COBIT 5 Explained .. "Geek Week" COBIT 5 Update

Robert E Stroud (CGEIT)
ISACA Strategic Advisory Council
Vice President Strategy & Innovation, CA Technologies

COBIT 5 Explained

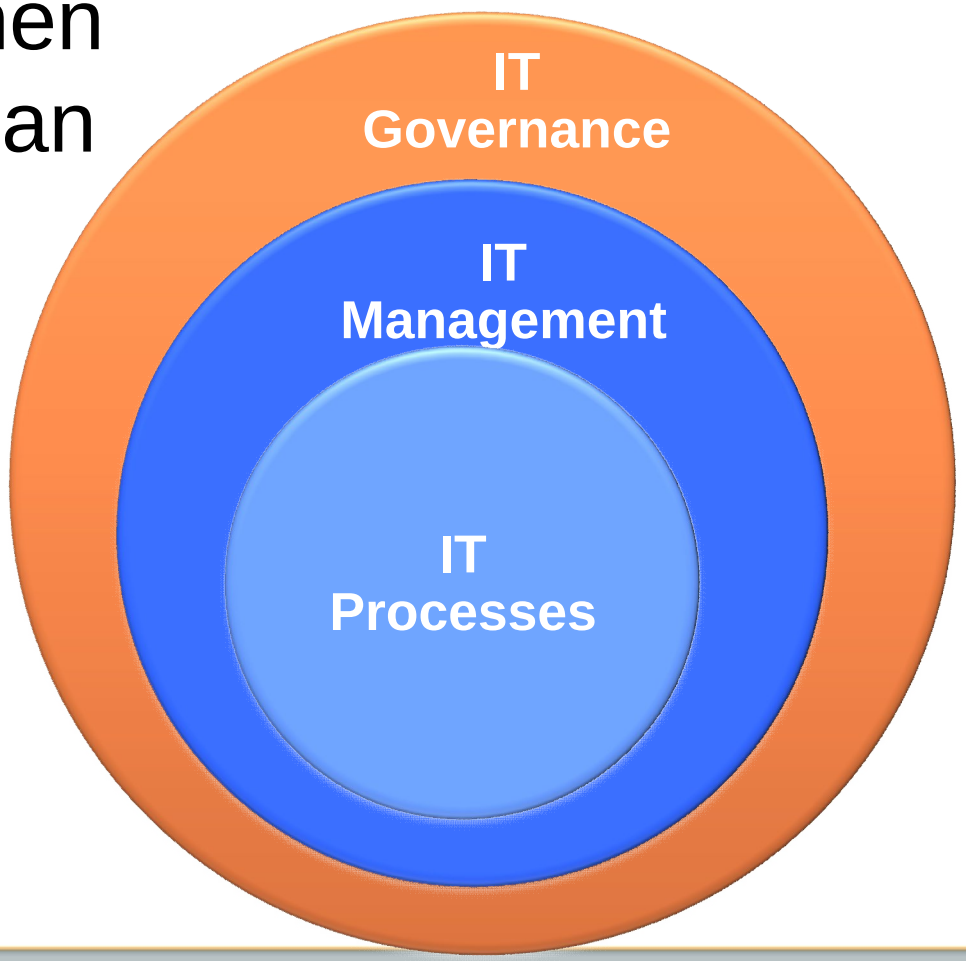
Robert Stroud, Vice President Strategy & Innovation CA Technologies

- The Control Objectives for Information and Related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management, created by the Information Systems Audit and Control Association (now know as simply “ISACA”) and the IT Governance Institute (ITGI) in 1996.

- ISACA is currently creating the COBIT 5 framework combining COBIT, Val IT and Risk IT for a detailed framework for the effective governance and management of IT enabled business. While COBIT ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. And while COBIT provides a set of controls to mitigate IT risk in IT processes, Risk IT provides a framework for enterprises to identify, govern and manage IT-related risks. This session will update you on the development to date, anticipated outcomes and set timeline expectations.

COBIT – a true IT Governance framework?

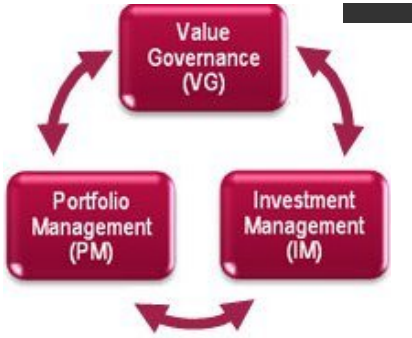
- If Governance is defined as “Management of Management”, then COBIT 4.1 is more an IT Management framework than an IT Governance framework!

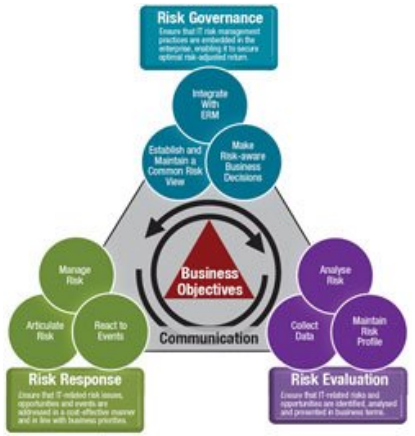


IT Governance in the current COBIT framework

ISACA
Trust in, and value from, information systems

- COBIT 4.1 (2007) introduces IT Governance, (e.g. the pentagon) and includes a few specific governance processes, e.g. “ME4 Provide IT Governance”
- Processes and Control Objectives are considered as governance means and all processes are related to the pentagon
- Management of stakeholder requirements (internal and external) is addressed by COBIT 4.1 (e.g. in the Management guidelines)
- More governance elements in Val IT 2.0 (2008) (“Value Governance”) and Risk IT (2009) (“Risk Governance”)
- Board Briefing on IT Governance (2003)





IT Governance in the current COBIT framework

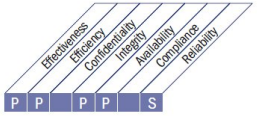
ISACA®
Trust in, and value from, information systems

Acquire and Implement AI6
Manage Changes

PROCESS DESCRIPTION

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.



Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

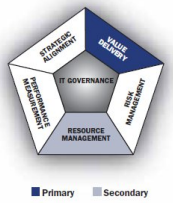
controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions; minimising errors due to incomplete request specifications; and halting implementation of unauthorised changes

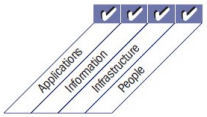
is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Amount of application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

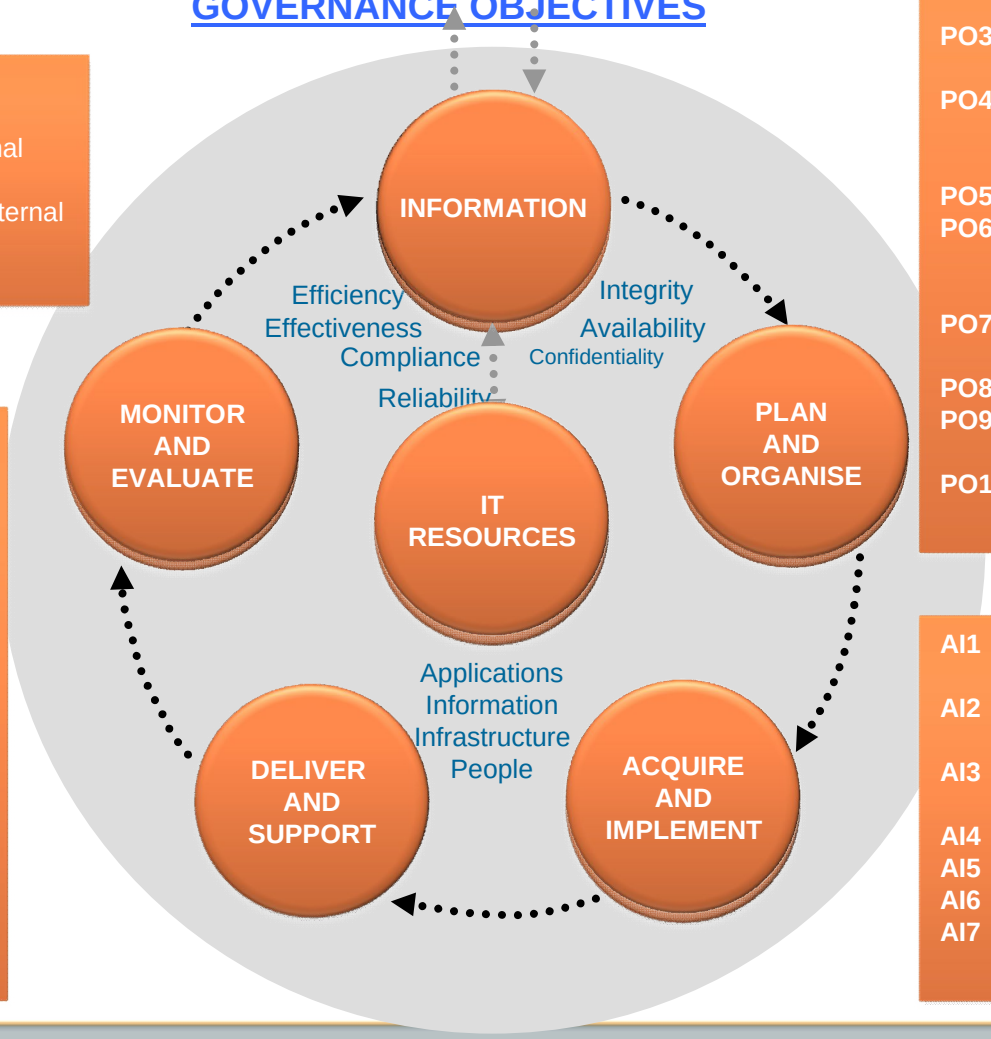




COBIT – Process Landscape

ISACA
Trust in, and value from, information systems

BUSINESS OBJECTIVES AND GOVERNANCE OBJECTIVES



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organization and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Taking Governance Forward

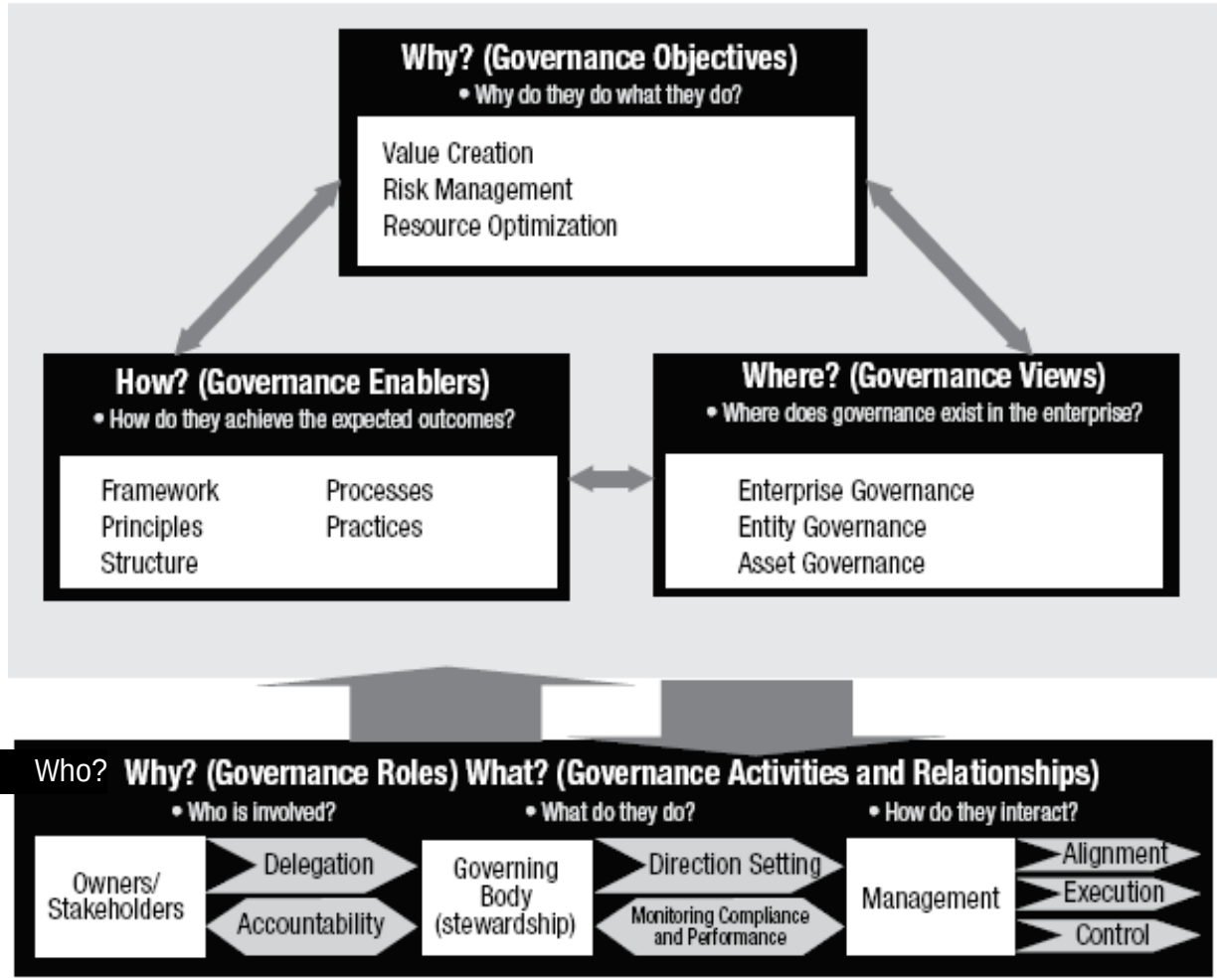
- The IT Governance Institute (ITGI) in 2008, launched the Taking Governance Forward initiative - a free online resource that provides a way for people to learn the latest on governance and join the debate on how to make it work for their organizations.
- Objectives of the initiative:
  - To reach agreement on a universally acceptable definition of governance.
  - To clarify the debate on governance by providing a comprehensive yet simple-to-use overview of the components and relationships of governance
  - To provide practical tools to understand the governance views model in the enterprise and learn high-level ways to initiate implementation
  - http://www.takinggovernanceforward.org

Source: Taking Governance Forward, 2008

Governance "On a Page"

ISACA
Trust in, and value from, information systems

Figure 1—Governance "On a Page"



Source: Taking Governance Forward, 2008

Governance Views

- Taking Governance Forward defines three views of governance: Enterprise, entity and asset.
  - Enterprise governance incorporates all views of governance within an enterprise.
  - Entity governance deals with a specific line of business, function or business entity within the enterprise.
  - Assets may be tangible or intangible; they are critical to the enterprise's success and involve many stakeholders.

Figure 2—Governance Views

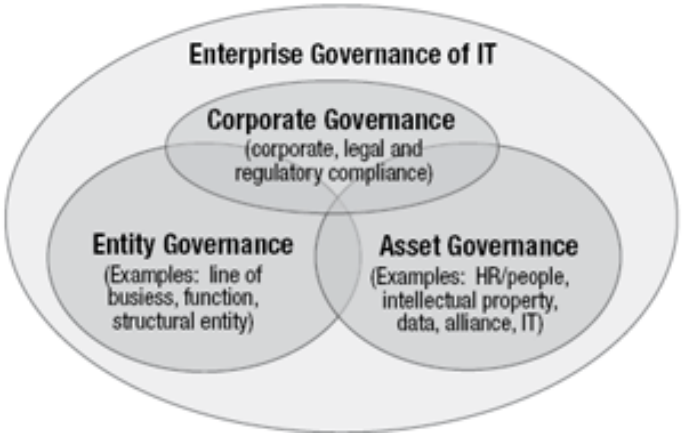
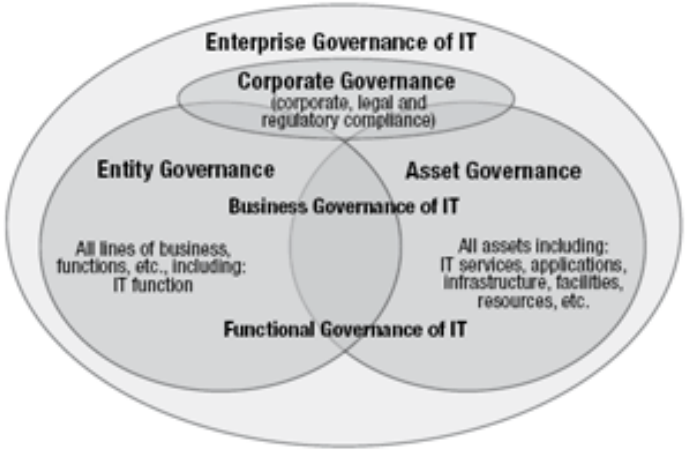


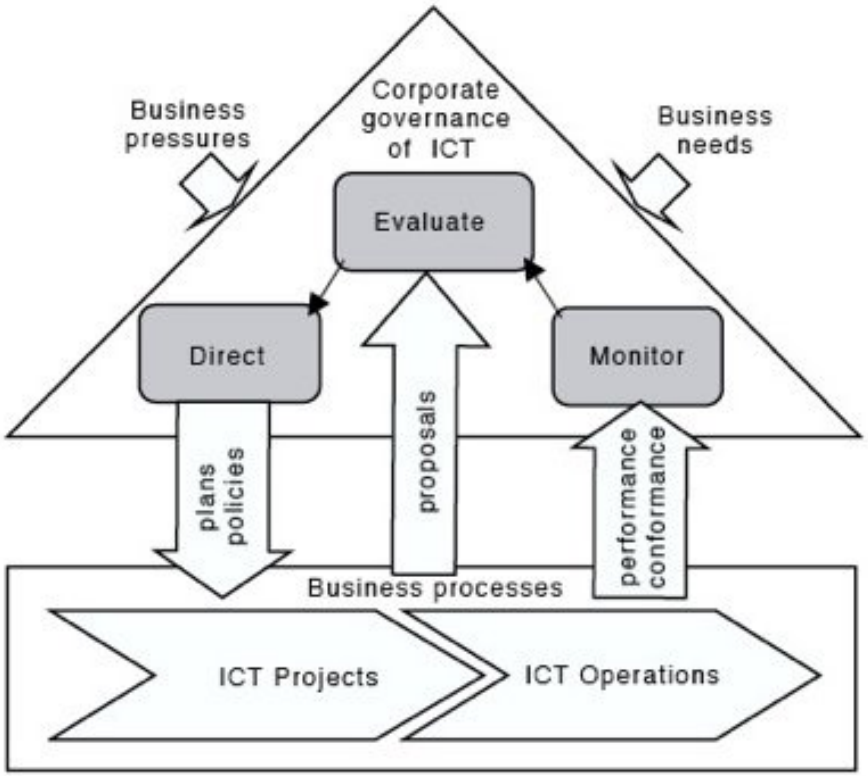
Figure 3—Enterprise Governance of IT



Source: Taking Governance Forward, 2008

Governance activities according to ISO/IEC 38500

- Evaluate
  - (Board Briefing: Compare objectives and performance)
- Direct
  - (Board Briefing: Provide direction)
- Monitor
  - (Board Briefing: Measure performance)

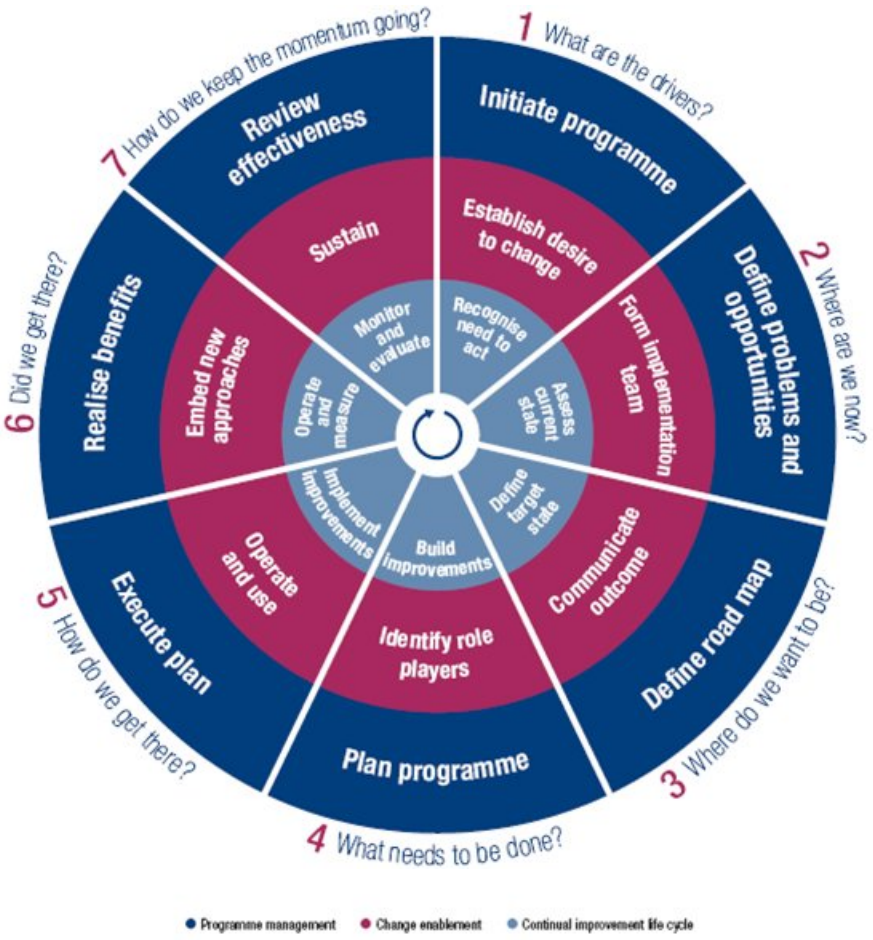


Implementing and Continually Improving IT Governance

- The IT Governance Institute (ITGI) in 2009 published the “Implementing and Continually Improving IT Governance” publication that provides detailed, structured guidance to the implementation and improvement of IT governance.
- The guidance is generic and not just for adopting and adapting COBIT.

Implementing and Continually Improving IT Governance

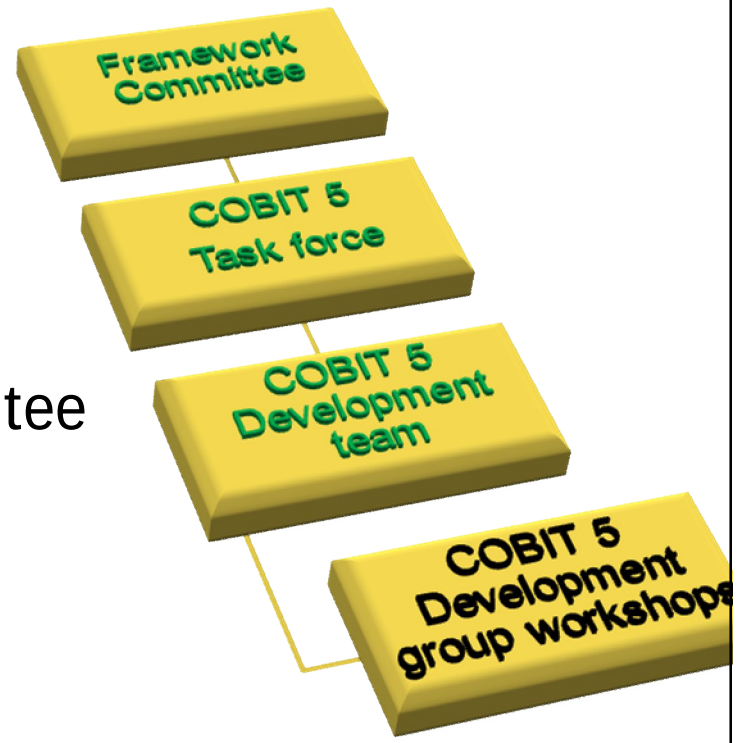
- Seven phases in the life c
  - What are the drivers?
  - Where are we now?
  - Where do we want to be?
  - What needs to be done?
  - How do we get there?
  - Did we get there?
  - How do we keep the momentum going?



Source: Implementing and Continually Improving IT Governance, 2009 © IT Governance Institute, 2009

COBIT 5 Initiative

- The initiative charge from the Board of Directors:
  - "tie together and reinforce all ISACA knowledge assets with COBIT."
- The COBIT 5 Task Force:
  - experts from ISACA constituency groups
  - reports to the Framework Committee and then the Knowledge Board



COBIT 5 Objectives

COBIT 5 will:

- Provide a renewed and authoritative governance and management framework for enterprise information and related technology, building on the current widely recognized and accepted COBIT framework, linking together and reinforcing all other major ISACA frameworks and guidance such as:

Val IT	**Risk IT**
BMIS	**ITAF**
Board Briefing	**Taking Governance Forward**

- Connect to other major frameworks and standards in the marketplace (ITIL, ISO standards, etc.)

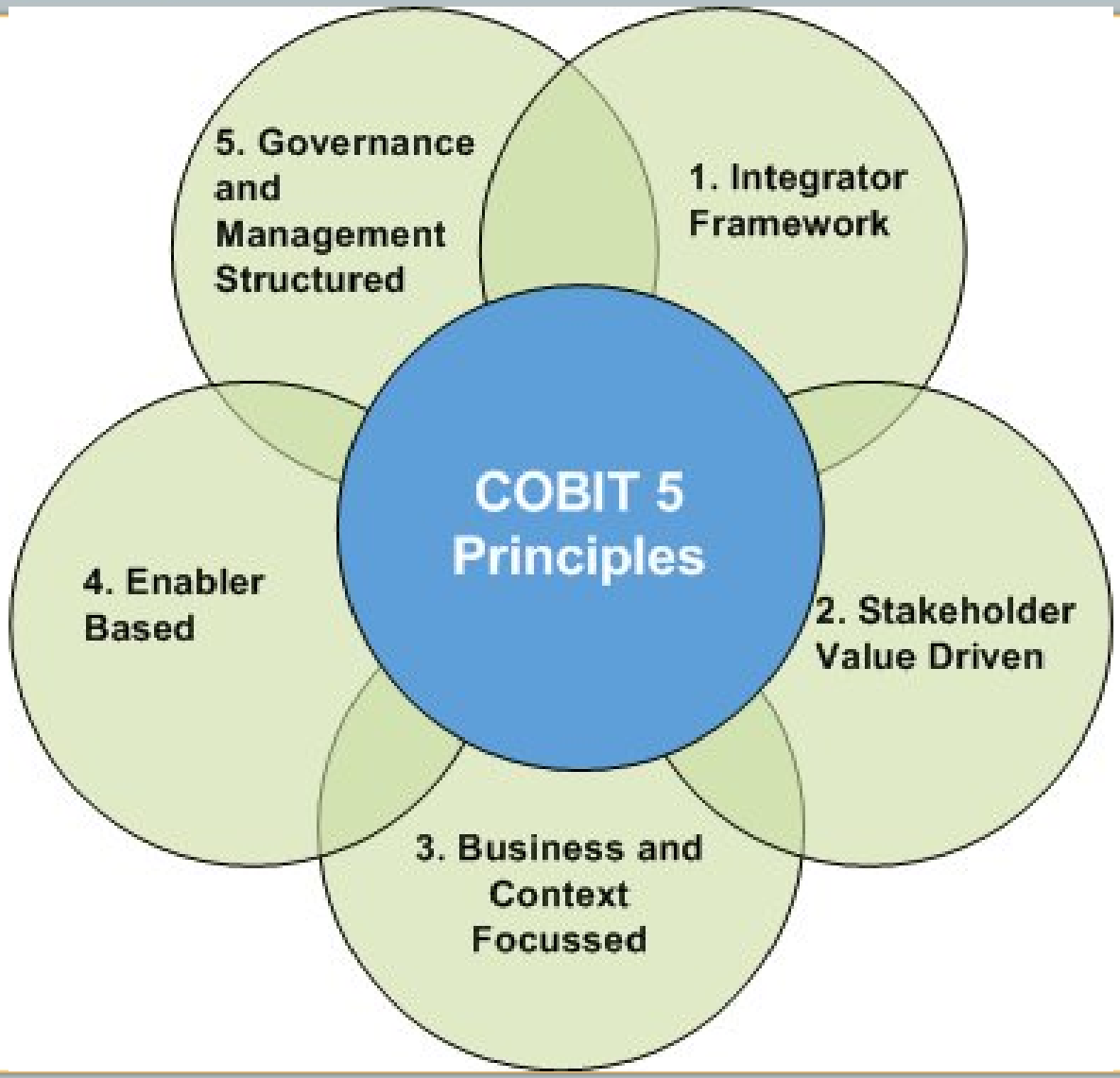
What Will Be Delivered?

- An enterprisewide, “end-to-end” framework addressing governance and management of information and related technology
- The framework structure will include familiar components such as a domain/process model and other components such as governance/management practices, RACI charts and inputs/outputs.
- An initial COBIT 5 product architecture, identifying the types of products and other guidance that could be developed for specific IT professional audiences (e.g., assurance, security, risk) in support of enterprise business needs

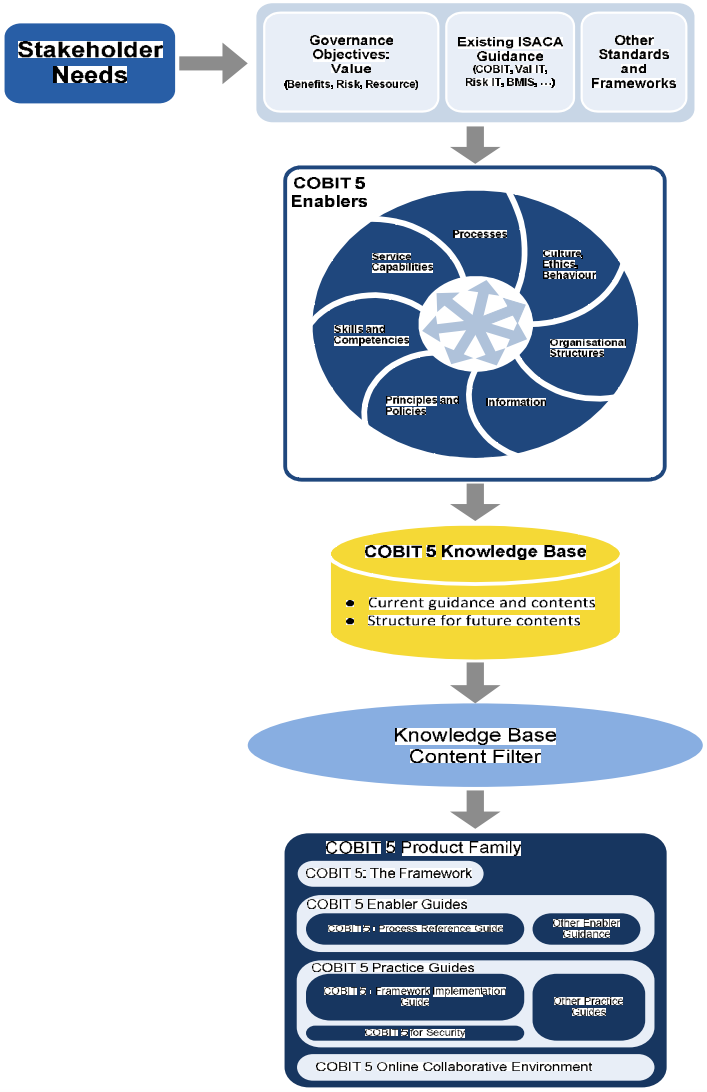
The COBIT 5 Framework

- An initial publication introduces, defines and describes the components that make up the COBIT Framework
  - Principles
  - Architecture
  - Enablers
  - Introduction to implementation guidance and the COBIT process assessment approach

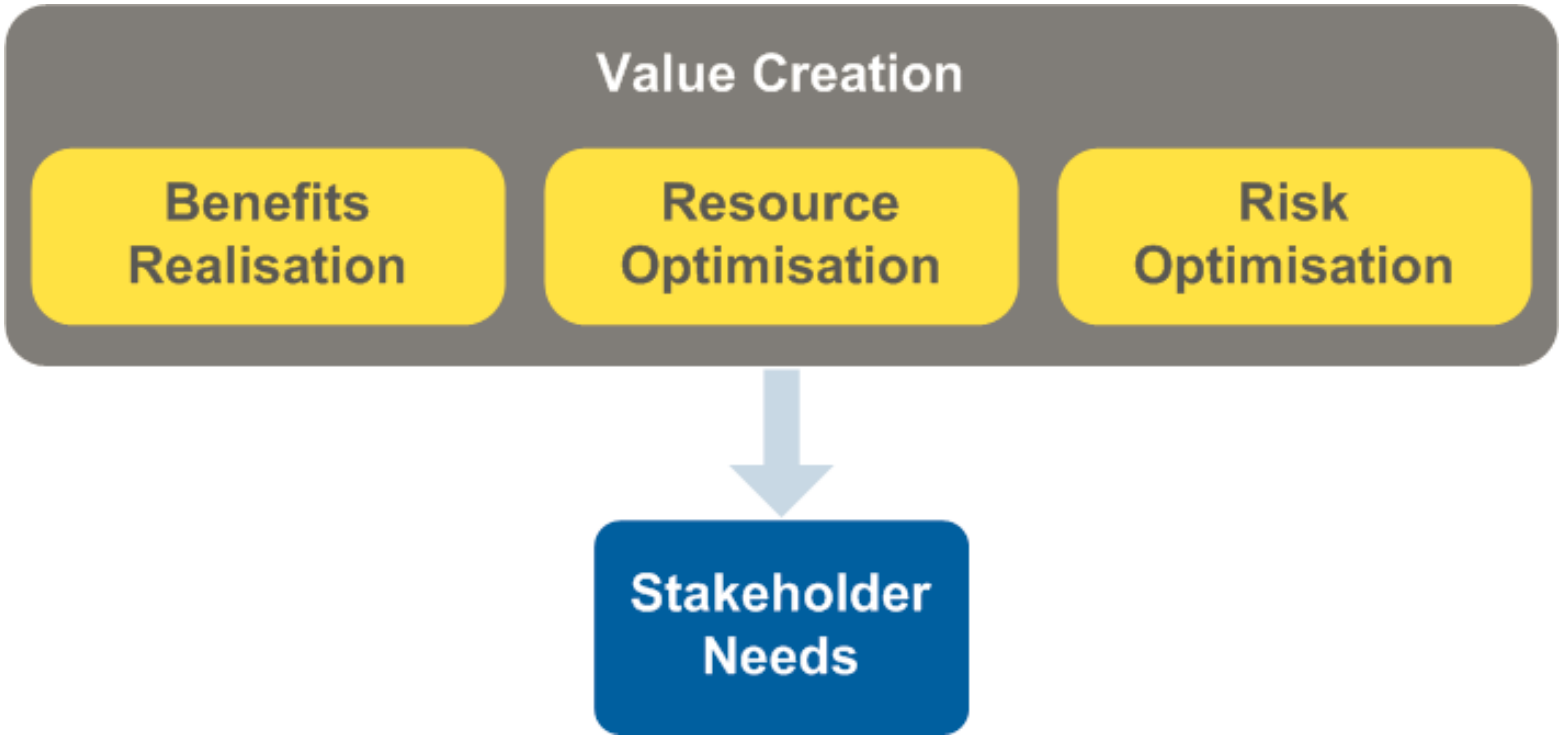
COBIT 5 Principles



COBIT 5 Architecture



Governance Objective



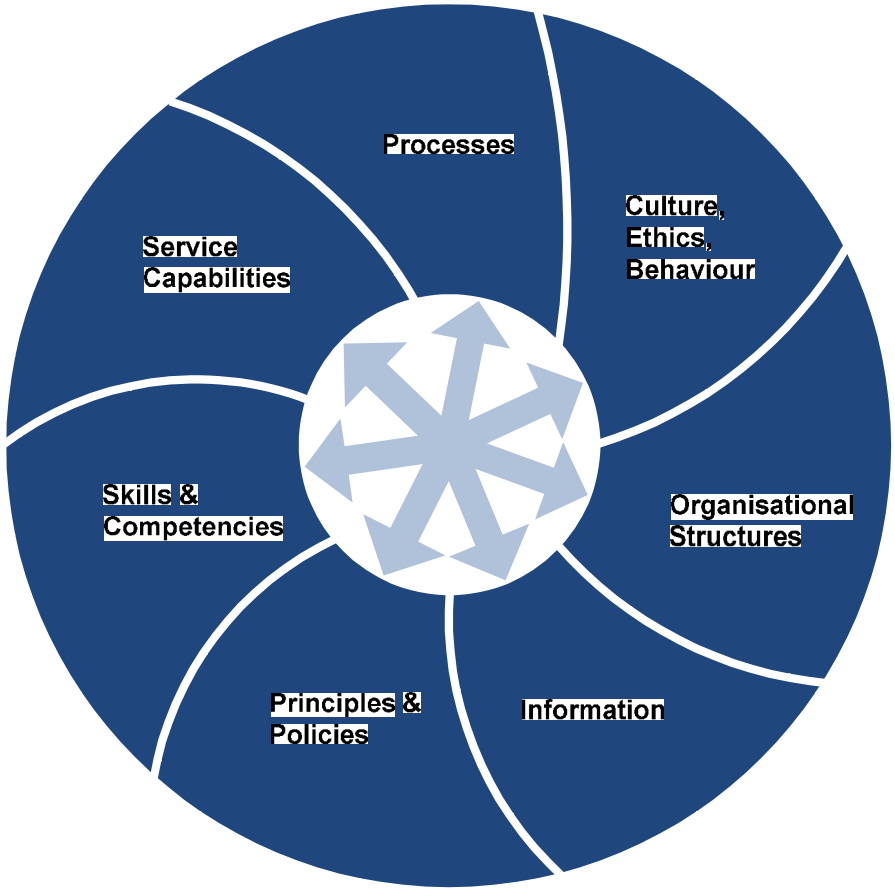
Benefits of Using COBIT 5

- **Enterprisewide benefits:**
  - **Increased value creation through effective governance and management of enterprise information and technology assets**
  - **Increased business user satisfaction with IT engagement and services–IT seen as a key enabler.**
  - **Increased compliance with relevant laws, regulations and policies**
- **IT function becomes more business focused**
- **Increases the COBIT 5 users' contribution to the enterprise**

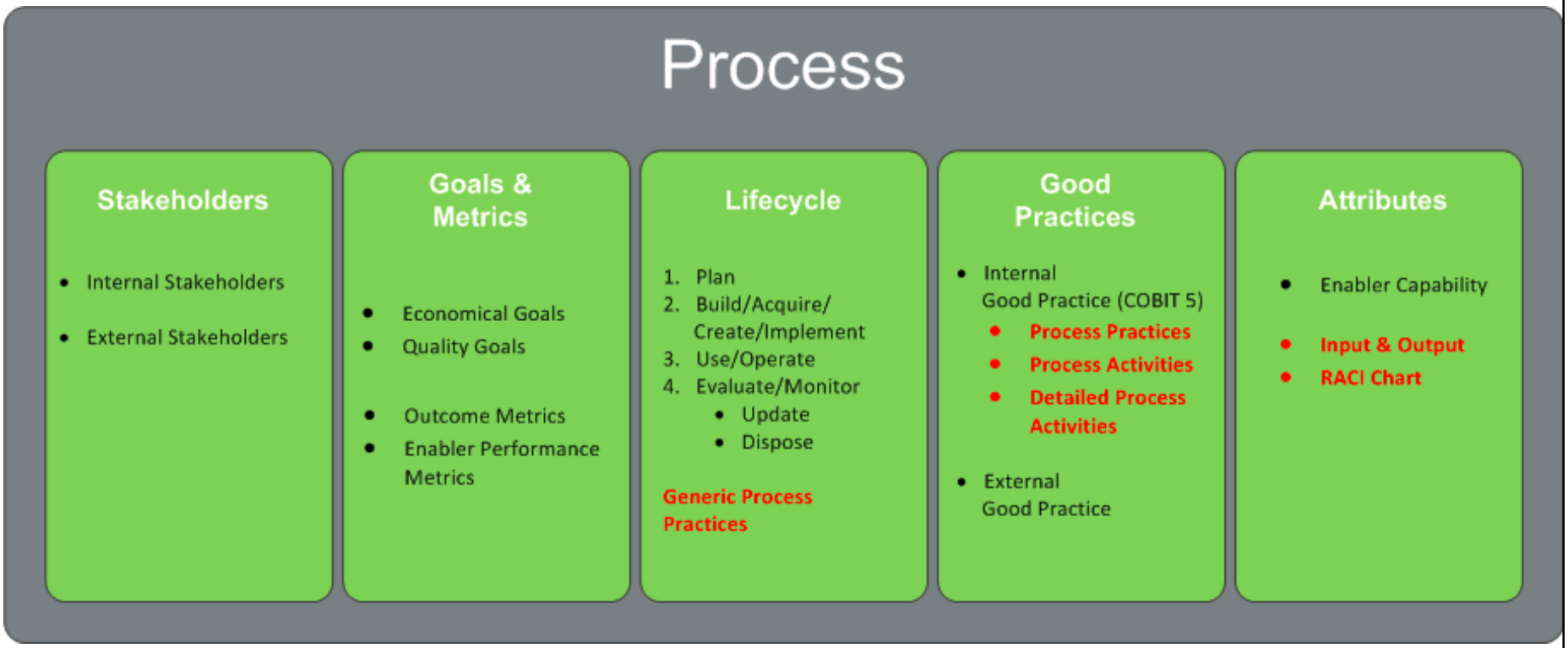
Enabler-based

ISACA
Trust in, and value from, information systems

COBIT 5 Enablers—Systemic Model With Interacting Enablers



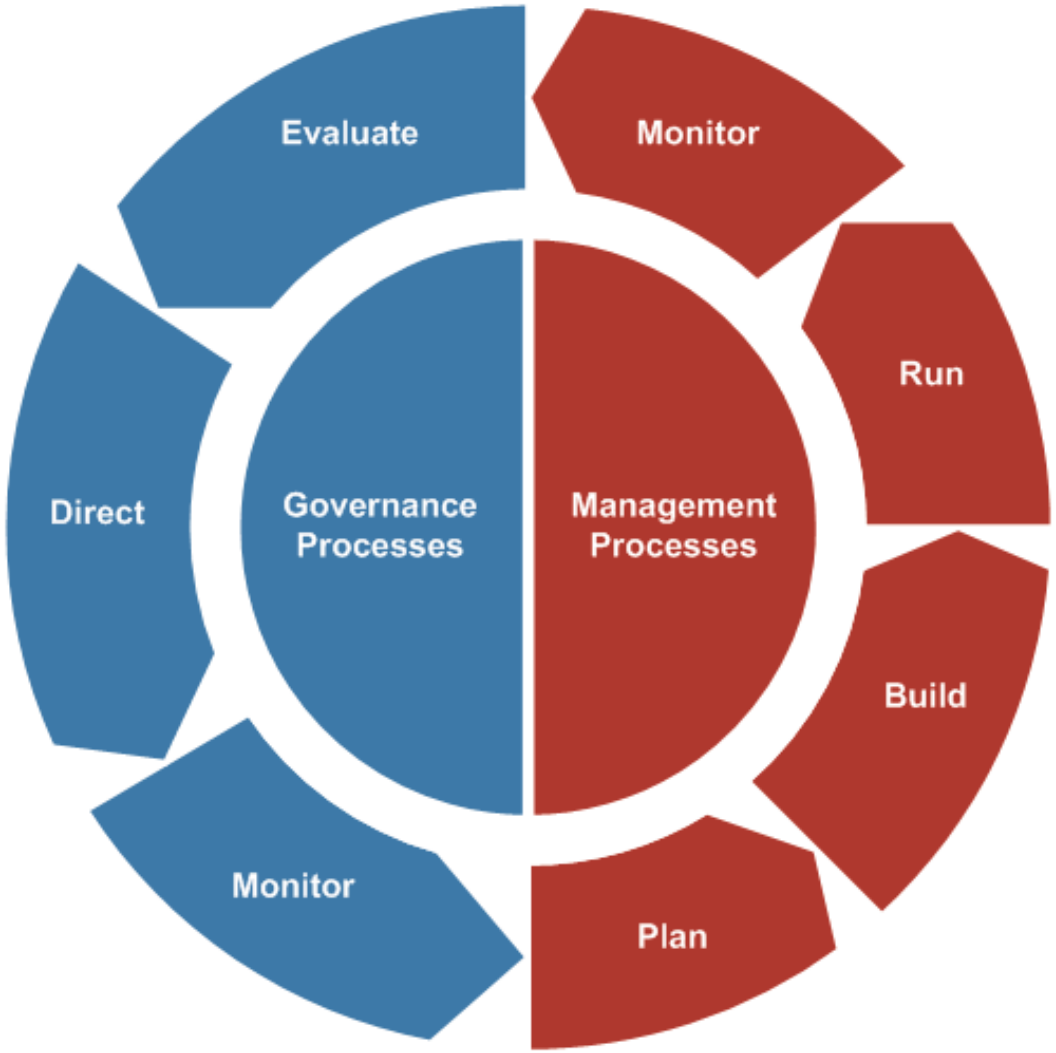
Process Enabler Model



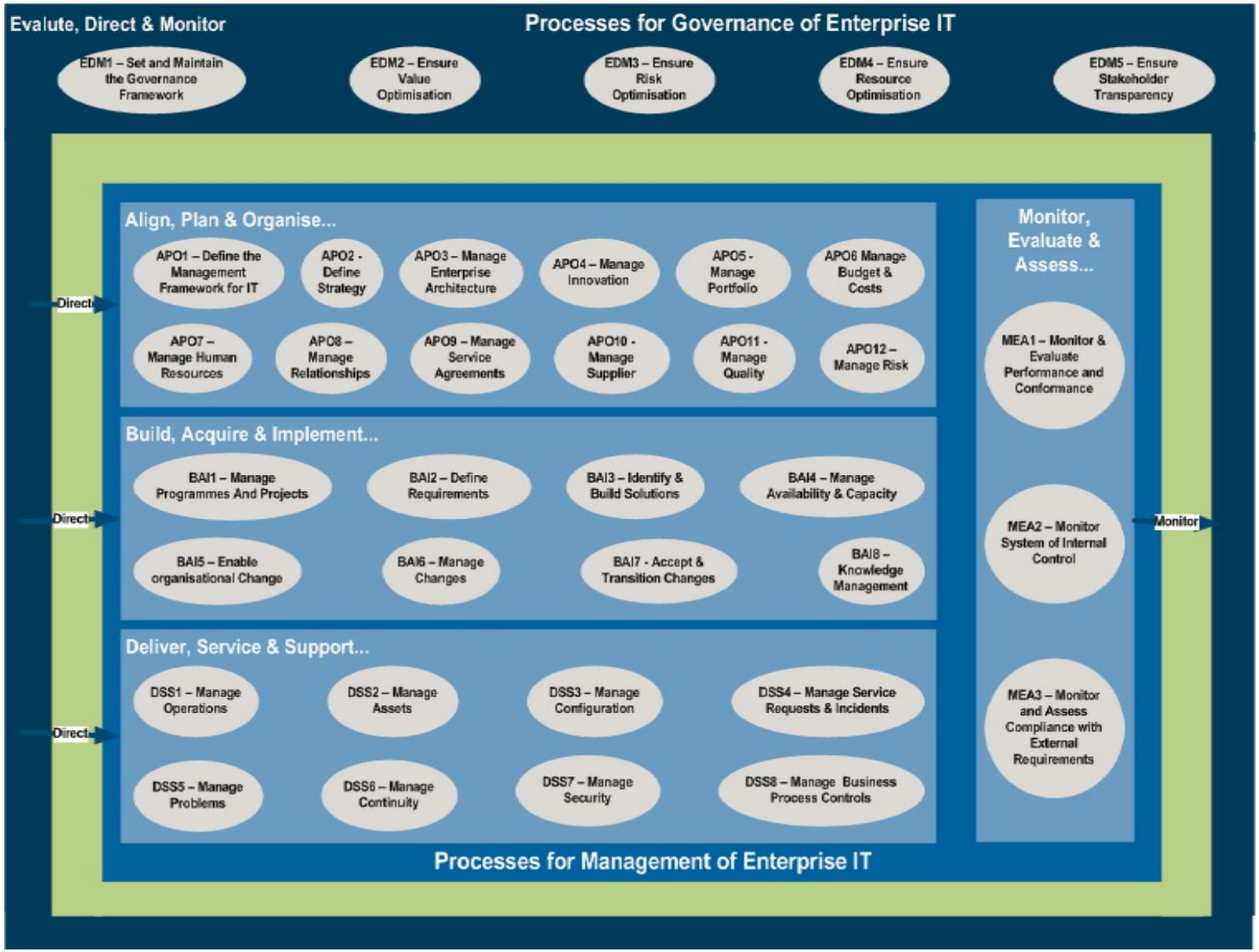
Process Reference Guide

- A separate publication that expands on the process-enabler model
- Contains full details of the COBIT processes in a similar way to the process documentation in COBIT 4.1

Governance and Management Processes

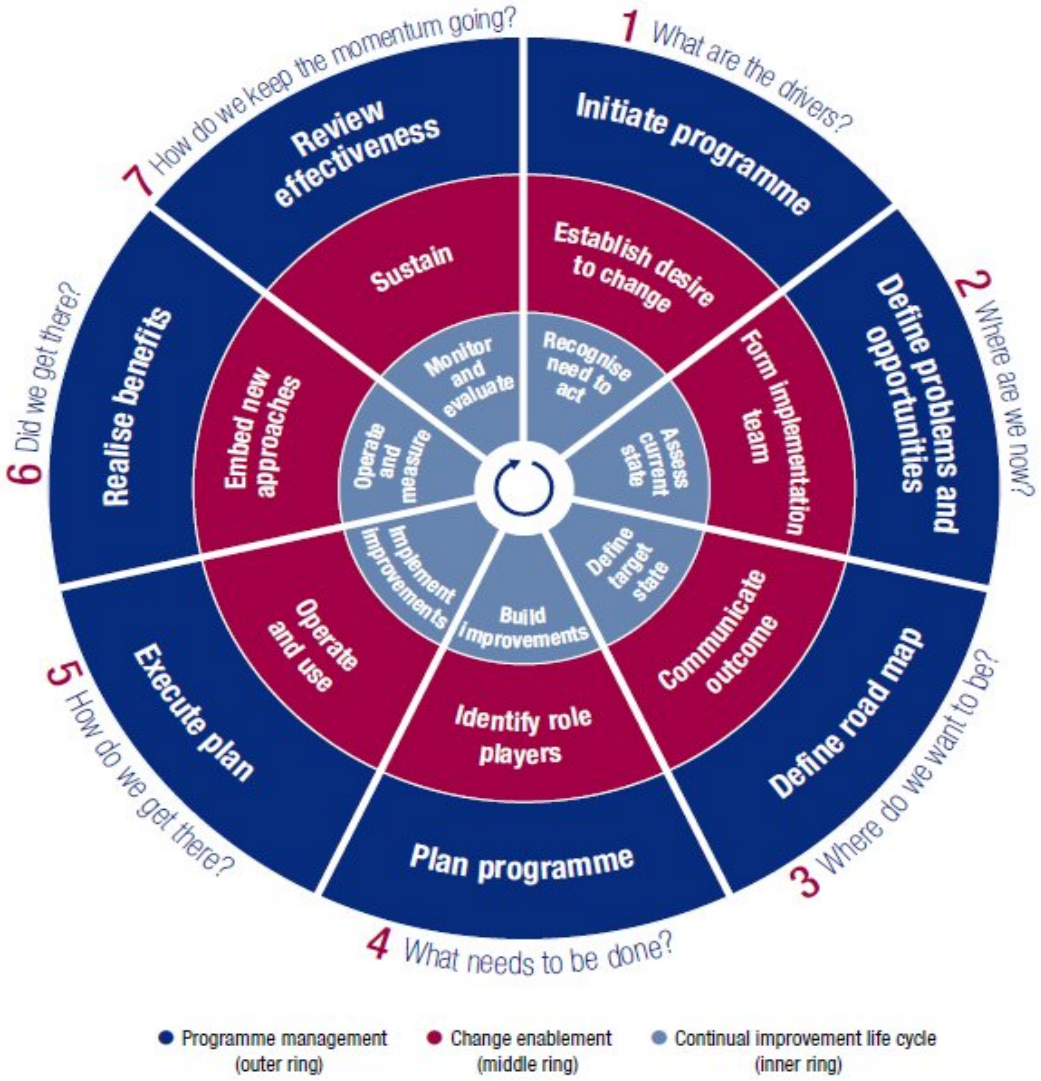


Process Reference Model



How many processes now? 36!

Implementation Guidance



- A separate publication
- Based on the current implementation guidance publication

On COBIT Process Capability assessment

- The process maturity model of COBIT 4.1 has been replaced with a capability model based on ISO/IEC 15504 to align with and support a separate ISACA initiative, the COBIT Assessment Program (CAP).
- There are a number of benefits in doing so:
  - Focus first on confirming that a process is achieving its intended purpose and delivering its required outcomes as expected.
  - Simplification of the content supporting process assessment.
  - Improved reliability and repeatability of process capability assessment activities and evaluations, reduced debates and disagreements between stakeholders on assessment results. Increased usability of process capability assessment results, as the new approach establishes a basis for more formal, rigorous assessments to be performed, for both internal and potential external purposes.
  - Compliance with a generally accepted process assessment standard and therefore strong support for process assessment approach in the market.

Process Capability Model Comparison

ISACA
Trust in, and value from, information systems

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.	

Moving Forward

- COBIT 5 is a major, high-profile, strategic initiative for ISACA. Market validation of the development work (i.e., the public exposure of the Framework and Process Reference Guide products) is planned for 27 June and to run throughout July to ensure that ISACA remains on the right track to satisfy market needs.
- SME exposure of the implementation guidance will follow later in 2011.
- Delivery of all three products to the market is planned for early 2012.

COBIT 5 News

- As the initiative progresses throughout 2011 and 2012 there will be periodic updates provided:
  - ✓On the ISACA web site, *www.isaca.org/COBIT5*
  - ✓In the *COBIT Focus* newsletter
  - ✓In other ISACA membership communications, events, marketing materials and PR activities
- Watch these spaces for more news!

Thank you

Contact details:

Robert E Stroud CGEIT

Email: Robert.Stroud@ca.com

Phone: (631) 880 2544

BLOG: www.ca.com/blogs/stroud

Twitter: www.twitter.com\RobertEStroud

Thank you!

ISACA®
Trust in, and value from, information systems