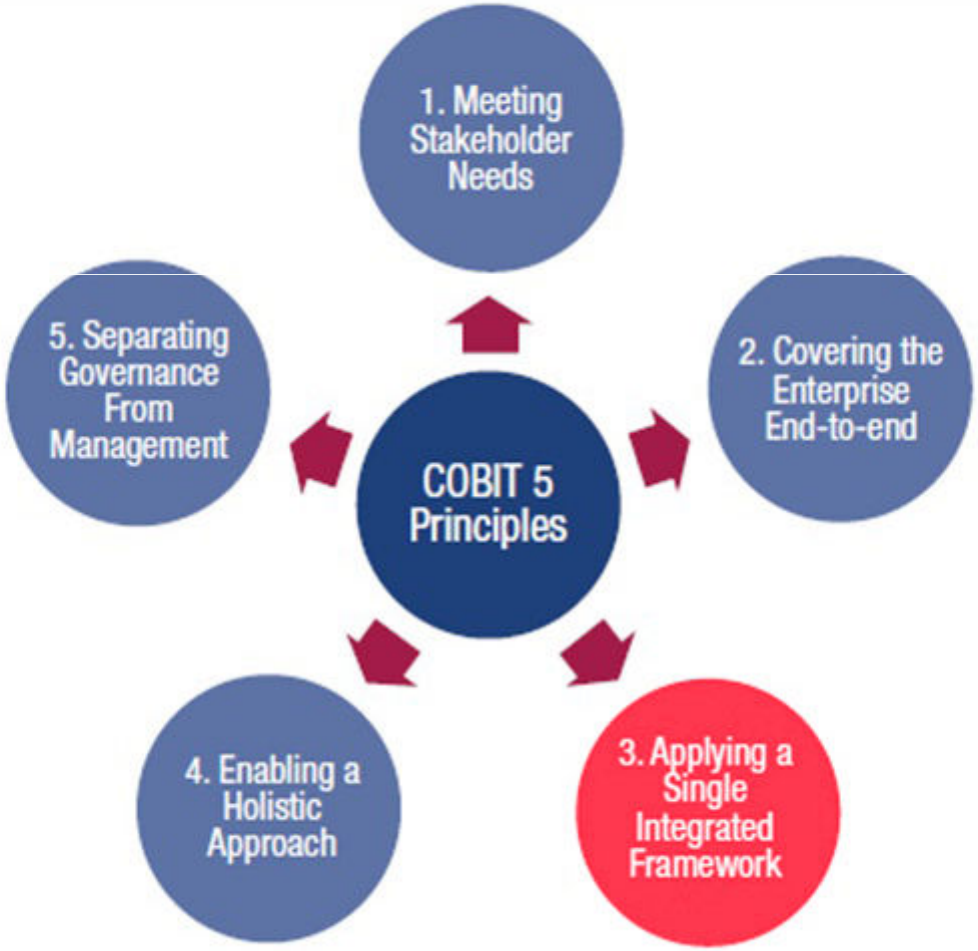
# Role etc

Figure 9—Key Roles, Activities and Relationships



# Prin-3

**Figure 2—COBIT 5 Principles**



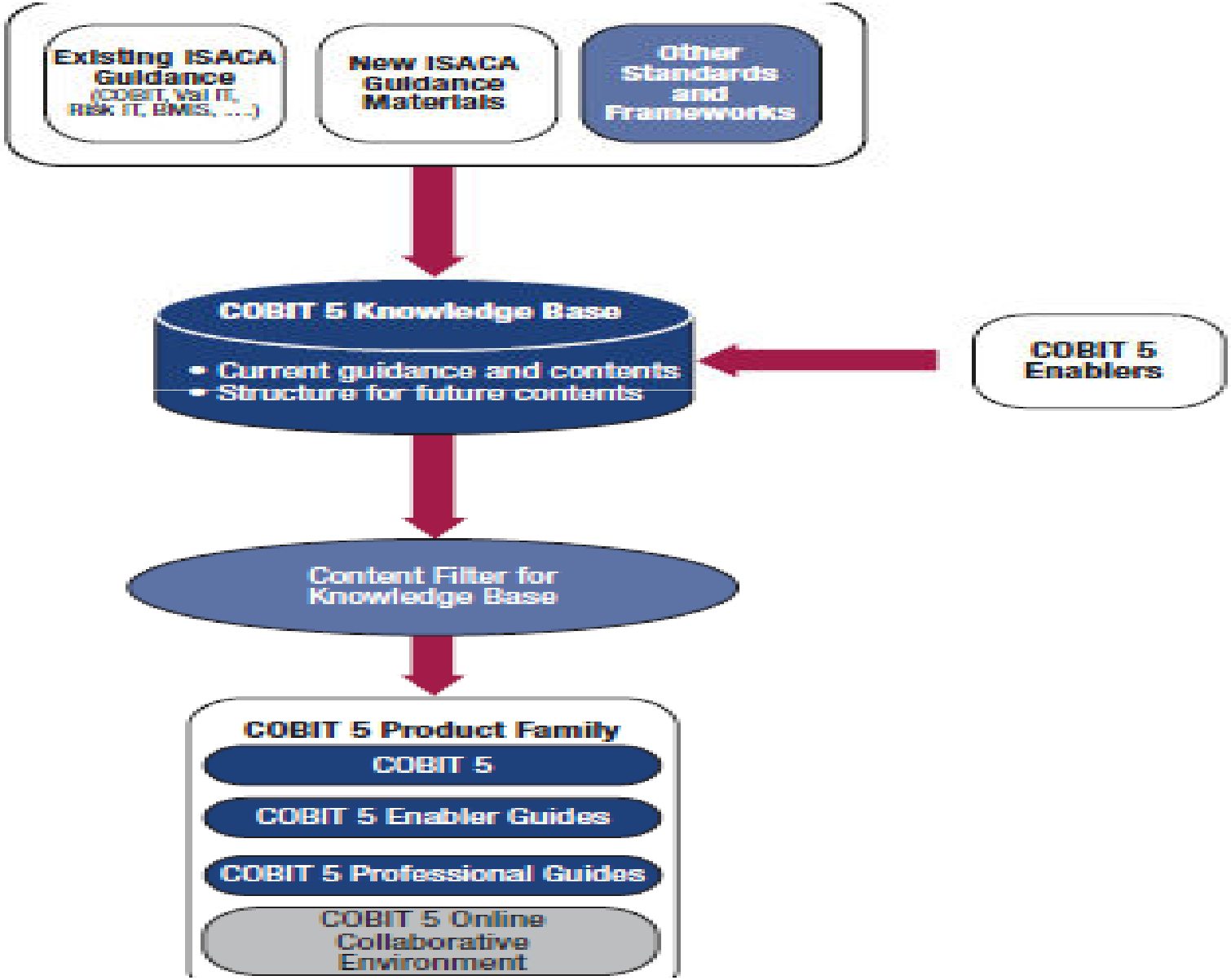
# Principle-3

- Applying a Single, Integrated Framework
- There are many IT-related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.

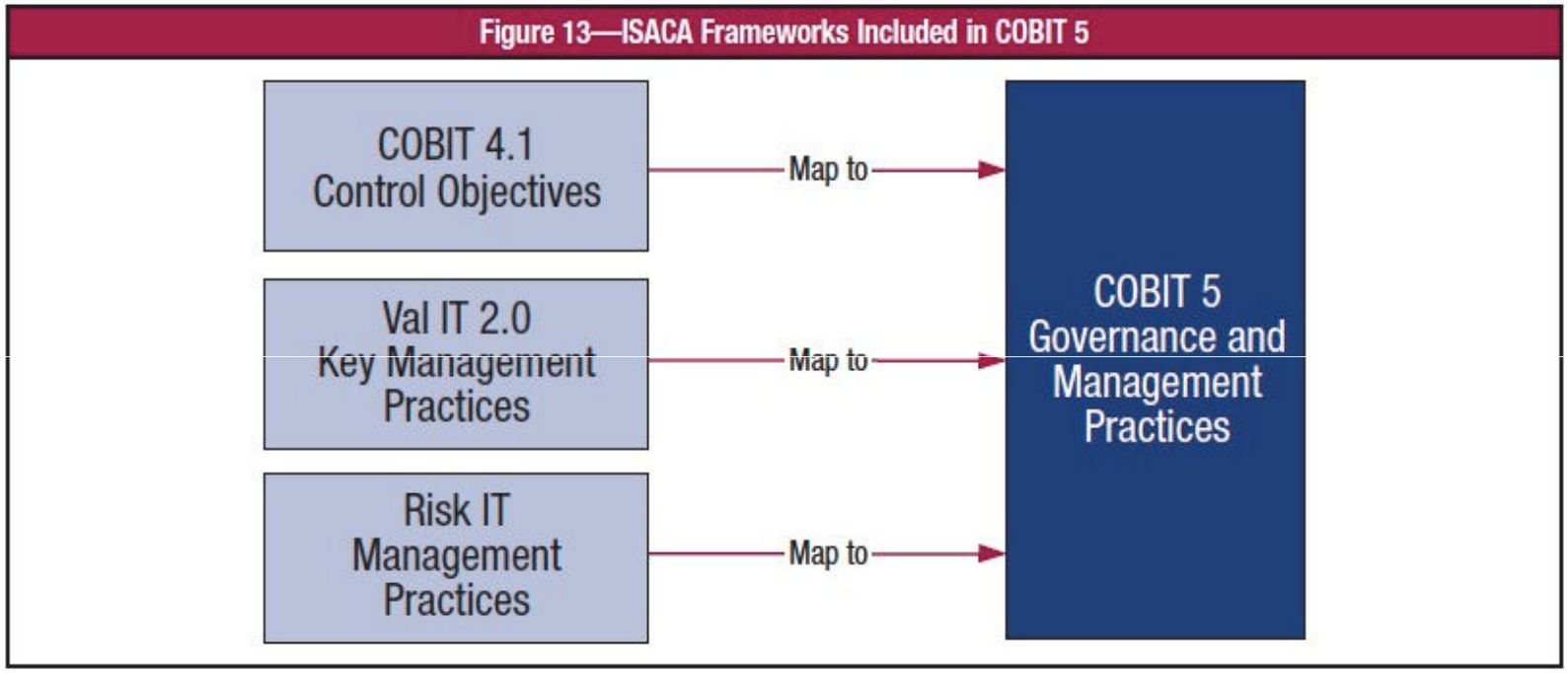
## Principle 3:
## Applying a Single Integrated Framework

- **COBIT 5:**
  - Aligns with the latest relevant standards and frameworks
  - Is complete in enterprise coverage
  - Provides a basis to integrate effectively other frameworks, standards and practices used
  - Integrates all knowledge previously dispersed over different ISACA frameworks
  - Provides a simple architecture for structuring guidance materials and producing a consistent product set

# Framework


Existing ISACA Guidance
(COBIT, Val IT, Risk IT, BMIS, ...)
New ISACA Guidance Materials
Other Standards and Frameworks
COBIT 5 Knowledge Base
• Current guidance and contents
• Structure for future contents
COBIT 5 Enablers
Content Filter for Knowledge Base
COBIT 5 Product Family
COBIT 5
COBIT 5 Enabler Guides
COBIT 5 Professional Guides
COBIT 5 Online Collaborative Environment

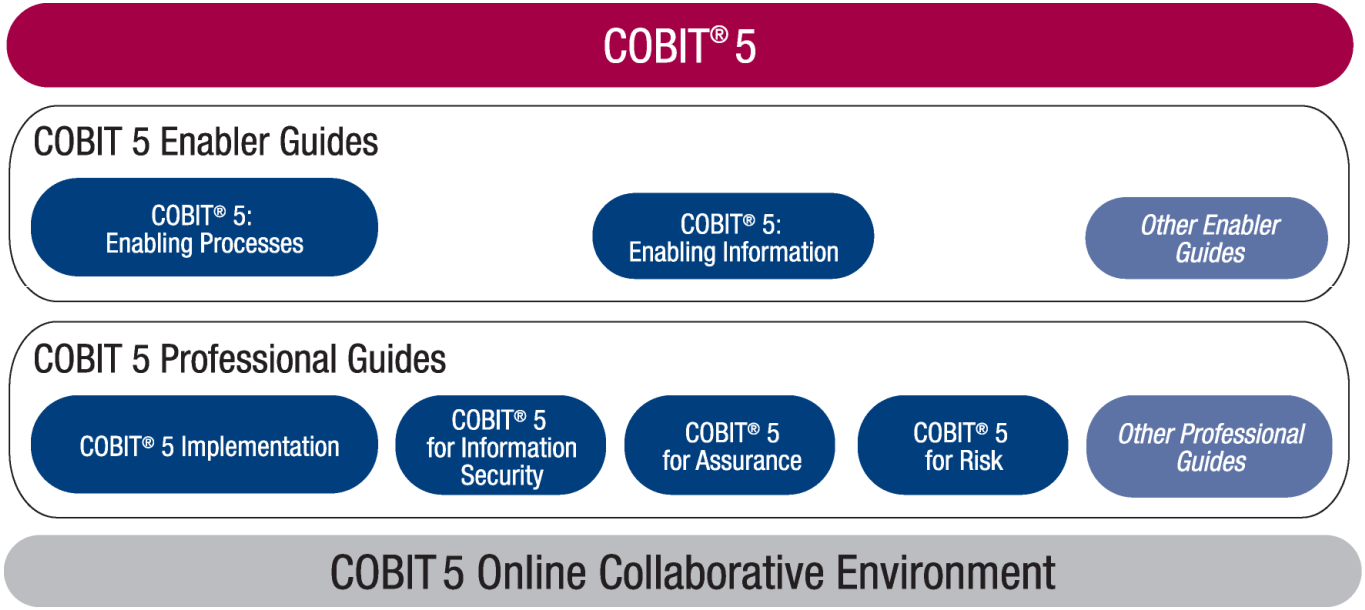
# COBIT 5 and Legacy ISACA Frameworks



## Principle 3:
## Applying a Single Integrated Framework

- The **COBIT 5** product family is the connection:
  - *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*
  - *COBIT 5: Enabling Processes*
  - *COBIT 5 Implementation Guide*
  - COBIT 5 for Information Security
  - COBIT 5 for Assurance
  - COBIT 5 for Risk
  - A series of other products is planned; they will be tailored for specific audiences or topics
  - COBIT 5 Online
- The perspective concept links the above to external sources for standards

# COBIT 5 Product Family



# Prin-4

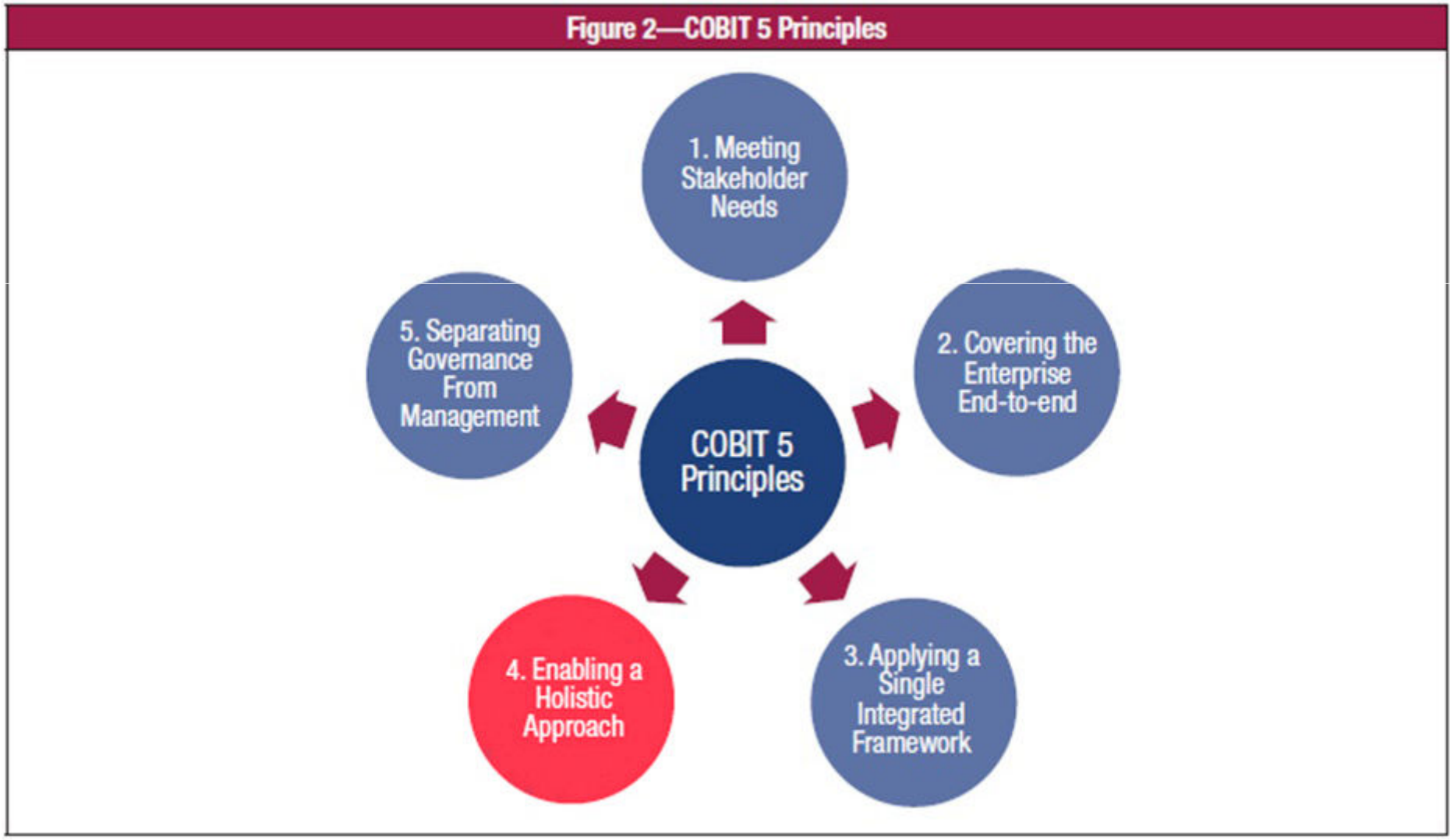


Figure 2—COBIT 5 Principles
1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

# Principle 4:
# Enabling a Holistic Approach

***COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.***

**COBIT 5 enablers are:**

- Factors that, individually and collectively, influence whether something will work
- Driven by the **goals cascade**
- Described by the COBIT 5 framework in **seven categories**

# Principle-4

- Enabling a Holistic Approach—

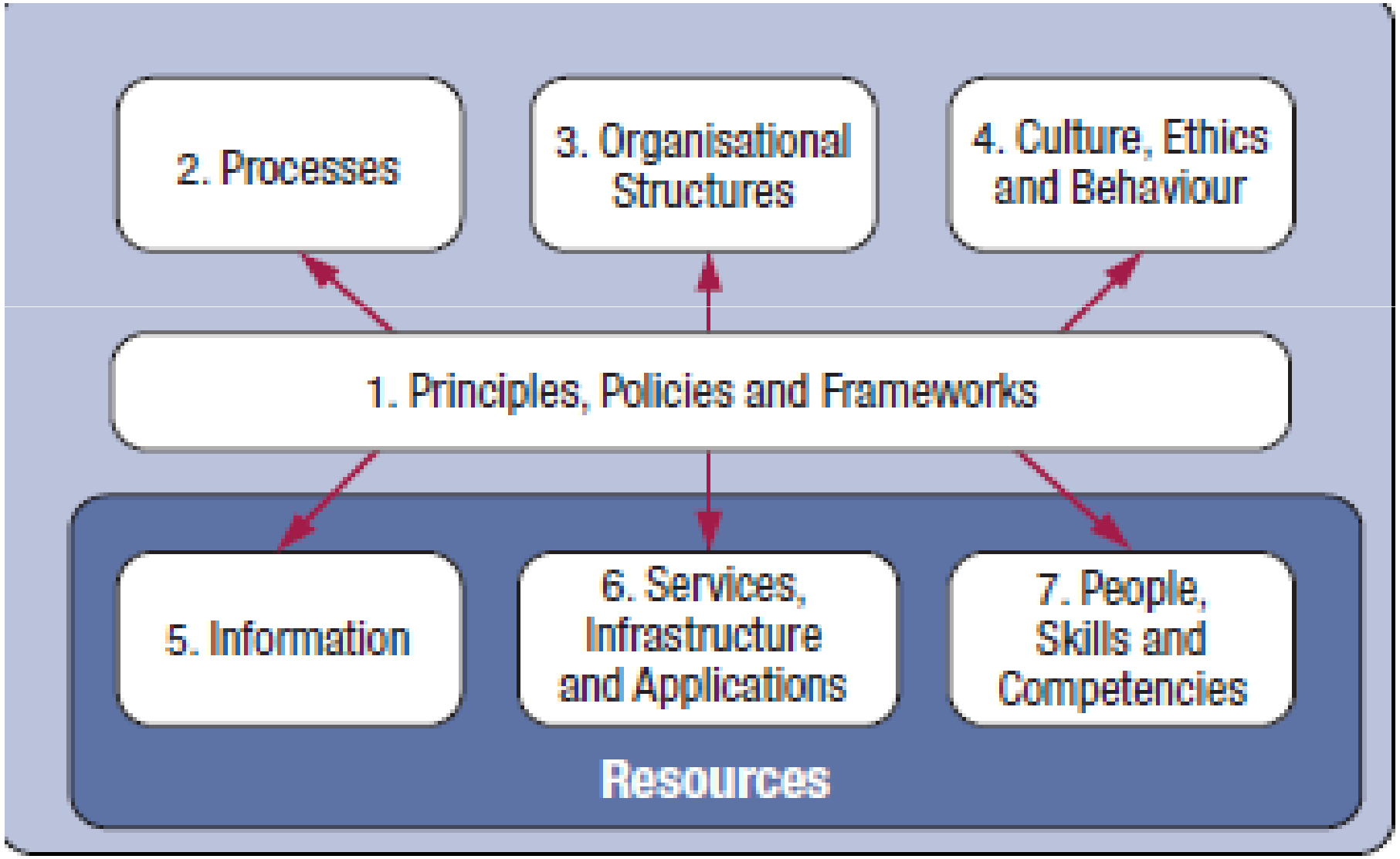
Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise

# Prin-4 contd

- Seven categories of enablers:
  - Principles, Policies and Frameworks
  - Processes
  - Organisational Structures
  - Culture, Ethics and Behaviour
  - Information
  - Services, Infrastructure and Applications
  - People, Skills and Competencies

# Principle-4


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

# Holistic Approach

- Jumbo Bank, New York, USA
  Requirement gathering session – Day 12
  Client: “Our next requirement, this is something big, you know, we need an elephant…”
  Ram: Mr. Richard but why don’t you adjust with a buffalo, even it is big…. and black?”
  C: No Ramasamy, we need only elephant, let me explain our current process……” (client explains for an hour)

# Holistic Approach

- R: Fine Richard, i understand ur requirement. But ours supports only buffalo…
- C: Samy..our central bank regulations needs only elephant!
  R: Ok.. Let me see if i can customize”
  Requirement taken : Bank wants a big black four legged animal, long tail, less hair. Having trunk is mandatory. The same was documented, signed off and sent to offshore for development!

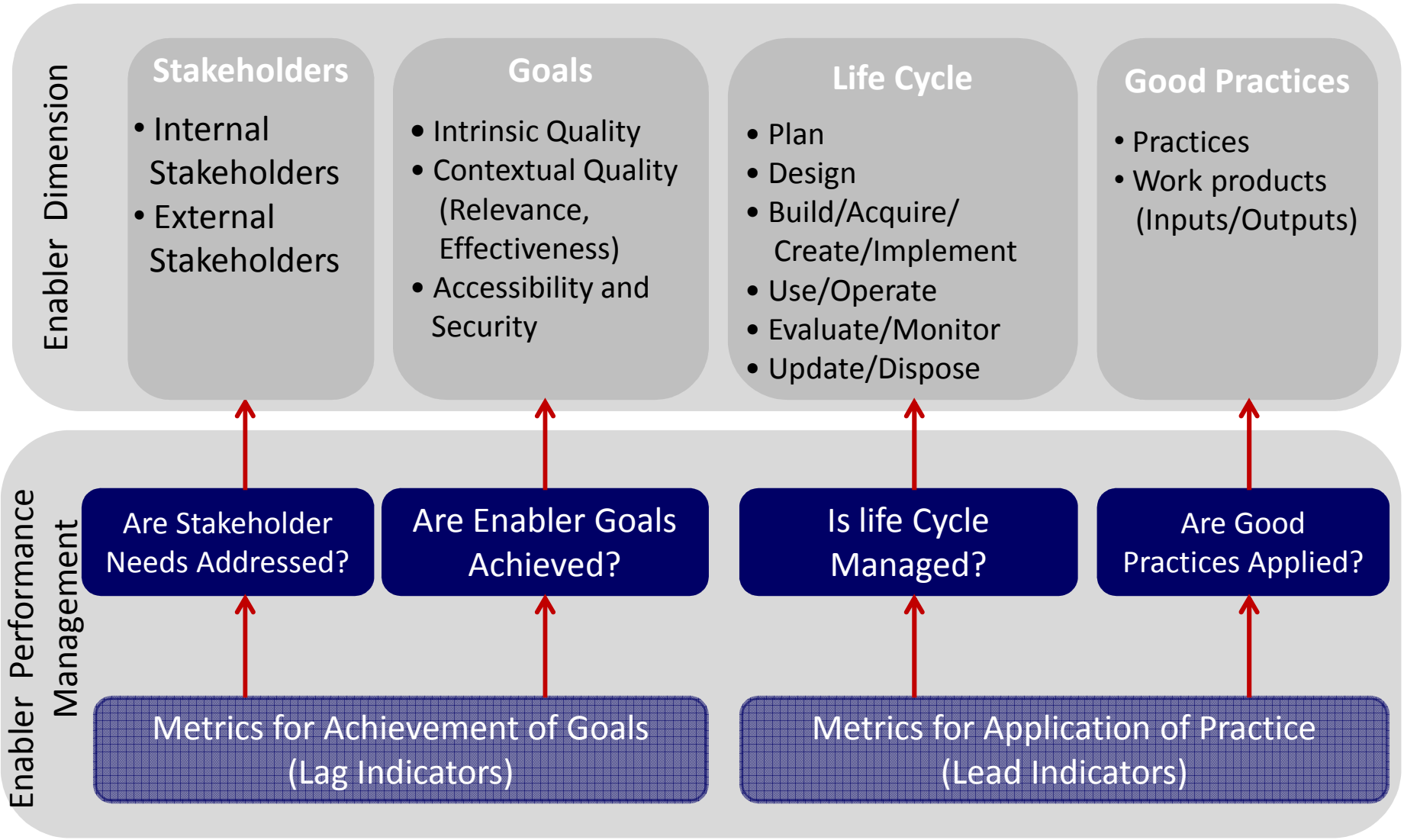
# Holistic Approach

- Design/Development – Base on requirement all features are supported in base product (as buffalo) , for trunk alone a separate customization is done.

  Finally the customization is shown to client

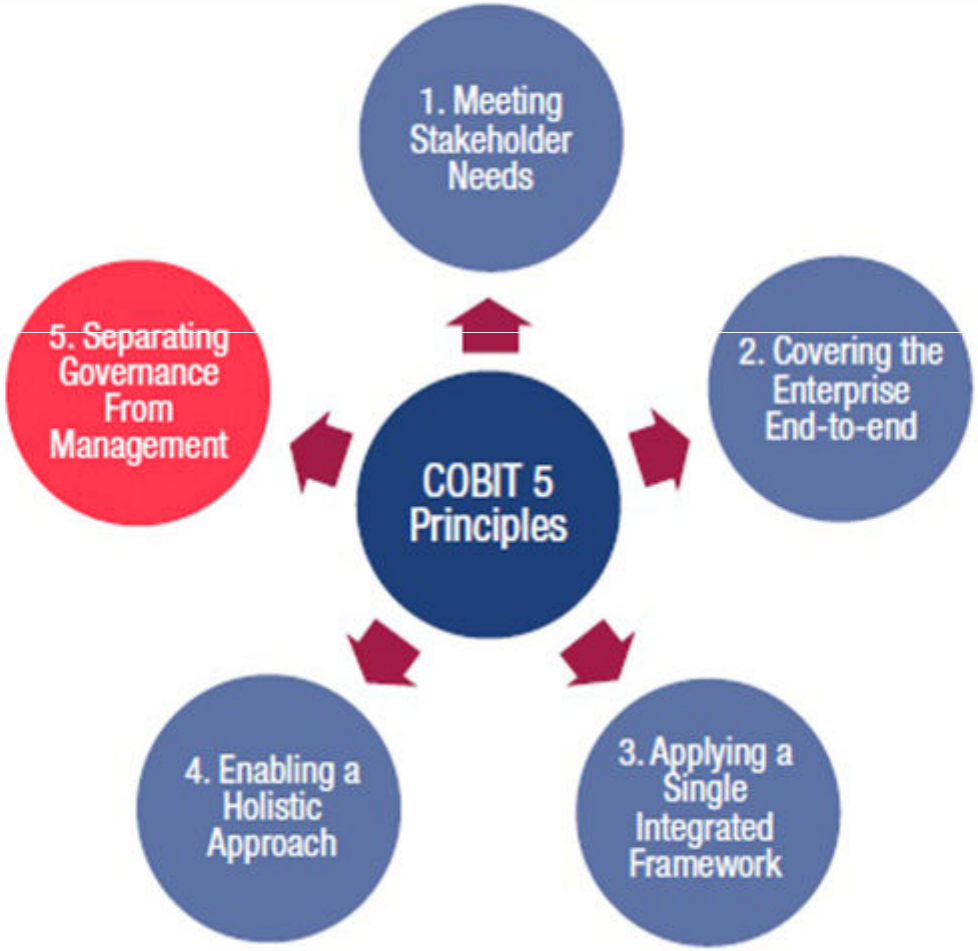
# Holistic Approach

# The COBIT 5 Generic Enabler Model



# Prin-5

**Figure 2—COBIT 5 Principles**



# Principle-5

- Separating Governance From Management—The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:

# Governance Defined

- The framework, principles and policies, structures, processes and practices, information, skills, culture, ethics, and behaviour to set direction and monitor compliance and performance of the enterprise aligned with the overall purpose and defined objectives. Governance defines accountability, responsibility and decision making (among other elements).

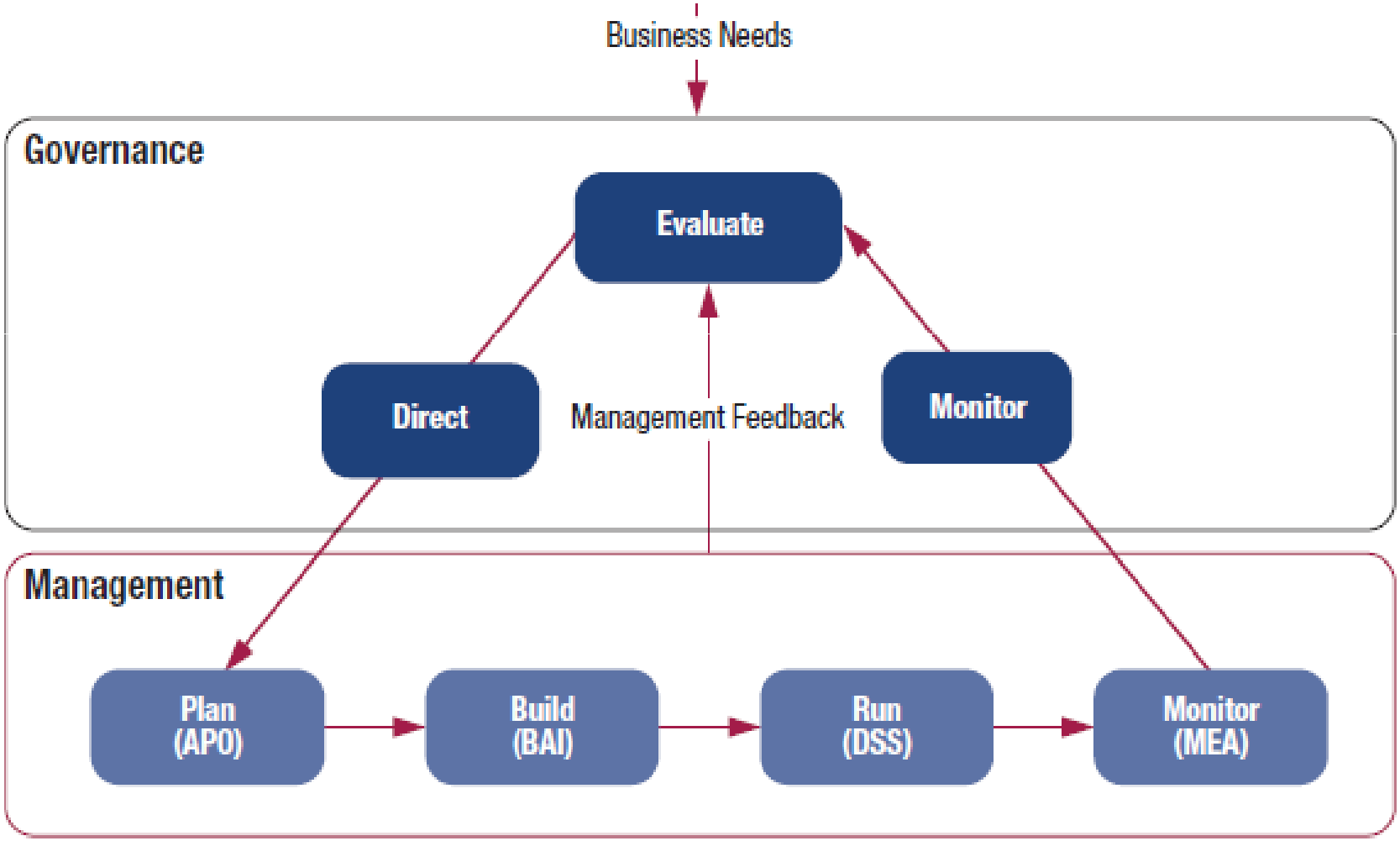
# Governance

- Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making ; and monitoring performance and compliance against agreed-on direction and objectives.

# Management

- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

# Principle 5


Business Needs
Governance
Evaluate
Direct
Management Feedback
Monitor
Management
Plan
(APO)
Build
(BAI)
Run
(DSS)
Monitor
(MEA)

## Processes for Governance of Enterprise IT

### Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency

### Align, Plan and Organise

APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security

### Build, Acquire and Implement

BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration

### Deliver, Service and Support

DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls

### Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

**Processes for Management of Enterprise IT**

# Process Template

| Process Name | Area:<br>Domain: |
|---|---|
| **Process Description** | |
| **Process Purpose Statement** | |
| **The process supports the achievement of a set of primary IT-related goals:** | |
| **IT-related Goal** | **Related Metrics** |
| | |
| **Process Goals and Metrics** | |
| **Process Goal** | **Related Metrics** |
| | |
| **RACI Chart**: | |

| Management Practices | Inputs | | Outputs | |
|---|---|---|---|---|
| | From | Description | From | Description |
| | | | | |
| **Activities** | | | | |
| | | | | |

| Related Guidance | |
|---|---|
| **Related Standard** | **Detailed Reference** |
| | |

# Understanding Process-1

| EDM01 Ensure Governance Framework Setting and Maintenance | Area: Governance<br>Domain: Evaluate, Direct and Monitor |
|---|---|
| **Process Description**<br>Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. | |
| **Process Purpose Statement**<br>Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met. | |
| **The process supports the achievement of a set of primary IT-related goals:** | |
| **IT-related Goal** | **Related Metrics** |
| 01 Alignment of IT and business strategy | • Percent of enterprise strategic goals and requirements supported by IT strategic goals<br>• Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services<br>• Percent of IT value drivers mapped to business value drivers |

# Understanding Process-2

| Process Goals and Metrics | |
|---|---|
| **Process Goal** | **Related Metrics** |
| 1. Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements. | • Actual vs. target cycle time for key decisions<br>• Level of stakeholder satisfaction (measured through surveys) |
| 2. The governance system for IT is embedded in the enterprise. | • Number of roles, responsibilities and authorities that are defined, assigned and accepted by appropriate business and IT management<br>• Degree by which agreed-on governance principles for IT are evidenced in processes and practices (percentage of processes and practices with clear traceability to principles)<br>• Number of instances of non-compliance with ethical and professional behaviour guidelines |
| 3. Assurance is obtained that the governance system for IT is operating effectively. | • Frequency of independent reviews of governance of IT<br>• Frequency of governance of IT reporting to the executive committee and board<br>• Number of governance of IT issues reported |

# Understanding Process-3

**EDM01 RACI Chart**

| Key Governance Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **EDM01.01** Evaluate the governance system. | A | R | C | C | R | | R | | | | C | | C | C | C | C | C | R | C | C | C | | | | | |
| **EDM01.02** Direct the governance system. | A | R | C | C | R | I | R | I | I | I | C | I | I | I | I | C | C | R | C | I | I | I | I | I | I | I |
| **EDM01.03** Monitor the governance system. | A | R | C | C | R | I | R | I | I | I | C | I | I | I | I | C | C | R | C | I | I | I | I | I | I | I |

# Understanding Process-4

| EDM01 Process Practices, Inputs/Outputs and Activities | | | | |
|---|---|---|---|---|
| **Governance Practice** | **Inputs** | | **Outputs** | |
| **EDM01.01 Evaluate the governance system.** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make a judgement on the current and future design of governance of enterprise IT. | **From** | **Description** | **Description** | **To** |
| | MEA03.02 | Communications of changed compliance requirements | Enterprise governance guiding principles | All EDM<br>APO01.01<br>APO01.03 |
| | Outside COBIT | • Business environment trends<br>• Regulations<br>• Governance/decision-making model<br>• Constitution/bylaws/ statutes of organisation | Decision-making model | All EDM<br>APO01.01 |
| | | | Authority levels | All EDM<br>APO01.02 |
| **Activities** | | | | |
| 1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design. | | | | |
| 2. Determine the significance of IT and its role with respect to the business. | | | | |
| 3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT. | | | | |

# Understanding Process-5

| EDM01 Related Guidance | |
|---|---|
| **Related Standard** | **Detailed Reference** |
| Committee of Sponsoring Organizations of the Treadway Commission (COSO) | |
| ISO/IEC 38500 | |
| King III | • 5.1. The board should be responsible for information technology (IT) governance.<br>• 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework. |
| Organisation for Economic Co-operation and Development (OECD) | Corporate Governance Principles |