COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

COBIT 5

Presented by
Brian Barnier
C5 Workgroup Member
brian@valuebridgeadvisors.com

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?

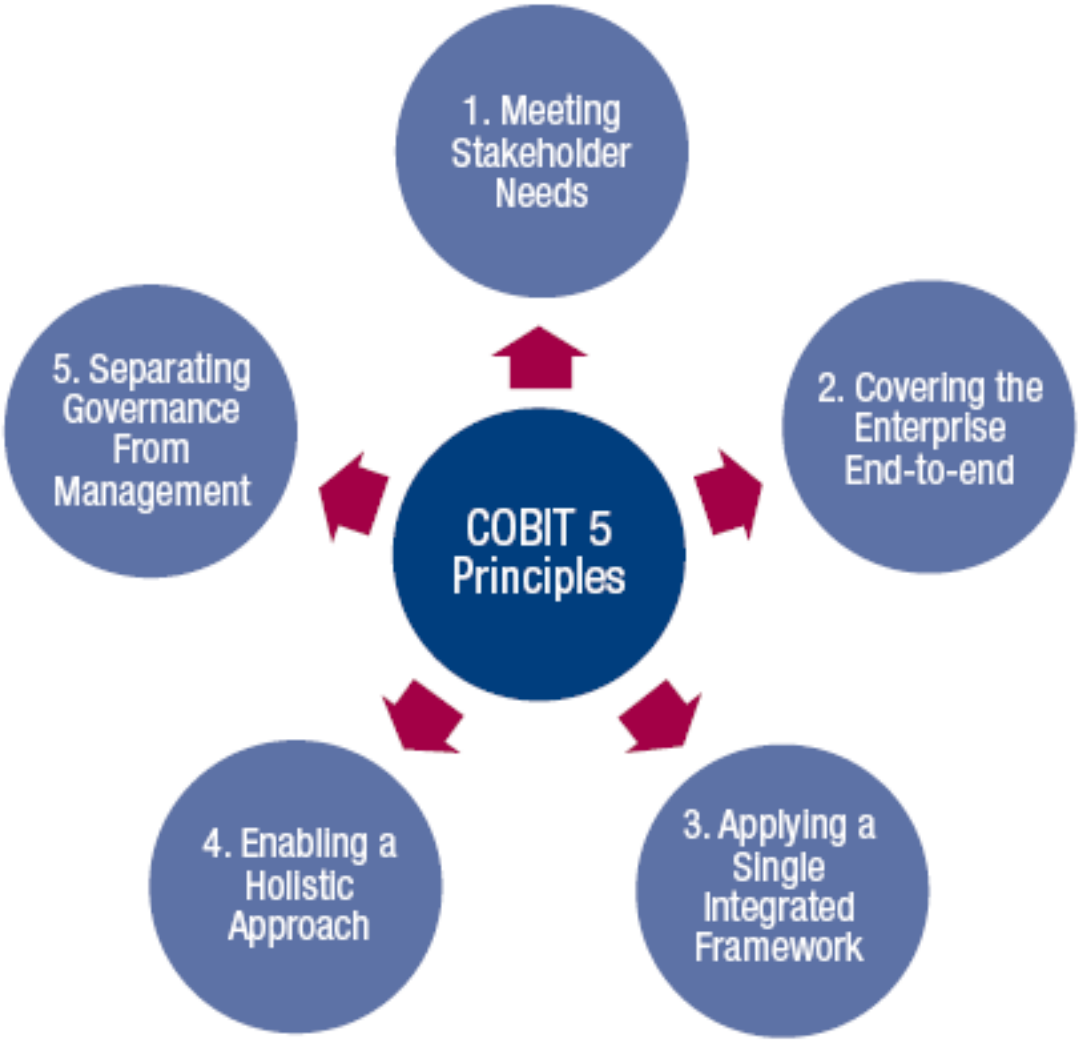
Stakeholder Value

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

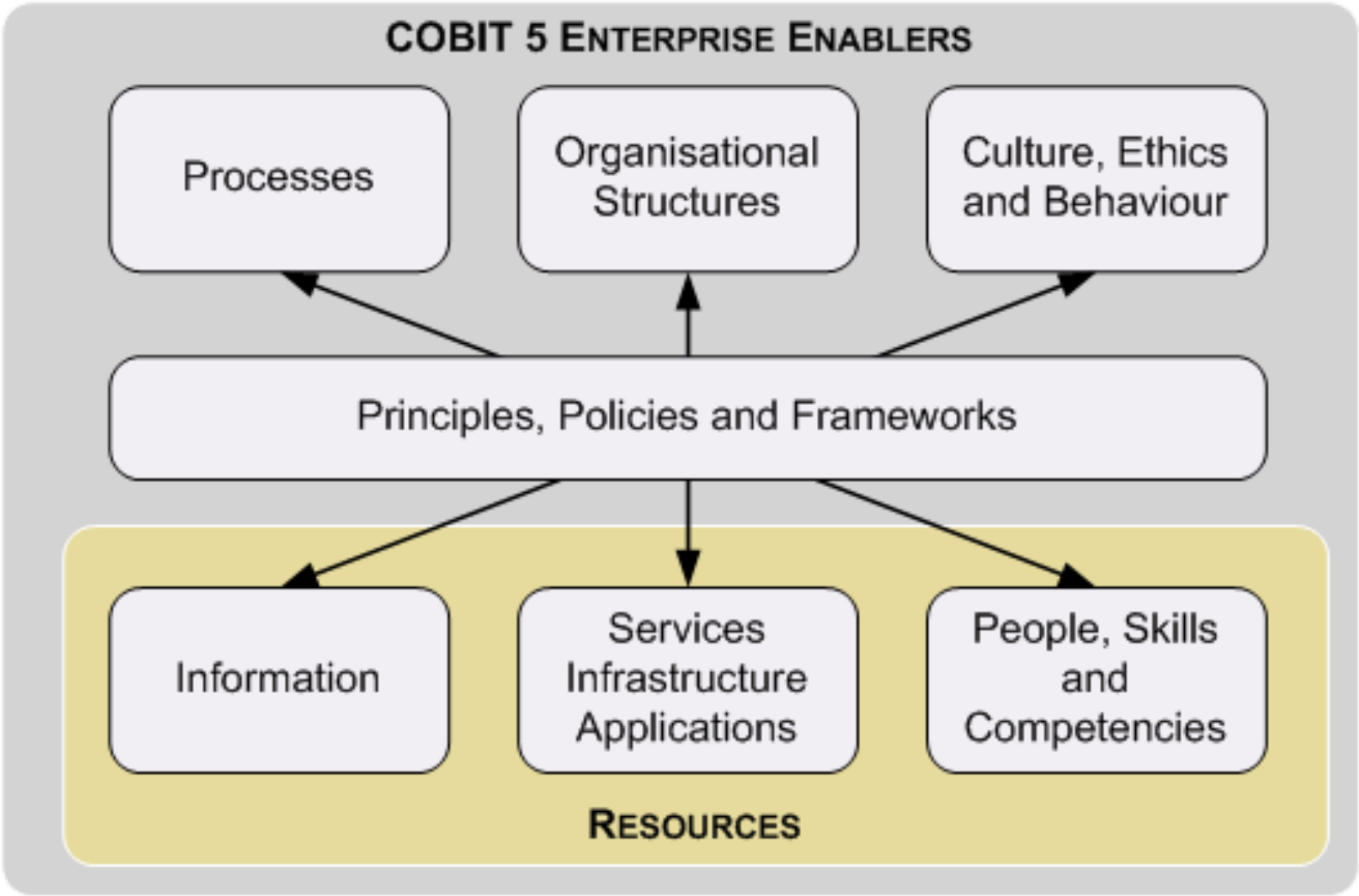
The COBIT 5 Framework

- 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

ISACA
Trust in, and value from, information systems

- **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.

About YOU

- **Industry**
- **Role**
- **Years of use of ISACA products**

YOUR situation

- **How process oriented is your organization?**
- **How process oriented is your IT organization?**
- **To what extent does your organization currently use: COBIT, ValIT, Risk IT, Implementation Guide, BMIS, ITAF:**
  - Full, Partial, Starting, Considering, No plans?
- **Conduct a formal maturity assessment?**
- **If yes, maturity level?**

Your management team

- **CIO background**
  - business, tech or equal balance?
- **What does your CIO think about ISACA products?**
  - Use!, if you want to, audit does, not so hot, not aware
- **CIO reports to**
  - CEO, CFO, COO, CAO, other?
- **What does that role think about ISACA products?**
  - Use!, if you want to, audit does, not so hot, not aware

Business needs

- **Clarity of objectives**
  - Business
  - IT

- **What complications/hurdles are faced in by IT leaders in achieving these business objectives?**

ISACA product use

- **What is most helpful about ISACA products?**
- **What is most helpful about ISACA support?**

- **What challenges have you faced in adopting?**
- **What challenges have you faced in implementing?**

- **What do YOU most want to learn today?**

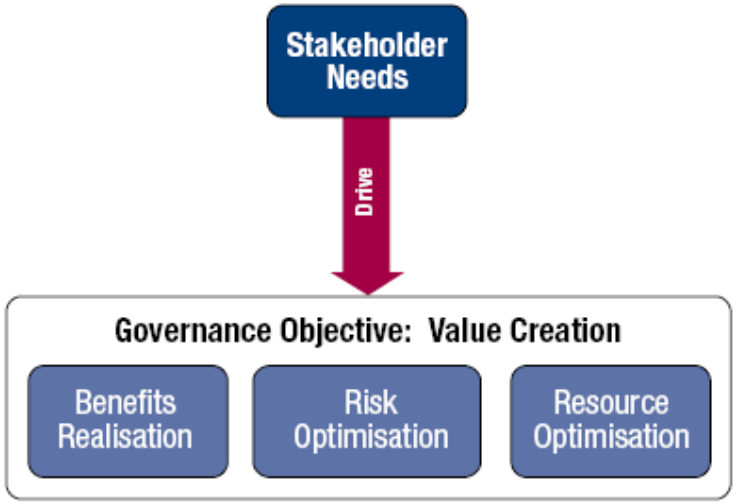
Comparing COBIT 5 and 4.1

Transition Message

- COBIT 5 builds on previous versions of COBIT (and Val IT and Risk IT) and so enterprises can also build on what they have developed using earlier versions.

Stakeholder Value and Business Objectives

- Enterprises exist to create value for their stakeholders. Consequently, any enterprise—commercial or not—will have value creation as a governance objective.
- Value creation means: Realising benefits at an optimal resource cost while optimising risk.

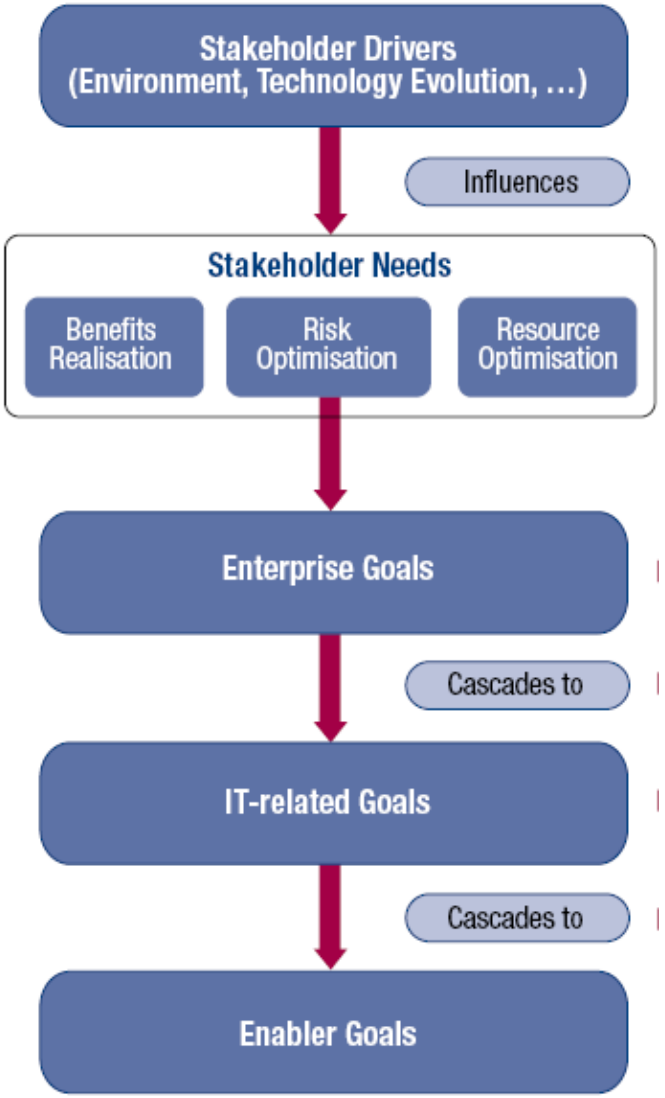


Stakeholder Value and Business Objectives (cont.)

Principle 1:

Meeting Stakeholder Needs

- Stakeholder needs have to be transformed into an enterprise's 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.



Stakeholder Value and Business Objectives (cont.)

- **Stakeholder needs** can be related to a set of generic **enterprise goals.**
- These enterprise goals have been developed using the Balanced Scorecard (BSC) dimensions. (Kaplan, Robert S.; David P. Norton; *The Balanced Scorecard: Translating Strategy into Action,* Harvard University Press, USA, 1996)
- The enterprise goals are a list of commonly used goals that an enterprise has defined for itself.
- Although this list is not exhaustive, most enterprise-specific goals can be easily mapped onto one or more of the generic enterprise goals.

Stakeholder Value and Business Objectives (cont.)

BSC Dimension	Enterprise Goals	Relation to Governance Objectives		
		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		

Stakeholder Value and Business Objectives (cont.)

- The goals cascade is not ‘new’ to COBIT.
- It was introduced in COBIT 4.0 in 2005.
- Those COBIT users who have applied the thinking to their enterprises have found value.
- BUT not everyone has recognized this value.
- The goals cascade supports the COBIT 5 stakeholder needs principle that is fundamental to COBIT and has therefore been made prominent early in the COBIT 5 guidance.
- The goals cascade has been revisited and updated for the COBIT 5 release.

Governance and Management Defined

- What sort of framework is COBIT?
  - An IT audit and control framework?
    - COBIT (1996) and COBIT 2nd Edition (1998)
    - Focus on Control Objectives
  - An IT management framework?
    - COBIT 3rd Edition (2000)
    - Management Guidelines added
  - An IT governance framework?
    - COBIT 4.0 (2005) and COBIT 4.1 (2007)
    - Governance and compliance processes added
    - Assurance processes removed
- BUT what is the difference between governance and management?

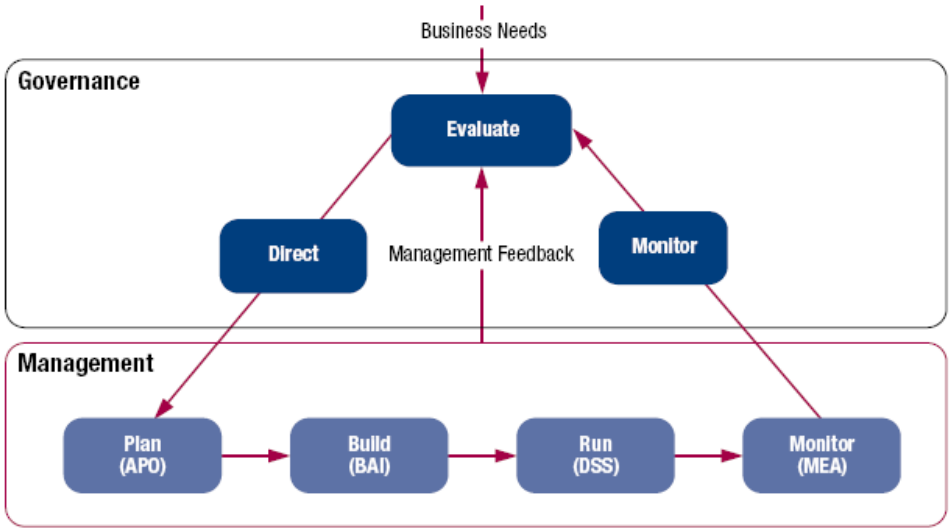
Governance and Management Defined (cont.)

- **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).**

Governance and Management Defined (cont.)

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)

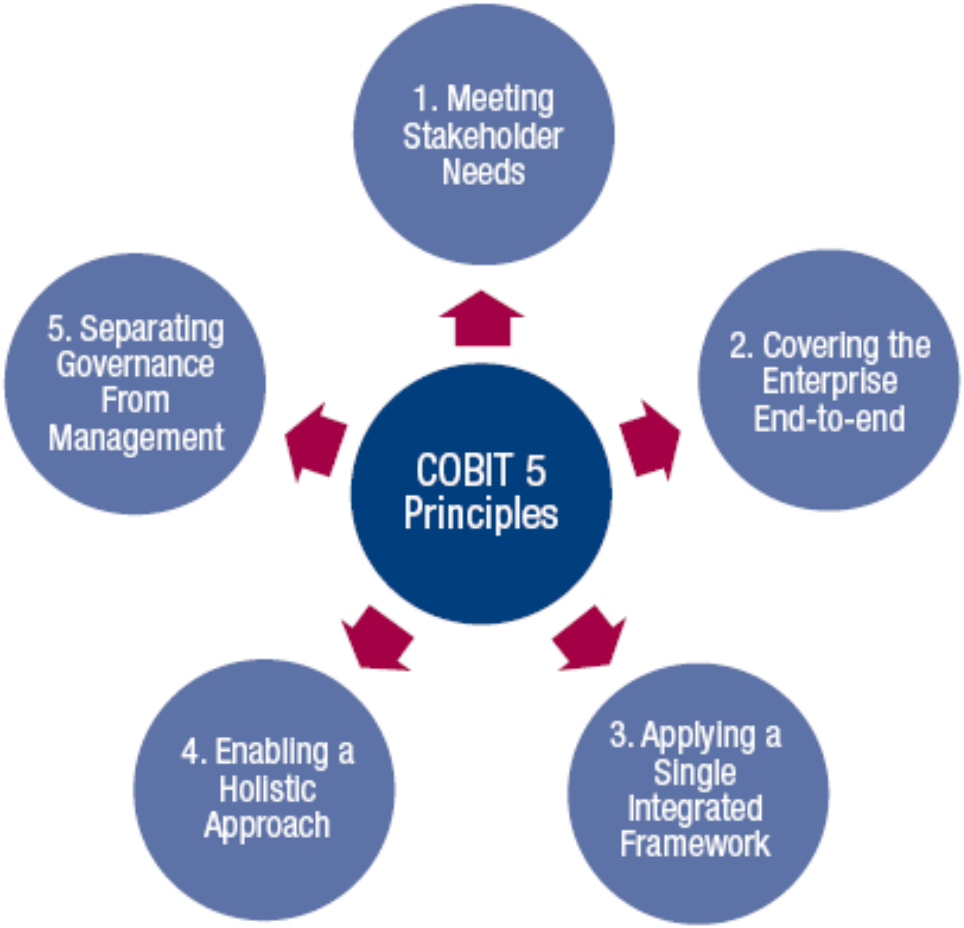


Areas of Change

- The following slides summarise the major changes in COBIT 5 content and how they may impact GEIT implementation/improvement:
  1. New GEIT Principles
  2. Increased Focus on Enablers
  3. New Process Reference Model
  4. New and Modified Processes
  5. Practices and Activities
  6. Goals and Metrics
  7. Inputs and Outputs
  8. RACI Charts
  9. Process Capability Maturity Models and Assessments

1. New GEIT Principles

COBIT 5 Principles

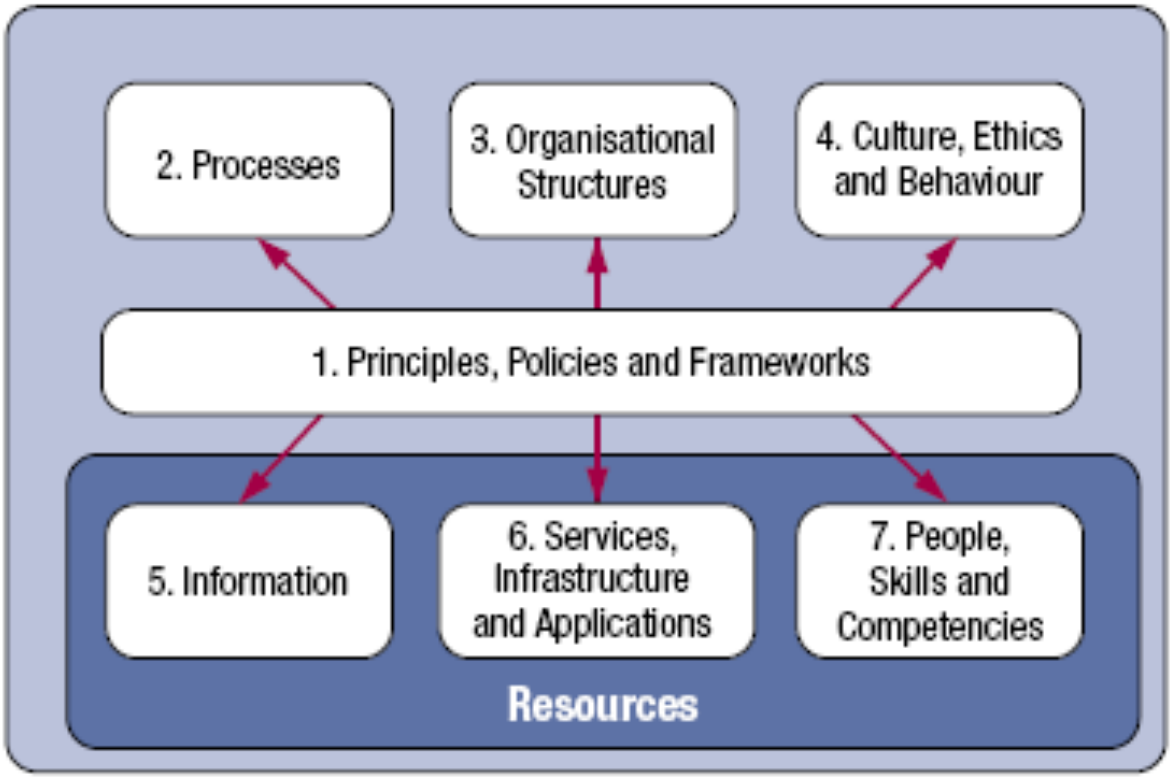


1. New GEIT Principles (cont.)

- Val IT and Risk IT frameworks are principles-based.
- Feedback indicated that principles are easy to understand and put into an enterprise context, allowing value to be derived from the supporting guidance more effectively.
- ISO/IEC 38500 also incorporates principles to underpin its messages to achieve the same market benefit delivery, although the principles in this standard and COBIT 5 are not the same.

2. Increased Focus on Enablers

- COBIT 4.1 did not have enablers! Yes it did—they were not called enablers, but they were there, explicitly or implicitly!



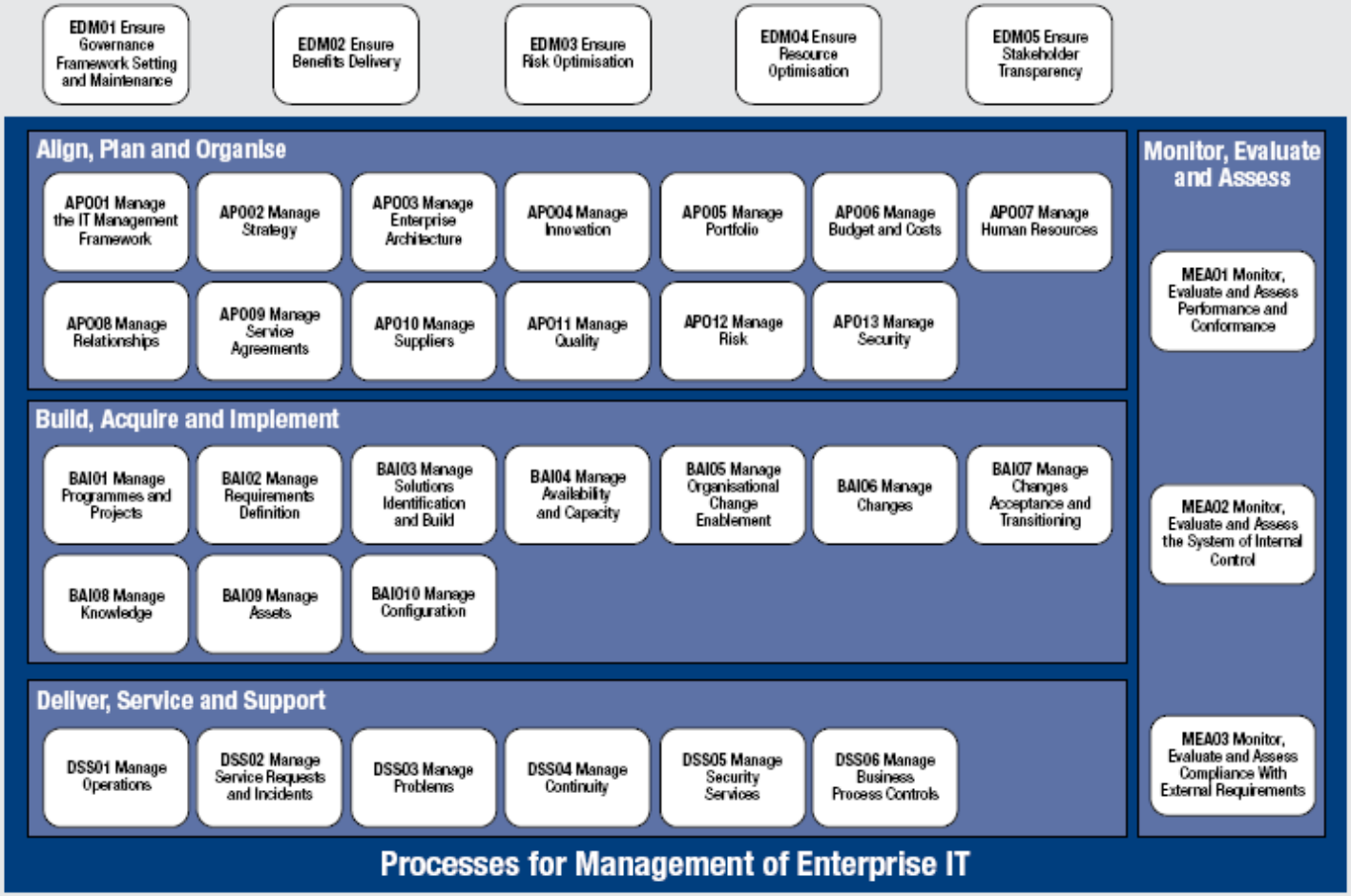
2. Increased Focus on Enablers (cont.)

- Information, infrastructure, applications (services) and people (people, skills and competencies) were COBIT 4.1 resources.
- Principles, policies and frameworks were mentioned in a few COBIT 4.1 processes.
- Processes were central to COBIT 4.1 use.
- Organisational structure was implied through the responsible, accountable, consulted or informed (RACI) roles and their definitions.
- Culture, ethics and behaviour were mentioned in a few COBIT 4.1 processes.

3. New Process Reference Model

- COBIT 5 is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities end-to-end—i.e., business and IT function areas.
- COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into one framework, and has been updated to align with current best practices—e.g., ITIL, TOGAF.
- The new model can be used as a guide for adjusting as necessary the enterprise's own process model (just like COBIT 4.1).

3. New Process Reference Model (cont.)

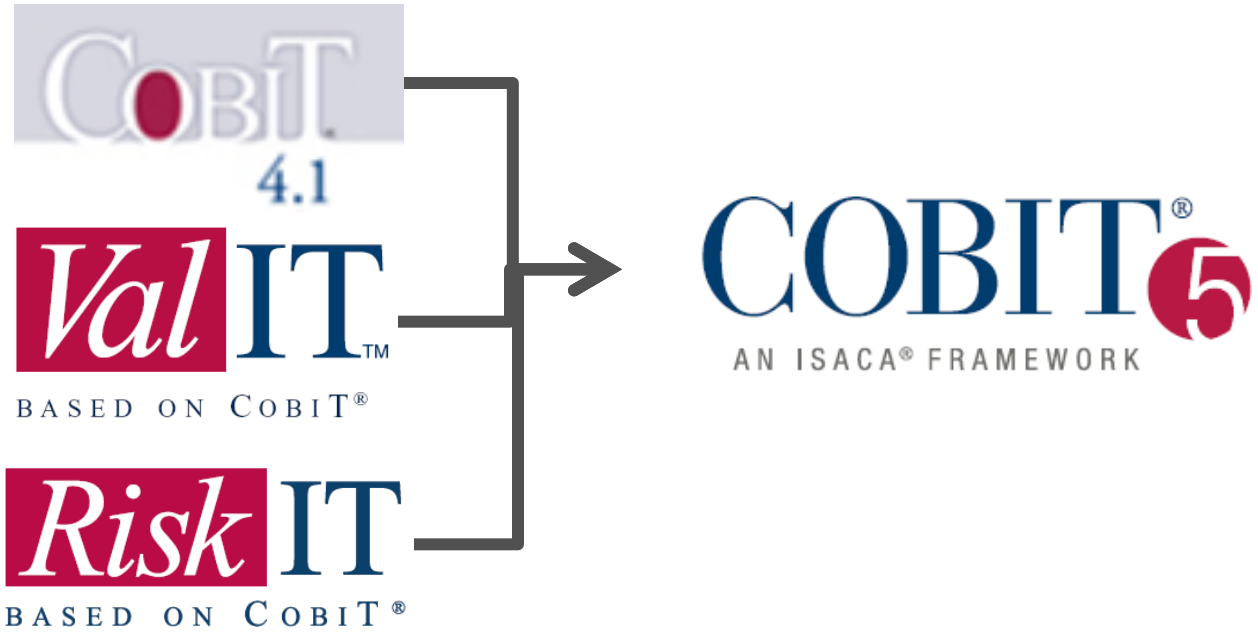


4. New and Modified Processes

- COBIT 5 introduces five new governance processes that have leveraged and improved COBIT 4.1, Val IT and Risk IT governance approaches.
- This guidance:
  - Helps enterprises to further refine and strengthen executive management-level GEIT practices and activities
  - Supports GEIT integration with existing enterprise governance practices and is aligned with ISO/IEC 38500

4. New and Modified Processes (cont.)

- COBIT 5 has clarified management level processes and integrated COBIT 4.1, Val IT and Risk IT content into one process reference model



4. New and Modified Processes (cont.)

- There are several new and modified processes that reflect current thinking, in particular:
  - APO03 Manage enterprise architecture.
  - APO04 Manage innovation.
  - APO05 Manage portfolio.
  - APO06 Manage budget and costs.
  - APO08 Manage relationships.
  - APO13 Manage security.
  - BAI05 Manage organisational change enablement.
  - BAI08 Manage knowledge.
  - BAI09 Manage assets.
  - DSS05 Manage security service.
  - DSS06 Manage business process controls.

4. New and Modified Processes (cont.)

- COBIT 5 processes now cover *end-to-end business and IT activities*—i.e., a full enterprise-level view.
- This provides for a more holistic and complete coverage of practices reflecting the pervasive enterprisewide nature of IT use.
- It makes the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more explicit and transparent.

5. Practices and Activities

- The COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives and Val IT and Risk IT processes.

  www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Where-Have-All-the-Control-Objectives-Gone.aspx
- The COBIT 5 activities are equivalent to the COBIT 4.1 control practices and Val IT and Risk IT management practices.
- COBIT 5 integrates and updates all of the previous content into the one new model, making it easier for users to understand and use this material when implementing improvements.

6. Goals and Metrics

- COBIT 5 follows the same goal and metric concepts as COBIT 4.1, Val IT and Risk IT, but these are renamed enterprise goals, IT-related goals and process goals reflecting an enterprise level view.
- COBIT 5 provides a revised goals cascade based on enterprise goals driving IT-related goals and then supported by critical processes.
- COBIT 5 provides examples of goals and metrics at the enterprise, process and management practice levels. This is a change to COBIT 4.1, Val IT and Risk IT, which went down one level lower.

7. Inputs and Outputs

- COBIT 5 provides inputs and outputs for every management practice, whereas COBIT 4.1 only provided these at the process level.
- This provides additional detailed guidance for designing processes to include essential work products and to assist with interprocess integration.

8. RACI Charts

- COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to COBIT4.1, Val IT and Risk IT.
- COBIT 5 provides a more complete, detailed and clearer range of generic business and IT role players and charts than COBIT 4.1 for each management practice, enabling better definition of role player responsibilities or level of involvement when designing and implementing processes.

8. RACI Charts (cont.)

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain a technology infrastructure plan.		I	I	A		C	R	C	C		C
Create and maintain technology standards.				A		C	R	C	I	I	I
Publish technology standards.		I	I	A		I	R	I	I	I	I
Monitor technology evolution.		I	I	A		C	R	C		C	C
Define (future) (strategic) use of new technology.		C	C	A		C	R	C		C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

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

9. Process Capability Maturity Models and Assessments

- COBIT 5 discontinues the COBIT 4.1, Val IT and Risk IT CMM-based capability maturity modelling approach.
- COBIT 5 will be supported by a new process capability assessment approach based on ISO/IEC 15504, and the **COBIT Assessment Programme** has already been established for COBIT 4.1 as an alternative to the CMM approach.

  www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Assessment-Programme.aspx
- The COBIT 4.1, Val IT and Risk IT CMM-based approaches are **not considered compatible** with the ISO/IEC 15504 approach because the methods use different attributes and measurement scales.

Process capability model comparison

COBIT 4.1 Maturity Model Levels	COBIT 5 ISO/IEC 15504 Based Capability Levels	Meaning of the COBIT 5 ISO/IEC 15504 Based Capability Levels	Context
5. Optimised	5. Optimised	Continuously improved to meet relevant current and projected enterprise goals.	Enterprise view/ corporate knowledge
4. Managed and Measurable	4. Predictable	Operates within defined limits to achieve its process outcomes.	
3. Defined	3. Established	Implemented using a defined process that is capable of achieving its process outcomes.	
N/A	2. Managed	Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	Instance view/ individual knowledge
N/A	1. Performed	Process achieves its process purpose.	
2. Repeatable 1. *Ad Hoc* 0. Non-existent	0. Incomplete	Not implemented or little or no evidence of any systematic achievement of the process purpose.	

9. Process Capability Maturity Models and Assessments (cont.)

COBIT 4.1/5

Process Reference Model
- Domain and Scope
- Process Purpose
- Process Outcomes

Measurement Framework
- Capability Levels
- Process Attributes
- Rating Scale

Process Assessment Model
- Scope
- Indicators
- Mapping
- Translation

INITIAL INPUT
- Purpose
- Scope
- Constraints
- Identities
- Approach
- Assessor Competence Criteria
- Additional Information

ASSESSMENT PROCESS
Planning
Data Collection
Data Validation
Process Attribute Rating
Reporting

OUTPUT
- Date
- Assessment Input
- Identification of Evidence
- Assessment Process Used
- Process Profiles
- Additional Information

Roles and Responsibilities
- Sponsor
- Competent Assessor
- Assessors

9. Process Capability Maturity Models and Assessments (cont.)

- The COBIT Assessment Programme approach is considered by ISACA to be more robust, reliable and repeatable as a process capability assessment method.
- The COBIT Assessment Programme supports:
  - Formal assessments by accredited assessors (assessor training is being developed)
  - Less rigorous self-assessments for internal gap analysis and process improvement planning
- The COBIT Assessment Programme, in the future, will also potentially enable an enterprise to obtain an independent and certified assessments aligned to the ISO/IEC standard.

9. Process Capability Maturity Models and Assessments (cont.)

- What materials support the COBIT Assessment Programme approach?
  - ***COBIT Process Assessment Model (PAM): Using COBIT 4.1***—Serves as a base reference document for the performance of a capability assessment of an organisation's current IT processes against COBIT
  - ***COBIT Assessor Guide: Using COBIT 4.1***—Provides details on how to undertake a full ISO-compliant assessment
  - ***COBIT Self-assessment Guide: Using COBIT 4.1***—Provides guidance on how to perform a basic self-assessment of an organisation's current IT process capability levels against COBIT processes
- The above materials exist to support COBIT 4.1-based assessments now; versions will be produced to support COBIT 5-based assessments.

9. Process Capability Maturity Models and Assessments (cont.)

- COBIT 4.1, Val IT and Risk IT users wishing to move to the new COBIT Assessment Programme approach will need to realign their previous ratings, adopt and learn the new method, and initiate a new set of assessments in order to gain the benefits of the new approach.
- Although some of the information gathered from previous assessments may be reusable, care will be needed in migrating this information forward because there are significant differences in requirements.

9. Process Capability Maturity Models and Assessments (cont.)

- COBIT 4.1, Val IT and Risk IT users wishing to continue with the CMM-based approach, either as an interim or ongoing approach, can use the COBIT 5 guidance, but must use the COBIT 4.1 generic attribute table without the high-level maturity models.

ISACA®
Trust in, and value from, information systems

COBIT 5 Implementation

COBIT 5 Implementation

ISACA
Trust in, and value from, information systems

- 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 COBIT 5 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 COBIT 5.
- 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

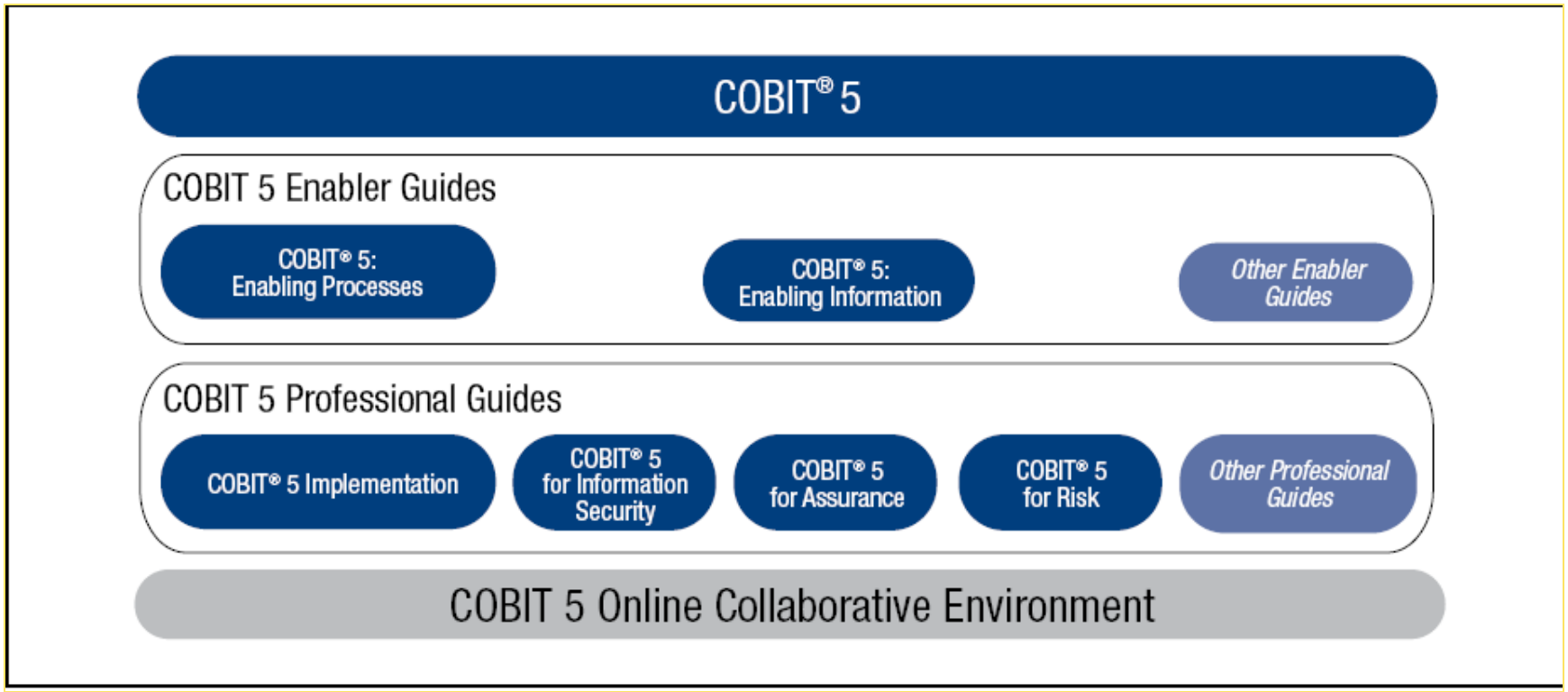
COBIT 5 Implementation (cont.)

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

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:

- Professional 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