COBIT® 5
AN ISACA® FRAMEWORK

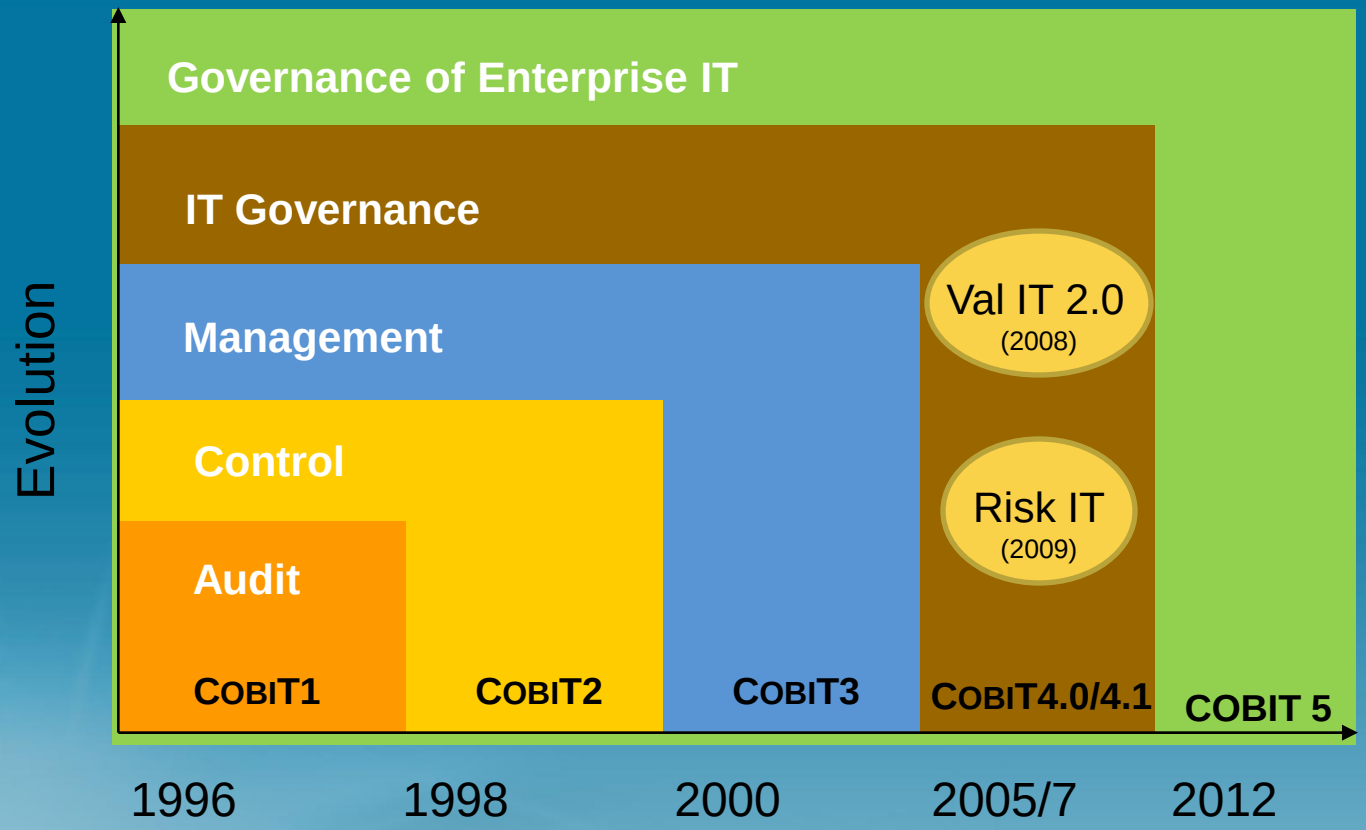
ISACA®
Trust in, and value from, information systems

COBIT 5

For Governance & Management of the Enterprise's Information & Technology

John Lainhart, CGEIT, CISA, CISM, CRISC, CIPP/G, CIPP/US
Partner
IBM Global Business Services
US Public Sector Cybersecurity & Privacy Service Area Leader
&
Chair COBIT 5 Online Task Force

COBIT: An IT Audit & Control Framework? – NOT ANY MORE!!



An business framework from ISACA, at www.isaca.org/cobit

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

COBIT 5
Executive Summary

Information!

- 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 does information and technology bring to enterprises?

Enterprise Benefits

Enterprises and their executives strive to:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- 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 realised to create enterprise stakeholder value?

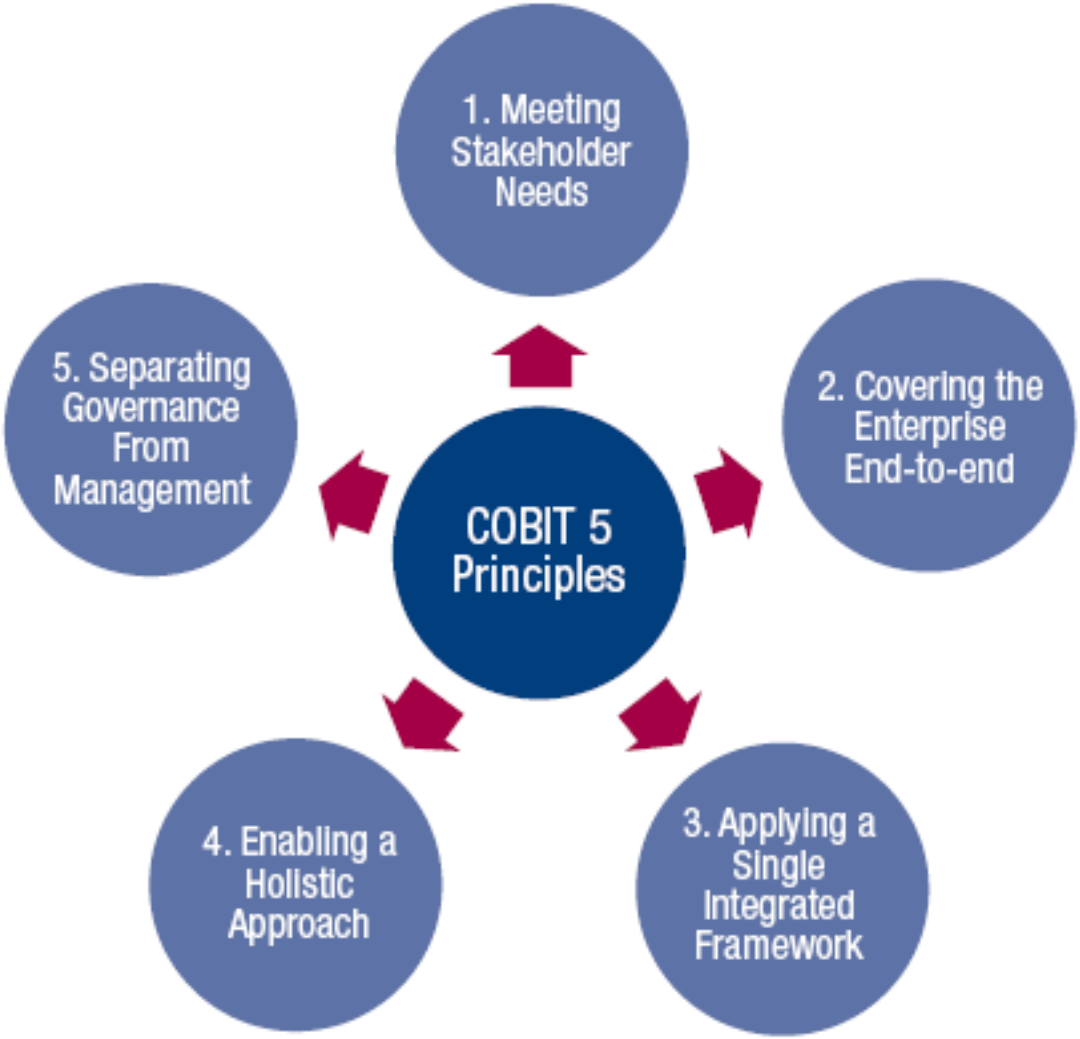
Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Enterprise boards, executives and management must **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.
- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.**

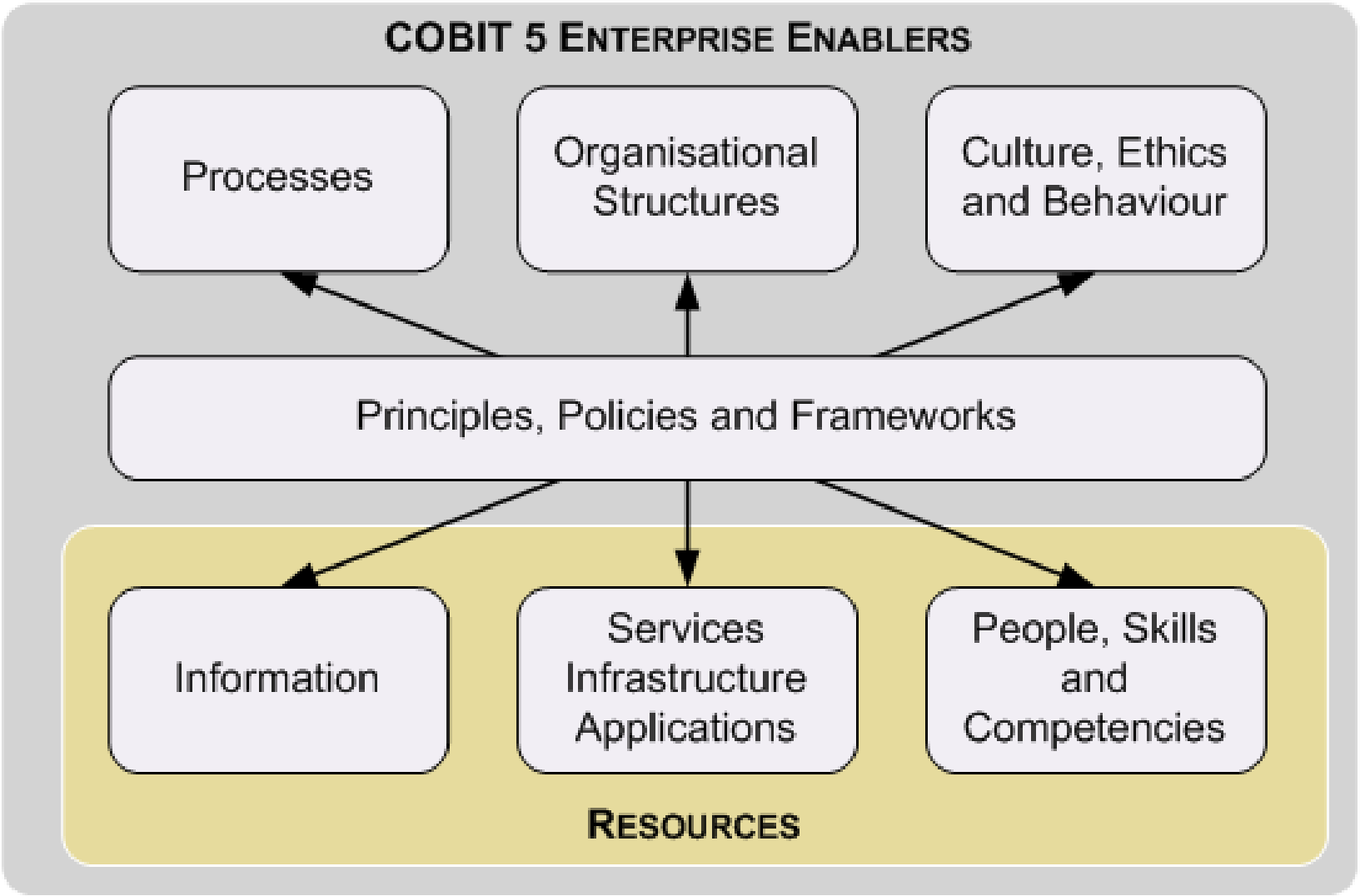
The COBIT 5 Framework

- Simply stated, COBIT 5 helps enterprises to 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 whole 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.

COBIT 5 Principles



COBIT 5 enablers



Governance and Management

- **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 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)**

In summary ….

COBIT 5 brings together the **five principles** that allow the enterprise to build an effective **governance** and **management** framework based on a holistic set of **seven enablers** that optimises **information** and **technology** investment and use for the benefit of stakeholders.

COBIT® 5
AN ISACA® FRAMEWORK

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

COBIT 5

COBIT 5 Framework

COBIT 5 Framework:

- The main, overarching COBIT 5 product.
- Contains the executive summary and the full description of all of the COBIT 5 framework components:
  - **The five COBIT 5 principles**
  - **The seven COBIT 5 enablers** plus
  - An introduction to the implementation guidance provided by ISACA *(COBIT 5 Implementation)*
  - An introduction to the COBIT Assessment Programme *(not specific to COBIT 5)* and the process capability approach being adopted by ISACA for COBIT

Five COBIT 5 Principles

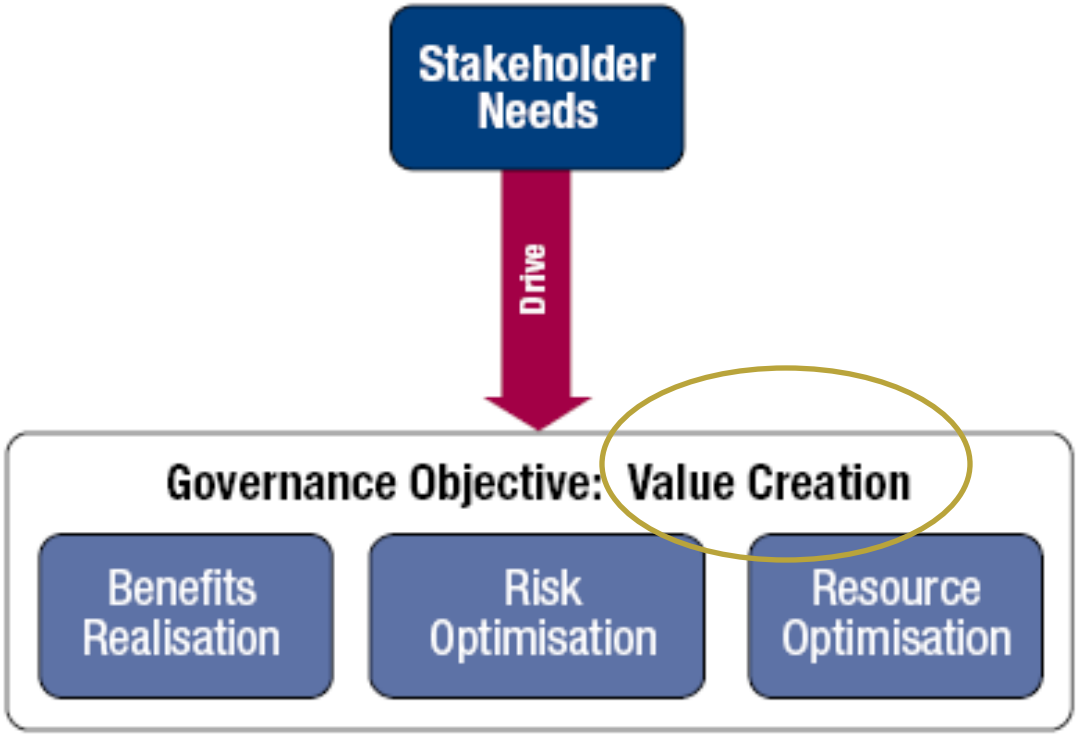
The five COBIT 5 principles:

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

1. Meeting Stakeholder Needs

Principle 1. Meeting Stakeholder Needs

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



1. Meeting Stakeholder Needs (cont.)

Principle 1. Meeting Stakeholder Needs

- 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:
  - For whom are the benefits?
  - Who bears the risk?
  - What resources are required?

1. Meeting Stakeholder Needs (cont.)

Principle 1. Meeting Stakeholder Needs

- Stakeholder needs have to be transformed into an enterprises' actionable strategy.
- The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals.

1. Meeting Stakeholder Needs (cont.)

Principle 1. Meeting Stakeholder Needs

Benefits of the COBIT 5 goals cascade:

- It allows the definition of priorities for implementation, improvement and assurance of enterprise governance of IT based on (strategic) objectives of the enterprise and the related risks.
- In practice, the goals cascade:
  - Defines relevant and tangible goals and objectives at various levels of responsibility.
  - Filters the knowledge base of COBIT 5, based on enterprise goals to extract relevant guidance for inclusion in specific implementation, improvement or assurance projects.
  - Clearly identifies and communicates how (sometimes very operational) enablers are important to achieve enterprise goals.

2. Covering the Enterprise End-to-End

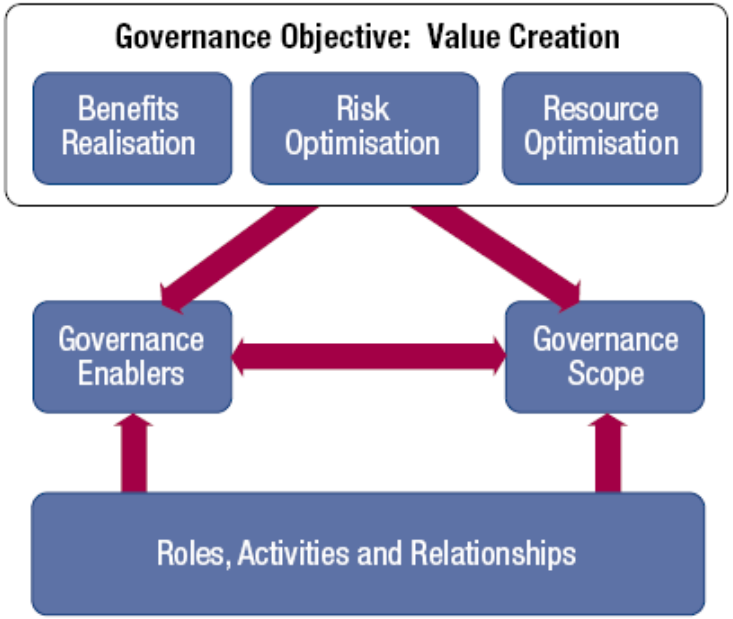
ISACA
Trust in, and value from, information systems

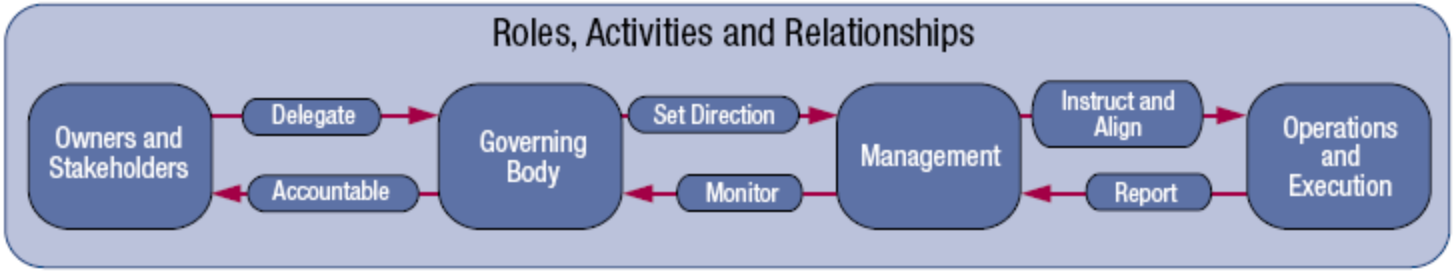
Principle 2. Covering the Enterprise End-to-End

- COBIT 5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective.
- This means that COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system, because COBIT 5 aligns with the latest views on governance.
  - Covers all functions and processes within the enterprise; **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 2. Covering the Enterprise End-to-End

Key components of a governance system





3. Applying a Single Integrated Framework

Principle 3. Applying a Single Integrated Framework

- COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:
  - Enterprise: COSO, COSO ERM, ISO 9000, ISO 31000
  - IT-related: ISO 38500, ITIL, ISO27000 series, TOGAF, PMBOK/PRINCE2, CMMI
  - Etc.
- This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
- ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.

4. Enabling a Holistic Approach

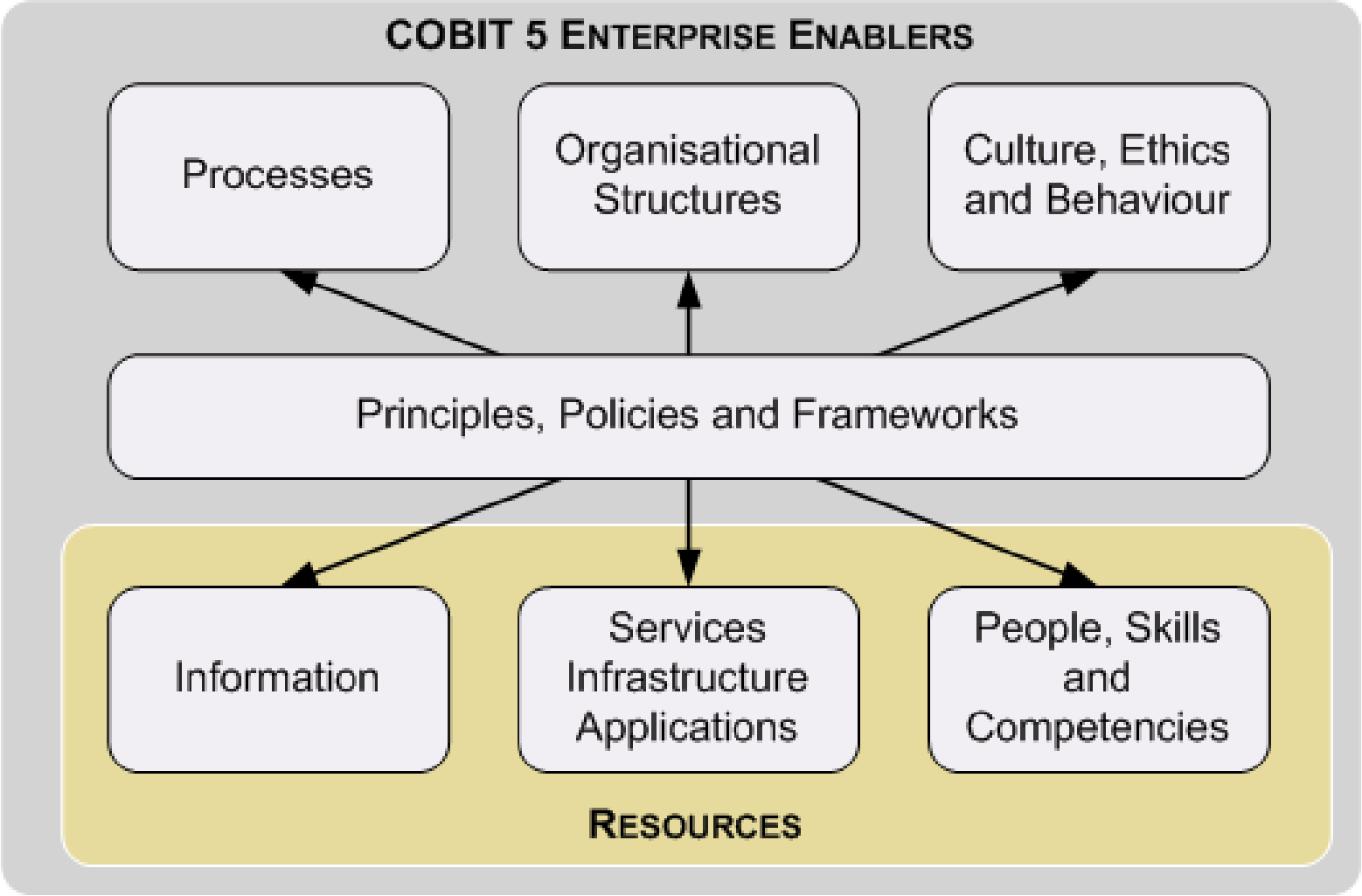
Principle 4. Enabling a Holistic Approach

COBIT 5 enablers are:

- Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT
- Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve
- Described by the COBIT 5 framework in **seven categories**

4. Enabling a Holistic Approach (Cont.)

Principle 4. Enabling a Holistic Approach



4. Enabling a Holistic Approach (Cont.)

Principle 4. Enabling a Holistic Approach

1. **Processes**—Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT related goals.
2. **Organisational structures**—Are the key decision-making entities in an organisation.
3. **Culture, ethics and behaviour**—Of individuals and of the organisation; very often underestimated as a success factor in governance and management activities.
4. **Principles, policies and frameworks**—Are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
5. **Information**—Is pervasive throughout any organisation, i.e., deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. **Services, infrastructure and applications**—Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. **People, skills and competencies**—Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

4. Enabling a Holistic Approach (Cont).

Principle 4. Enabling a Holistic Approach

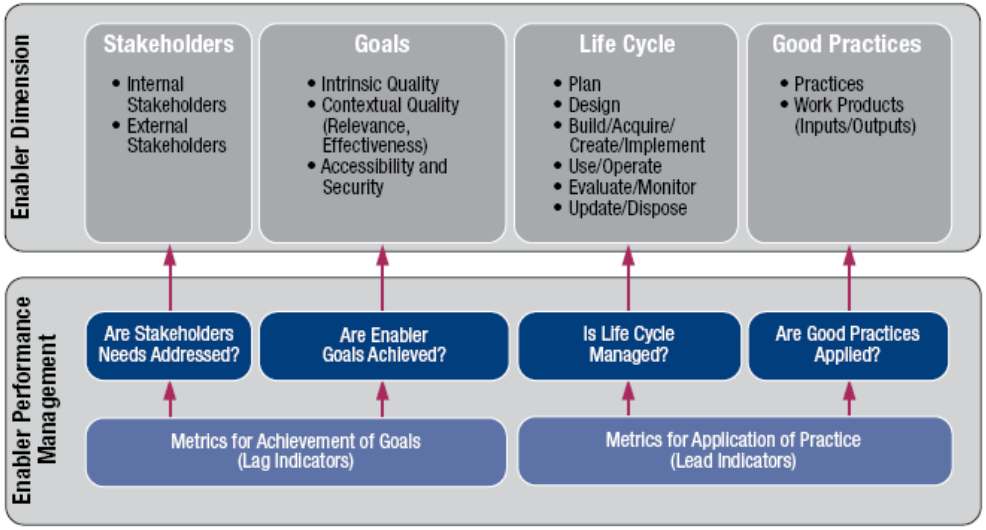
- **Systemic governance and management through interconnected enablers**—To achieve the main objectives of the enterprise, it must always consider an interconnected set of enablers, i.e., each enabler:
  - Needs the input of other enablers to be fully effective (e.g., processes need information, organisational structures need skills and behaviour)
  - Delivers output to the benefit of other enablers, e.g., processes deliver information, skills and behaviour make processes efficient
- This is a KEY principle emerging from the ISACA development work around the Business Model for Information Security (BMIS).

4. Enabling a Holistic Approach (Cont).

Principle 4. Enabling a Holistic Approach

COBIT 5 Enabler Dimensions

- All enablers have a set of common dimensions. This set of common dimensions:
  - Provides a common, simple and structured way to deal with enablers
  - Allows an entity to manage its complex interactions
  - Facilitates successful outcomes of the enablers



5. Separating Governance From Management

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
  - Serve different purposes
- **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.

5. Separating Governance From Management (Cont.)

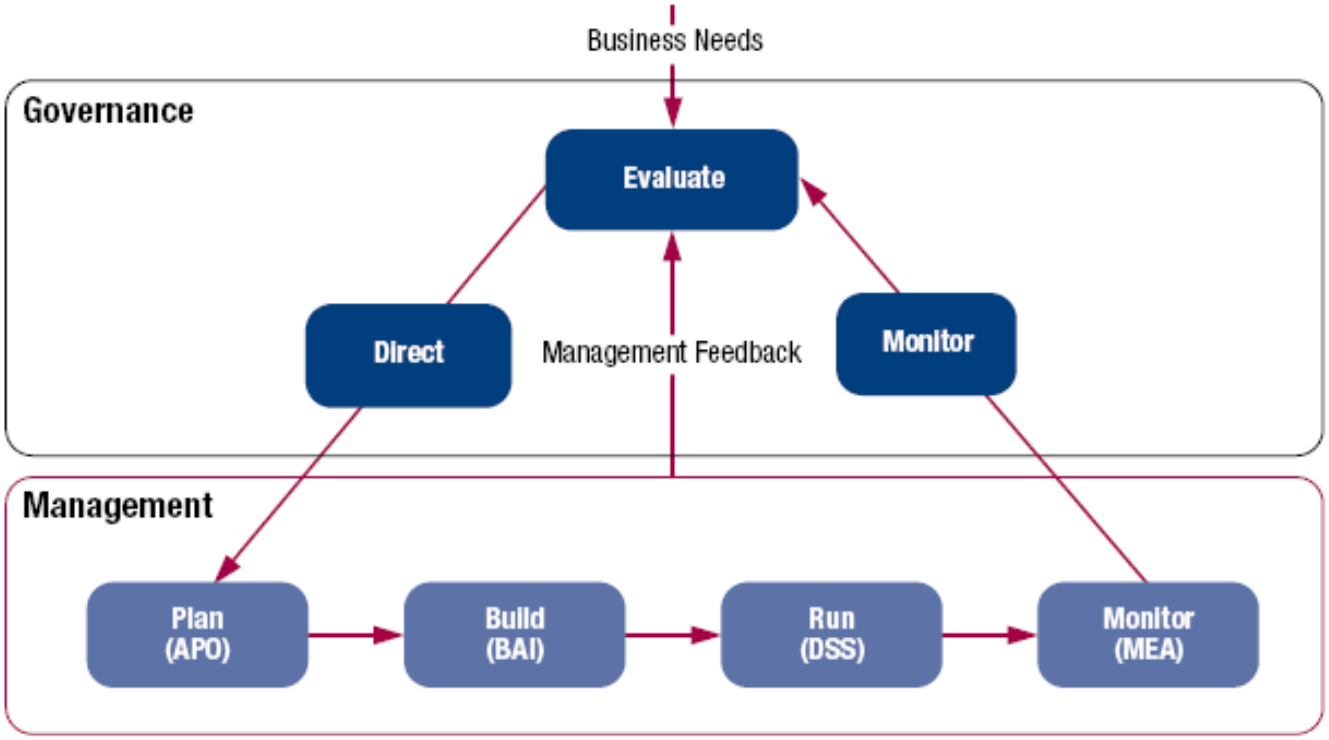
Principle 5. Separating Governance from Management

- **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 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)**

5. Separating Governance From Management (Cont.)

Principle 5. Separating Governance from Management

COBIT 5 is not prescriptive, but it advocates that organisations implement governance and management processes such that the key areas are covered, as shown.



5. Separating Governance From Management (Cont.)

Principle 5. Separating Governance from Management

- The COBIT 5 framework describes seven categories of enablers *(Principle 4).* Processes are one category.
- An enterprise can organise its processes as it sees fit, as long as all necessary governance and management objectives are covered. Smaller enterprises may have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.
- COBIT 5 includes a **process reference model (PRM)**, which defines and describes in detail a number of governance and management processes. The details of this specific enabler model can be found in the *COBIT 5 Enablers: Processes* volume.

COBIT 5
AN ISACA® FRAMEWORK

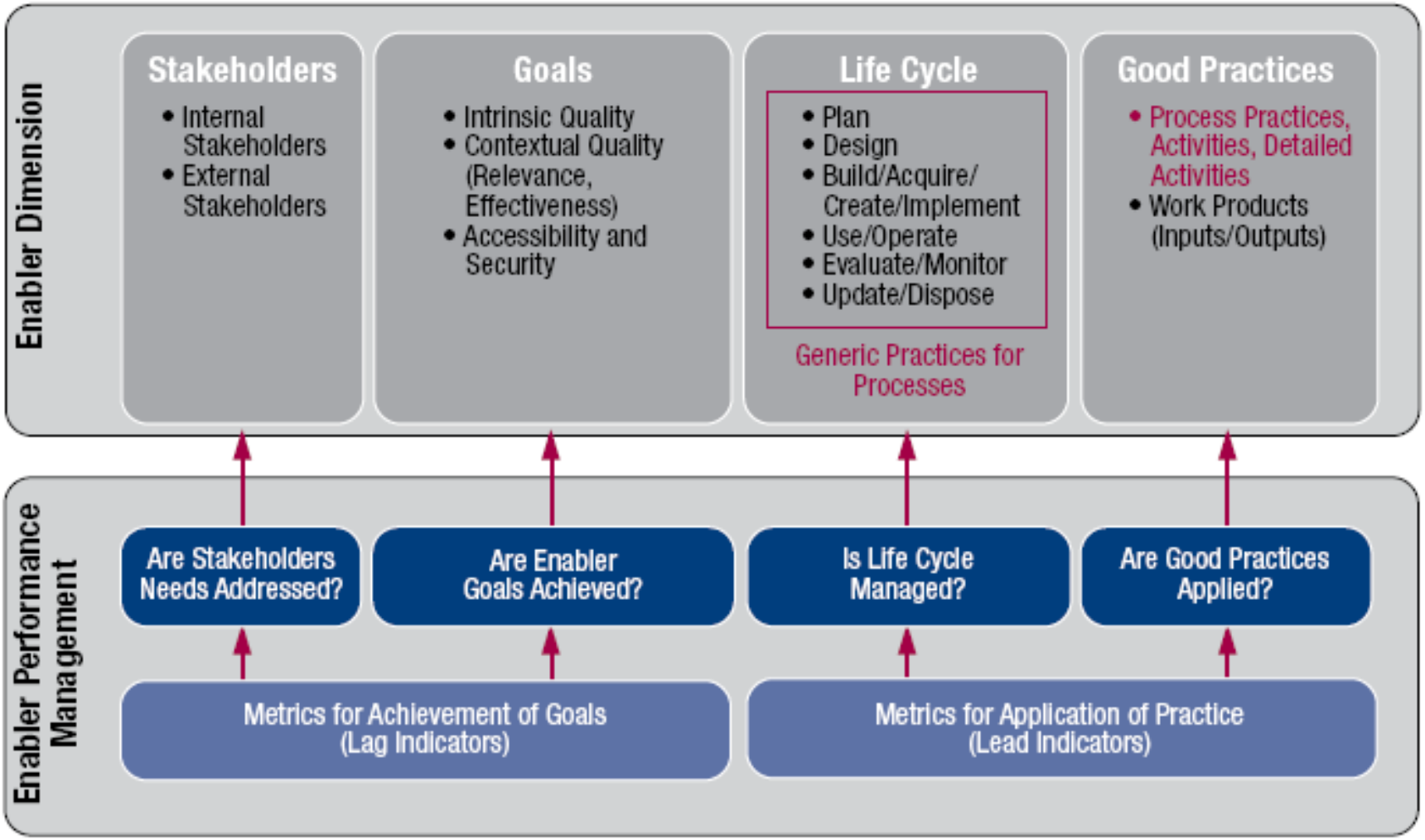
ISACA®
Trust in, and value from, information systems

COBIT 5 Enablers: Processes

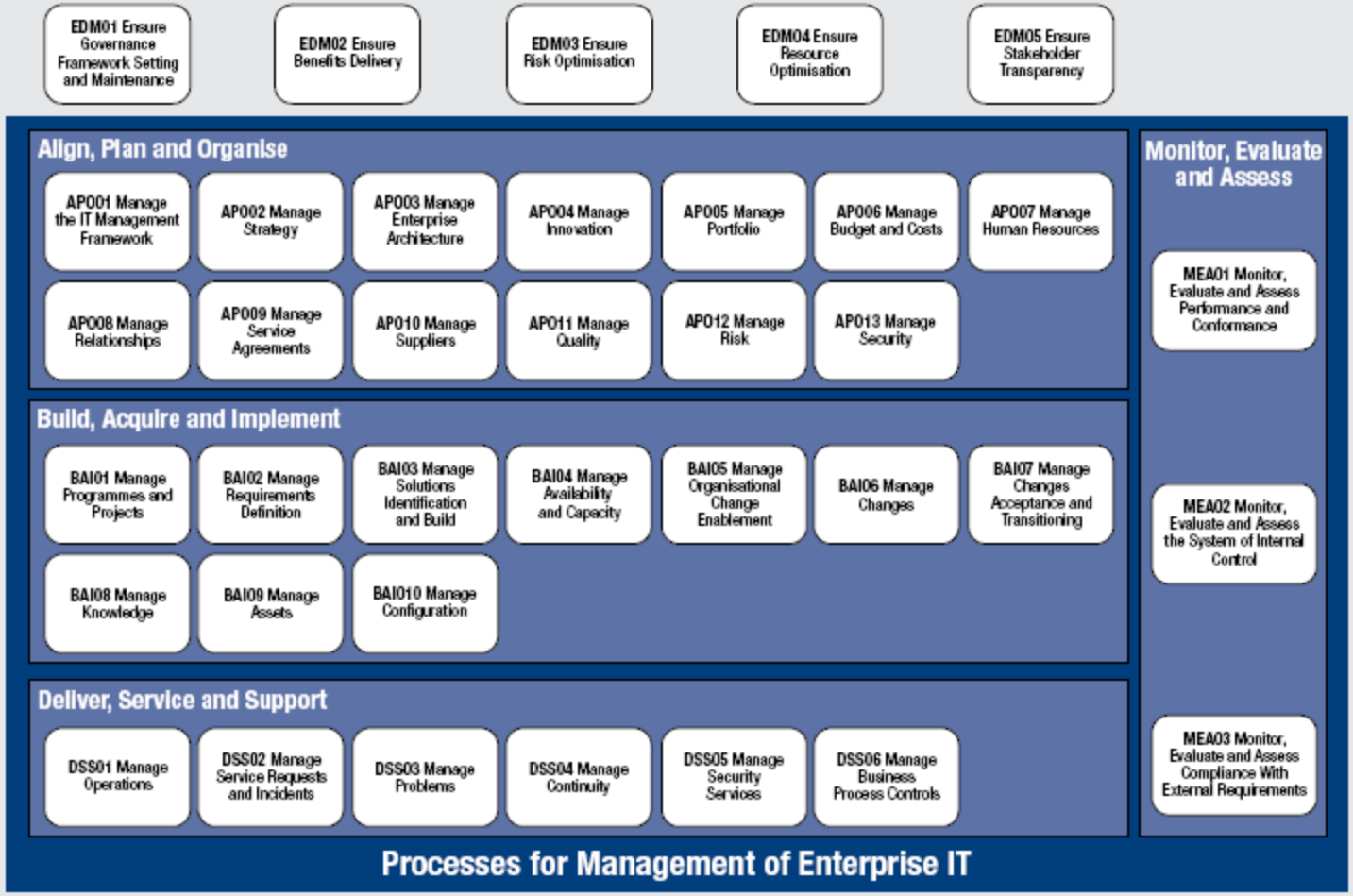
COBIT 5 Enablers: Processes

- *COBIT 5 Enablers: Processes* complements *COBIT 5* and contains a detailed reference guide to the processes that are defined in the COBIT 5 process reference model:
  - In section 2, the COBIT 5 goals cascade is recapitulated and complemented with a set of example metrics for the enterprise goals and the IT-related goals.
  - In section 3, the COBIT 5 process model is explained and its components defined.
  - Section 4 shows the diagram of this process reference model.
  - Section 5 contains the detailed process information for all 37 COBIT 5 processes in the process reference model.

COBIT 5 Enablers: Processes (Cont.)



COBIT 5 Enablers: Processes (Cont.)



COBIT 5 Enablers: Processes (Cont.)

COBIT 5: Enabling Processes

- The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management— with management further divided into domains of processes:
  - The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
  - The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM)

COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

COBIT 5 Implementation

COBIT 5 Implementation

- The improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance.
- Information and the pervasiveness of information technology are increasingly part of every aspect of business and public life.
- The need to drive more value from IT investments and manage an increasing array of IT-related risk has never been greater.
- Increasing regulation and legislation over business use of information is also driving heightened awareness of the importance of a well-governed and managed IT environment.

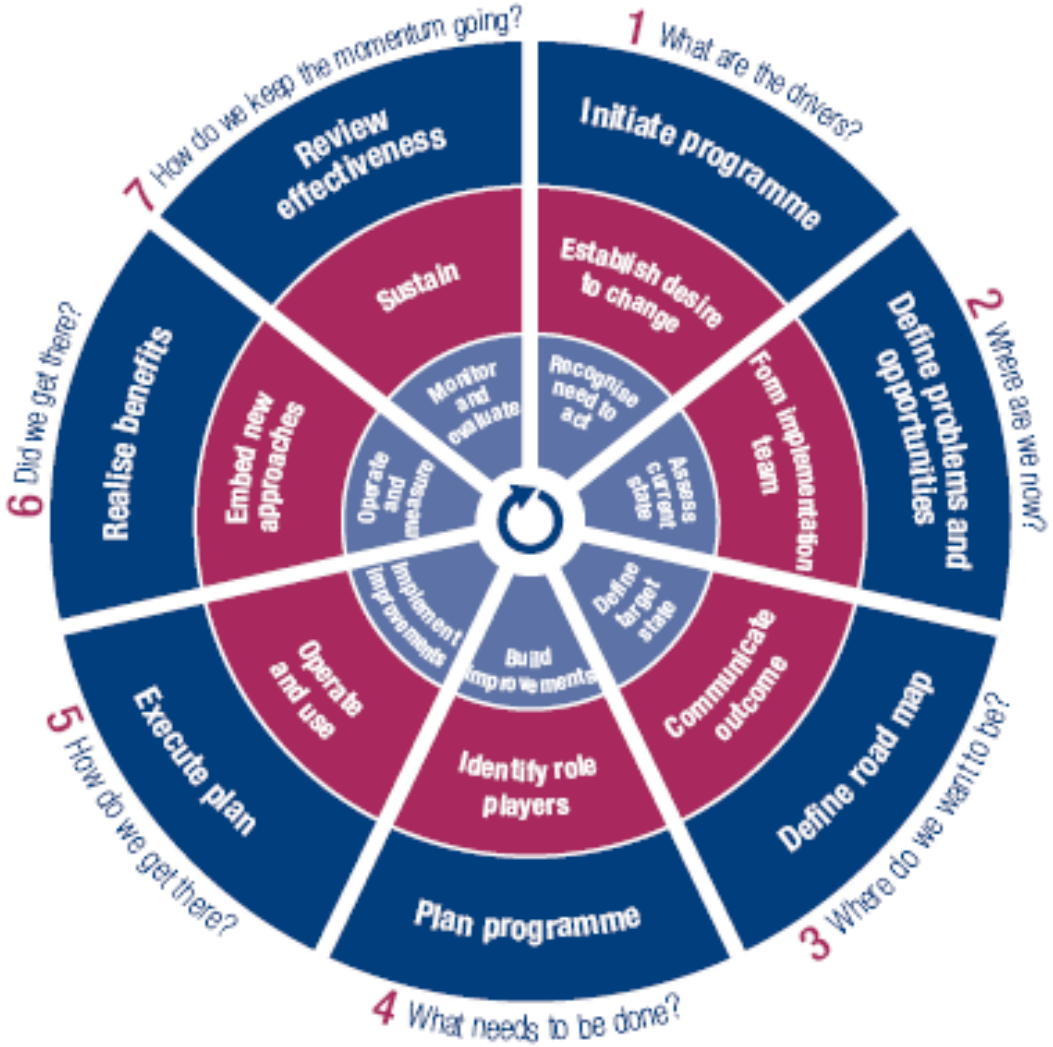
COBIT 5 Implementation (Cont.)

- ISACA has developed the COBIT5 framework to help enterprises implement sound governance enablers. Indeed, implementing good GEIT is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT5.
- However, frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.
- ***COBIT 5 Implementation* provides guidance on how to do this.**

COBIT 5 Implementation (Cont.)

- *COBIT 5 Implementation* covers the following subjects:
  - Positioning GEIT within an enterprise
  - Taking the first steps towards improving GEIT
  - Implementation challenges and success factors
  - Enabling GEIT-related organisational and behavioural change
  - Implementing continual improvement that includes change enablement and programme management
  - Using COBIT 5 and its components

COBIT 5 Implementation (Cont.)



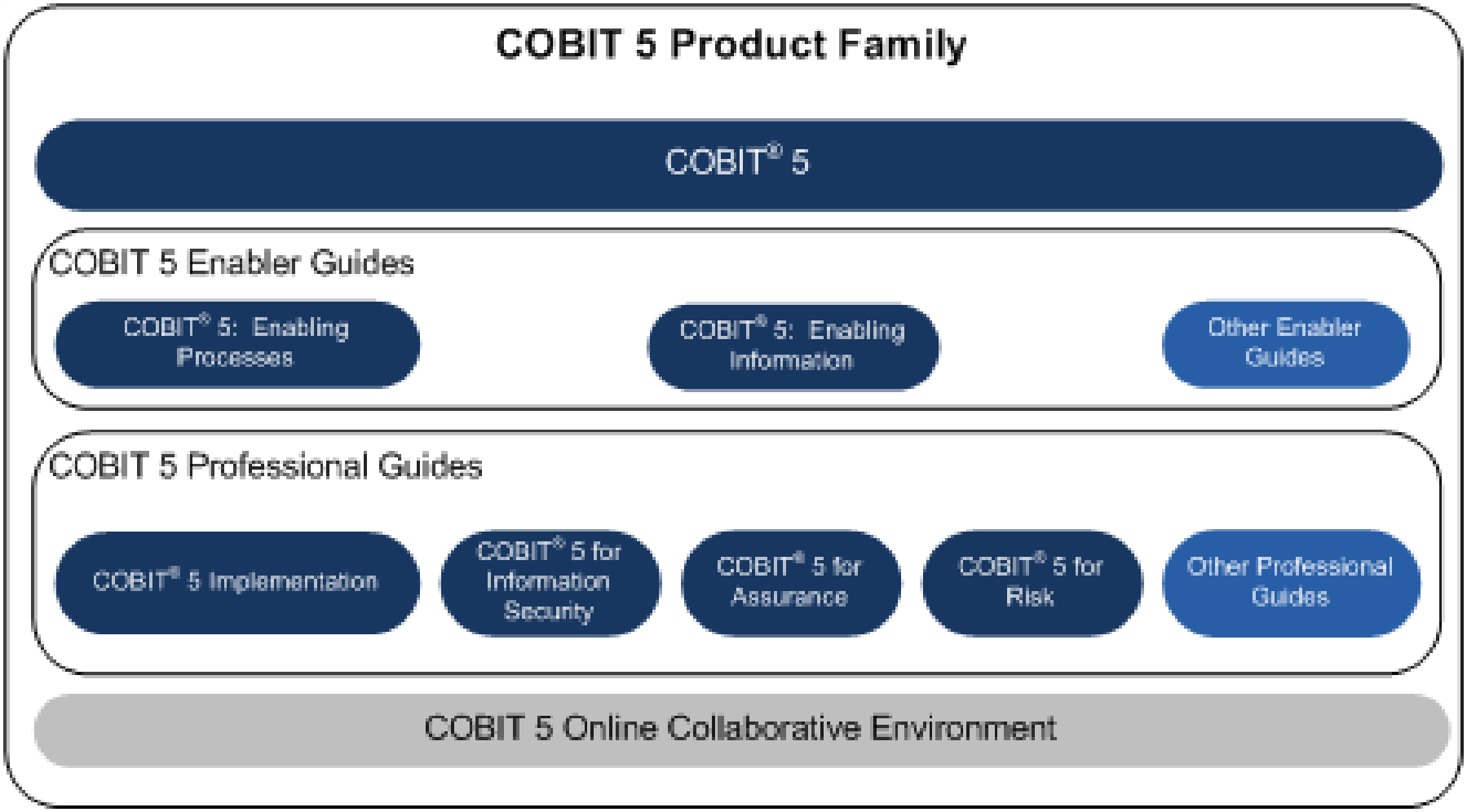
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

COBIT 5
AN ISACA® FRAMEWORK

ISACA
Trust in, and value from, information systems

COBIT 5
Future Supporting Products

COBIT 5 Product Family



COBIT 5 Future Supporting Products

Future supporting products:

- **Practice Guides:**
  - **COBIT 5 for Information Security**
  - **COBIT 5 for Assurance**
  - **COBIT 5 for Risk**
- **Enabler Guides:**
  - **COBIT 5: Enabling Information**
- **COBIT Online Replacement**
- **COBIT Assessment Programme:**
  - **Process Assessment Model (PAM): Using COBIT 5**
  - **Assessor Guide : Using COBIT 5**
  - **Self-assessment Guide: Using COBIT 5**

Questions?

or

email me at:

john.w.lainhart@us.ibm.com