



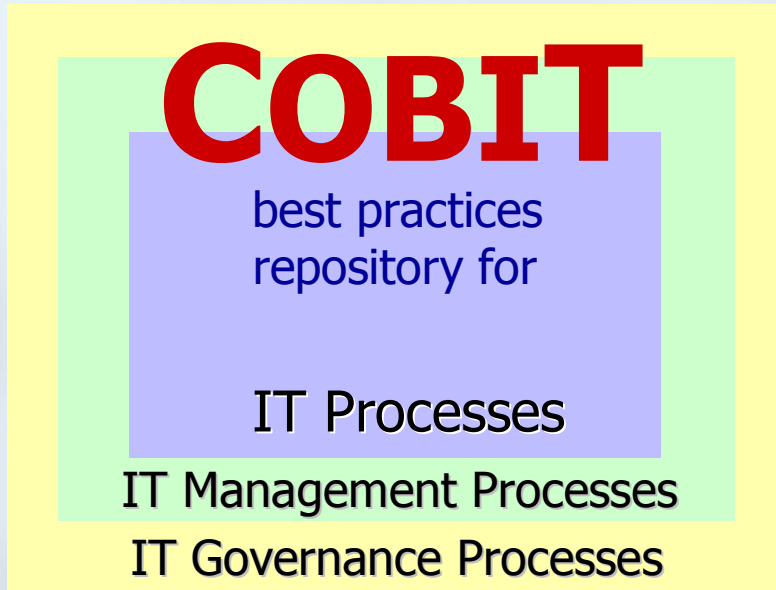
COBIT® : IT Governance Overview and ITIL V3 Mapping

AGENDA



- **What is COBIT®? An Overview.**
- **The ITGI Governance Framework.**
- **COBIT® and ITIL V3 Mapping.**
- **Integration of COBIT® with other frameworks.**
- **Assessing IT management capability using the COBIT® Maturity Model and Control Objectives.**
- **Reference tools, materials and thought leadership available through ISACA and ITGI.**

COBIT 4.1 – The IT Governance Framework



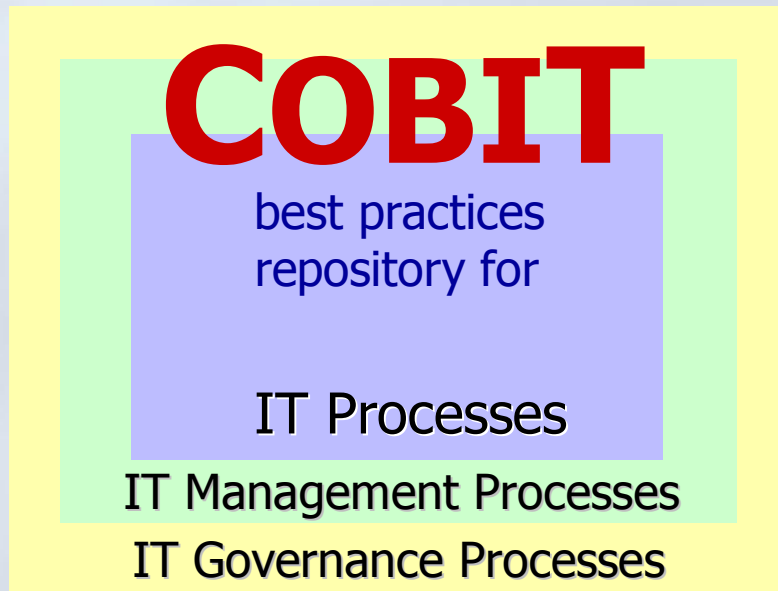
The *only* IT management and control framework that covers the end-to-end IT life cycle

- Internationally accepted good practices
- Management-oriented
- Supported by tools and training
- Freely available
- Sharing knowledge and leveraging expert volunteers
- Continually evolving
- Maintained by reputable not-for-profit organisation
- Maps 100 percent to COSO
- Maps strongly to all major related standards

COBIT 4.1 – The IT Governance Framework



- Is a reference, set of best practices, *not* an “off-the-shelf” cure
- Enterprises still to need to analyse their control requirements and customise based on:
 - Value drivers
 - Risk profile
 - IT infrastructure, organisation and project portfolio



Developed by the Leaders in IT Governance



Globally respected not-for-profit research institute established by ISACA in 1998 to advance international thinking and standards in directing and controlling IT.

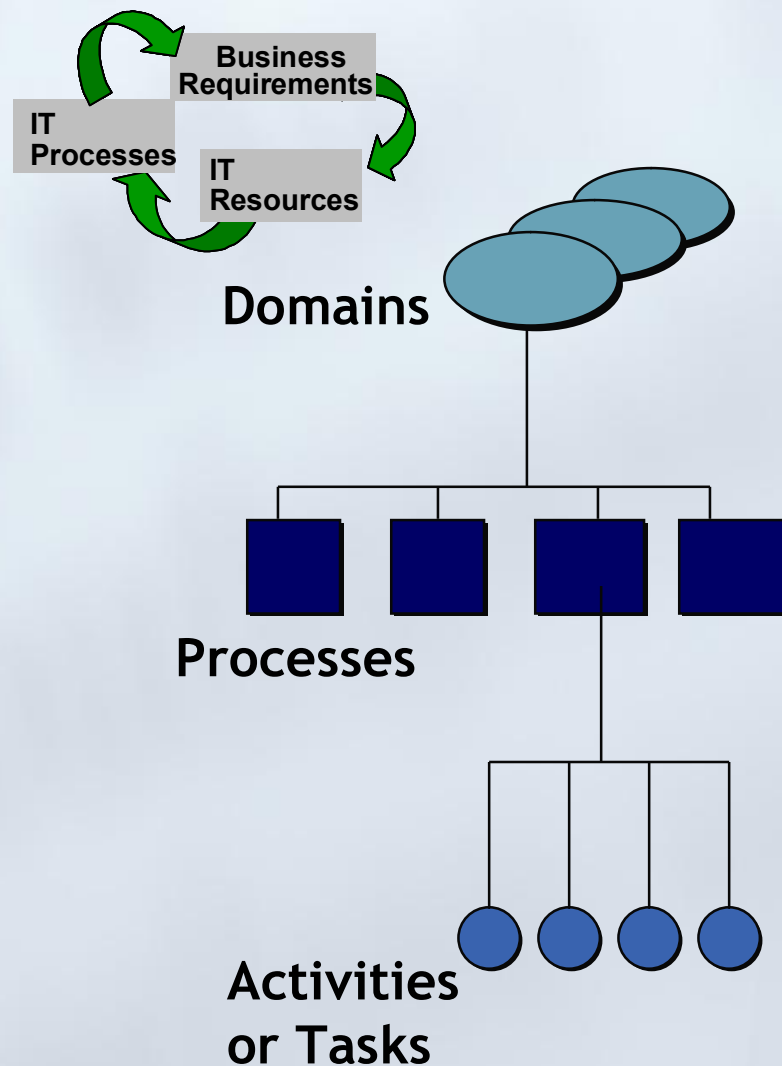


Professional association with 75,000 members. Worldwide leader in IT governance, control, security and assurance and offers the CISA, CISM and CGEIT certifications.



An Overview of COBIT®

Process Orientation



Natural grouping of processes, often matching an organisational domain of responsibility

A series of joined activities with natural control breaks

Actions needed to achieve a measurable result—activities have a life cycle whereas tasks are discrete

Process Orientation



IT Domains

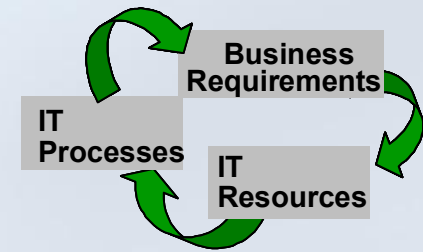
- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Natural grouping of processes, often matching an organisational domain of responsibility

IT Processes

- IT strategy
- Computer operations
- Incident handling
- Acceptance testing
- Change management
- Contingency planning
- Problem management

A series of joined activities with natural (control) breaks

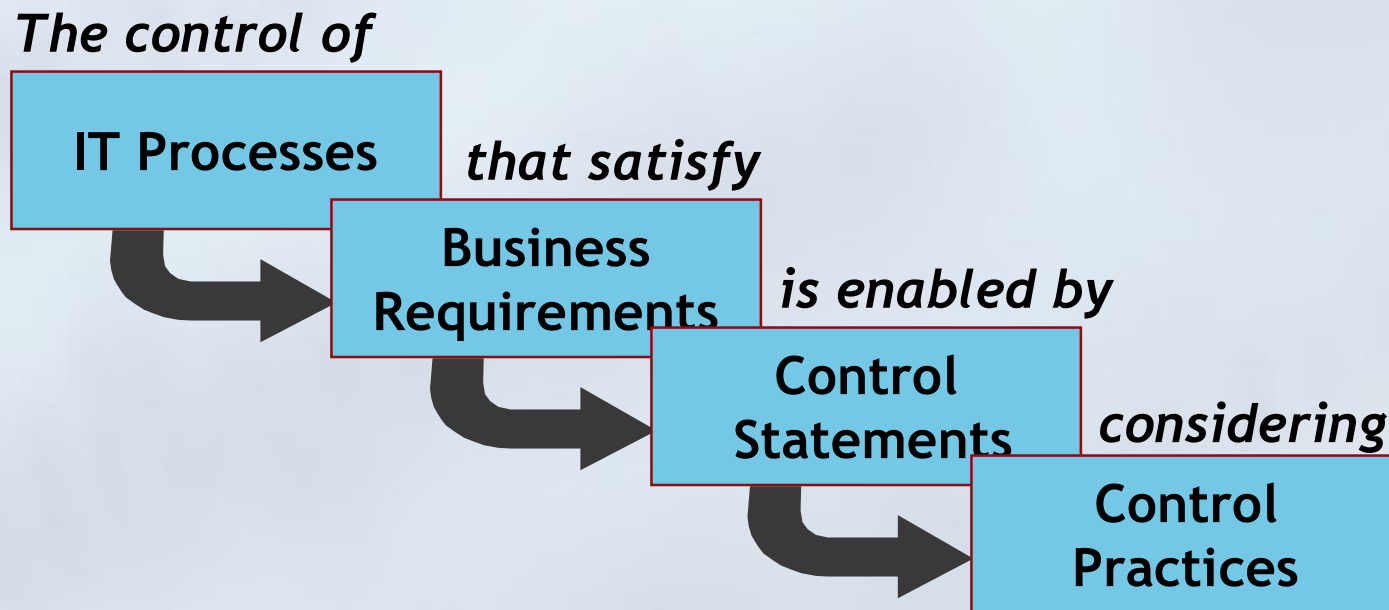


Activities

- Record new problem.
- Analyse.
- Propose solution.
- Monitor solution.
- Record known problem.

Actions needed to achieve a measurable result—activities have a life cycle whereas tasks are discrete

Waterfall Model



4 Domains - 34 Processes - 210 Control Objectives

COBIT® Framework

Business Objectives



Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources

- Data
- Application Systems
- Technology
- Facilities
- People

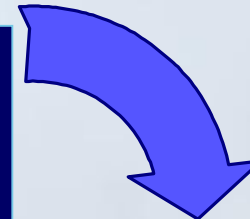
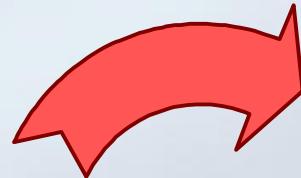
Monitor and Evaluate

Plan and Organise

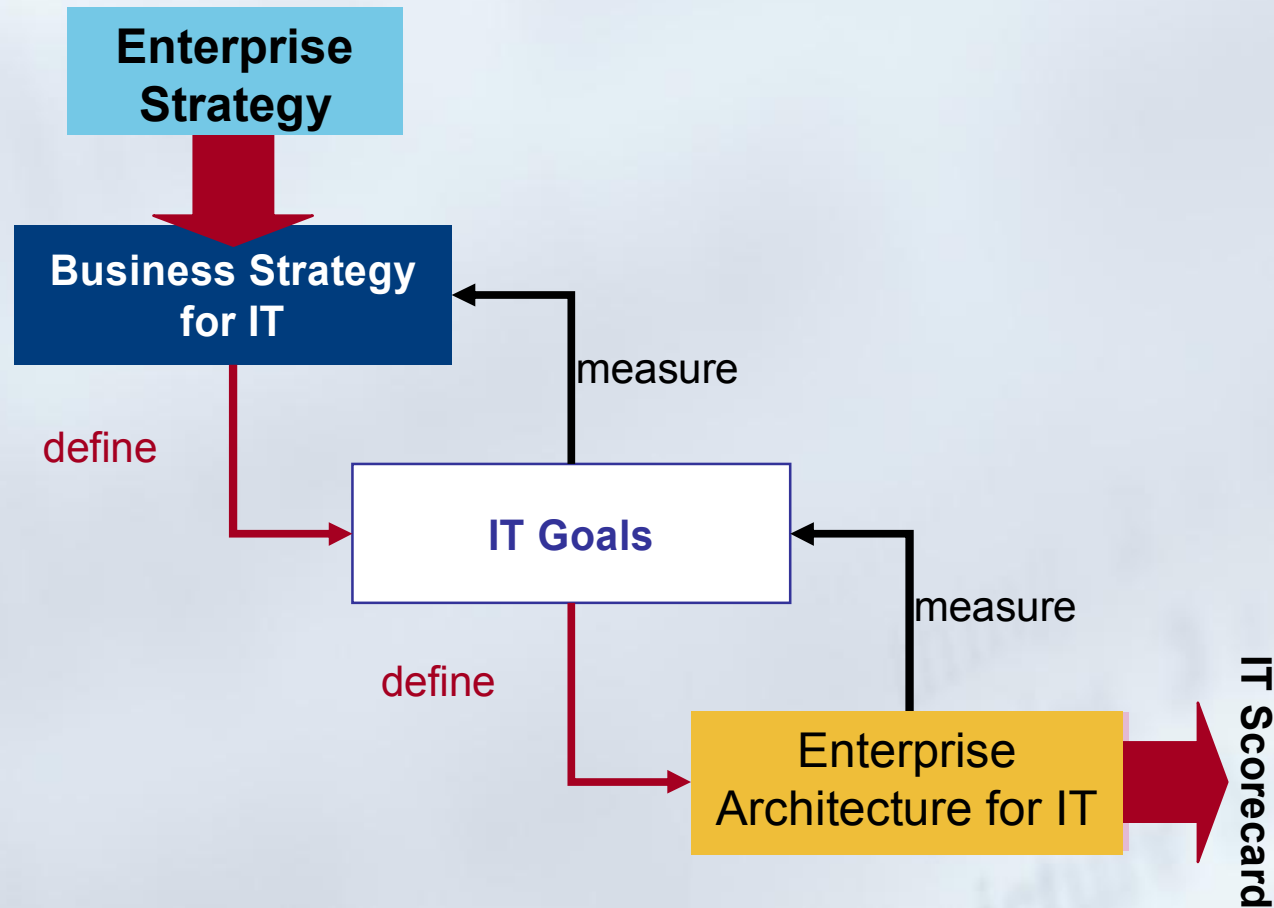
Deliver and Support

Acquire and Implement

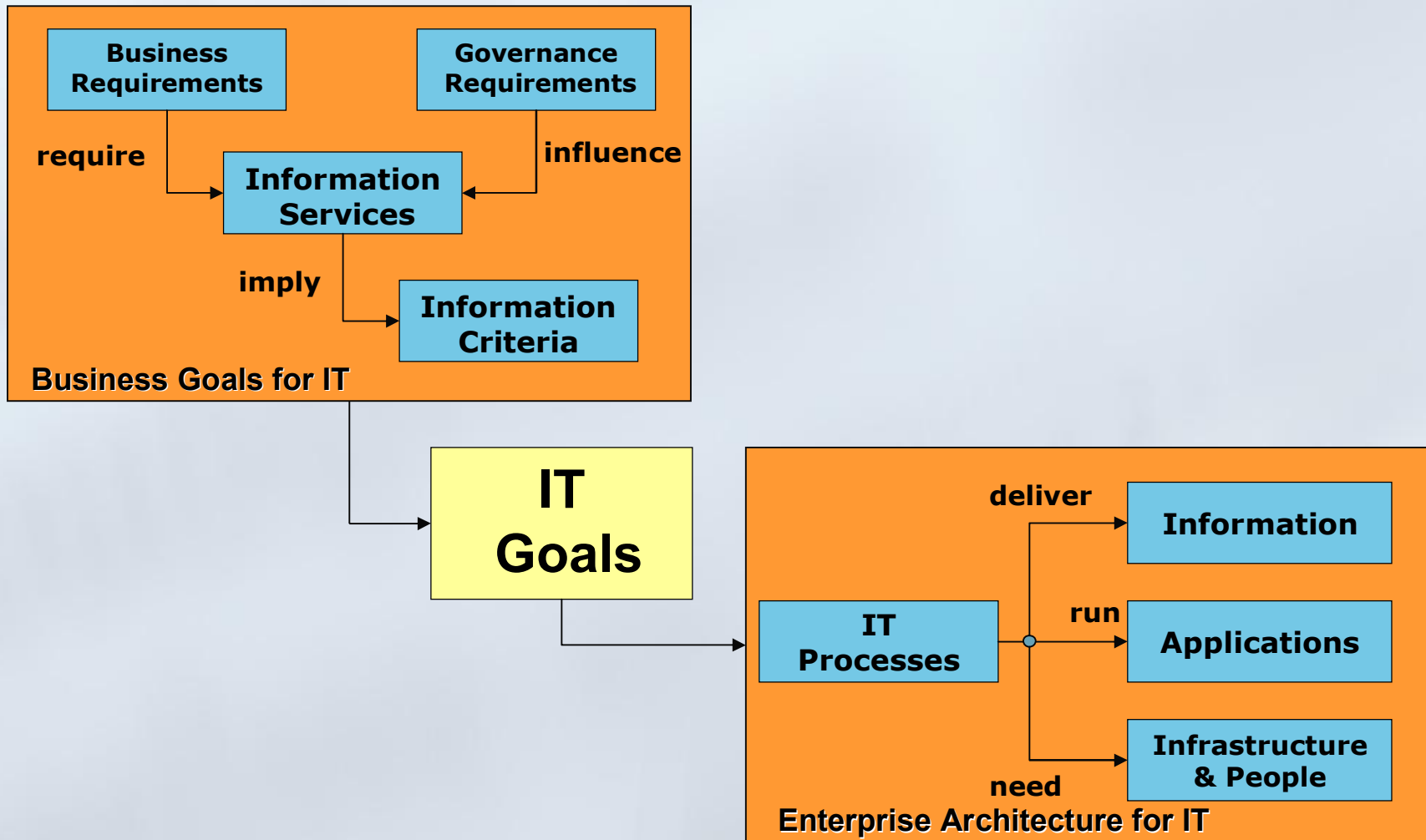
IT Life Cycle



Top-down approach



IT Process is derived from Business Goals



IT Governance

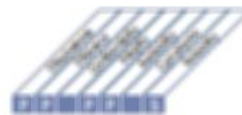


Acquire and Implement Manage Change AI6

HIGH-LEVEL CONTROL OBJECTIVE

All Manage Change

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, systems and service parameters) must be logged, assessed and authorized prior to implementation and reviewed against planned releases following implementation. This ensures mitigation of the risk of negatively impacting the stability or integrity of the production environment.



- Final Types
- Acquire and Implement
- Internal report
- External Issues

Control over the IT process of Manage Change

That satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery delays and errors.

by focusing on

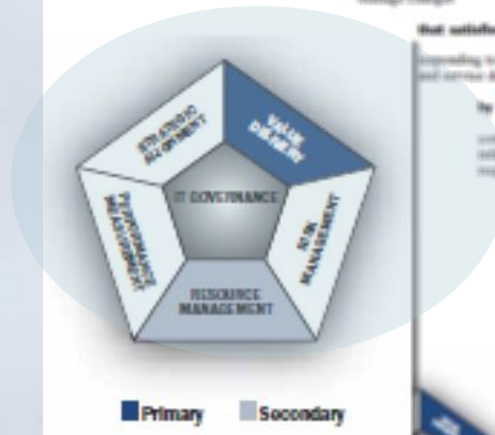
controlling request assessment, authorization and implementation of all changes to the IT infrastructure, applications and technical solutions, ensuring errors due to incomplete request specifications and faulty implementation of unauthorized changes.

is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritizing and authorizing changes
- Tracking status and reporting on changes

and is measured by

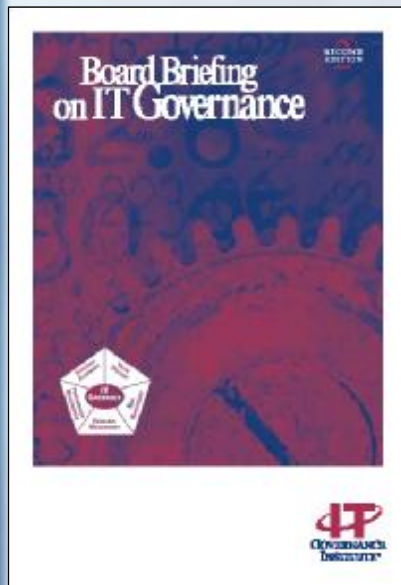
- Number of disruptions or data errors caused by incomplete specifications or incomplete request assessment
- Applications or infrastructure events caused by inadequate change specifications
- Percent of changes that follow formal change control processes





IT Governance

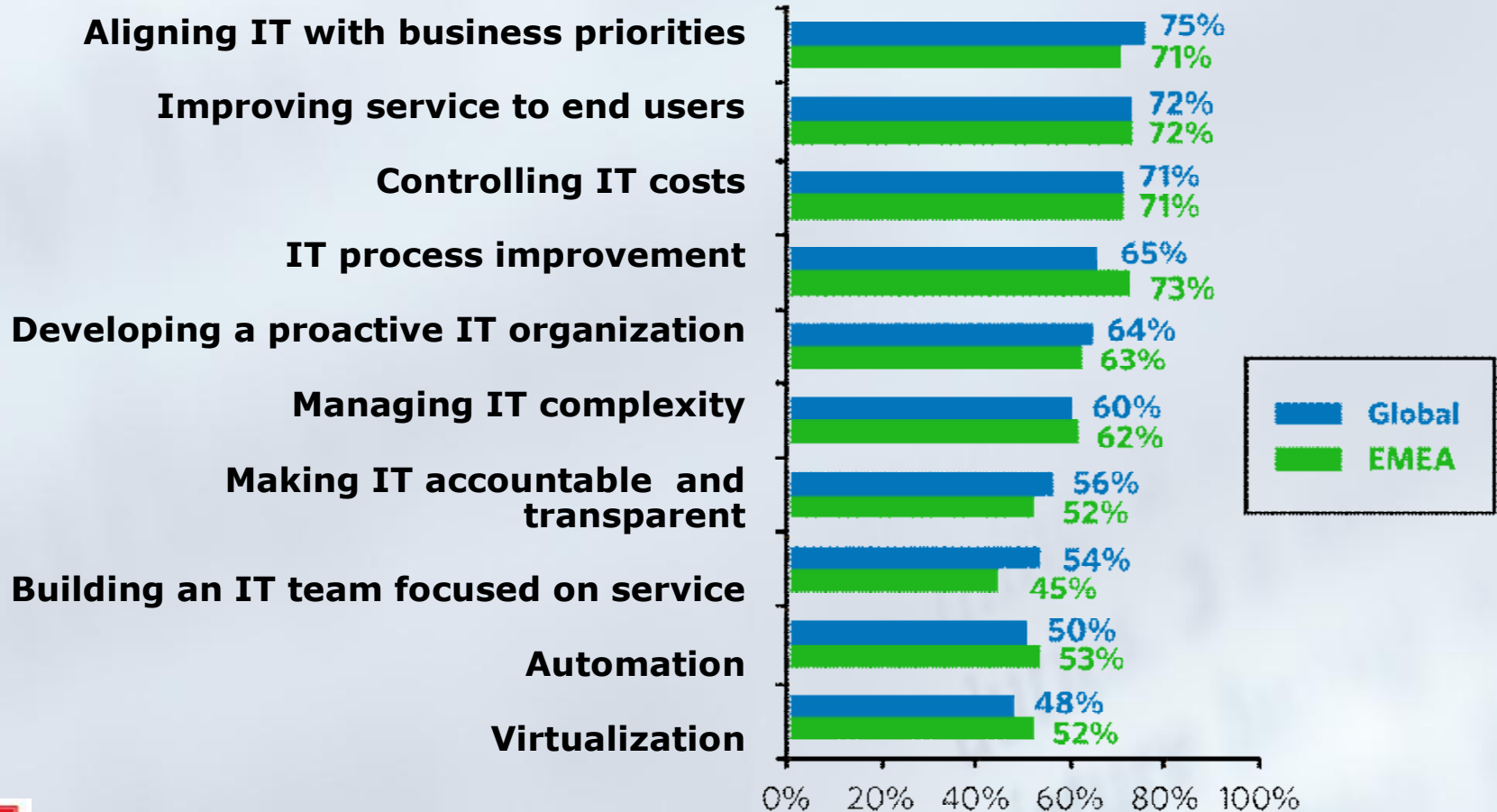
IT Governance



“**IT governance** is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.”

ITGI, Board Briefing on IT Governance

Forces Driving IT!



IT Governance Is the Key Issue



- Organizations are sacrificing money, productivity and competitive advantage by not implementing effective IT governance
- Executives need a better way to:
 - Direct IT for optimal advantage
 - Manage IT-related risks
 - Measure the value provided by IT



Five Focus Areas of IT Governance



FOCUS AREAS

1. Strategic Alignment

aligning with the business and providing collaborative solutions

2. Value Delivery

focus on IT costs and proof of value

3. Risk Management

safeguarding assets, business continuity and compliance

4. Resource Management

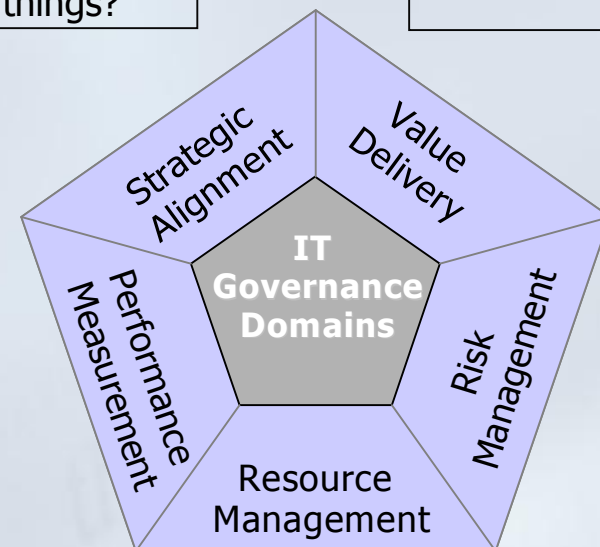
IT assets, knowledge, infrastructure and partners.

5. Performance Measurement

metrics, IT Scorecards and dashboards

Are we doing the right things?

Are we getting the benefits?



Are we doing them the right way?

Are we getting them done well?

COBIT® is a Road Map to Good IT Governance



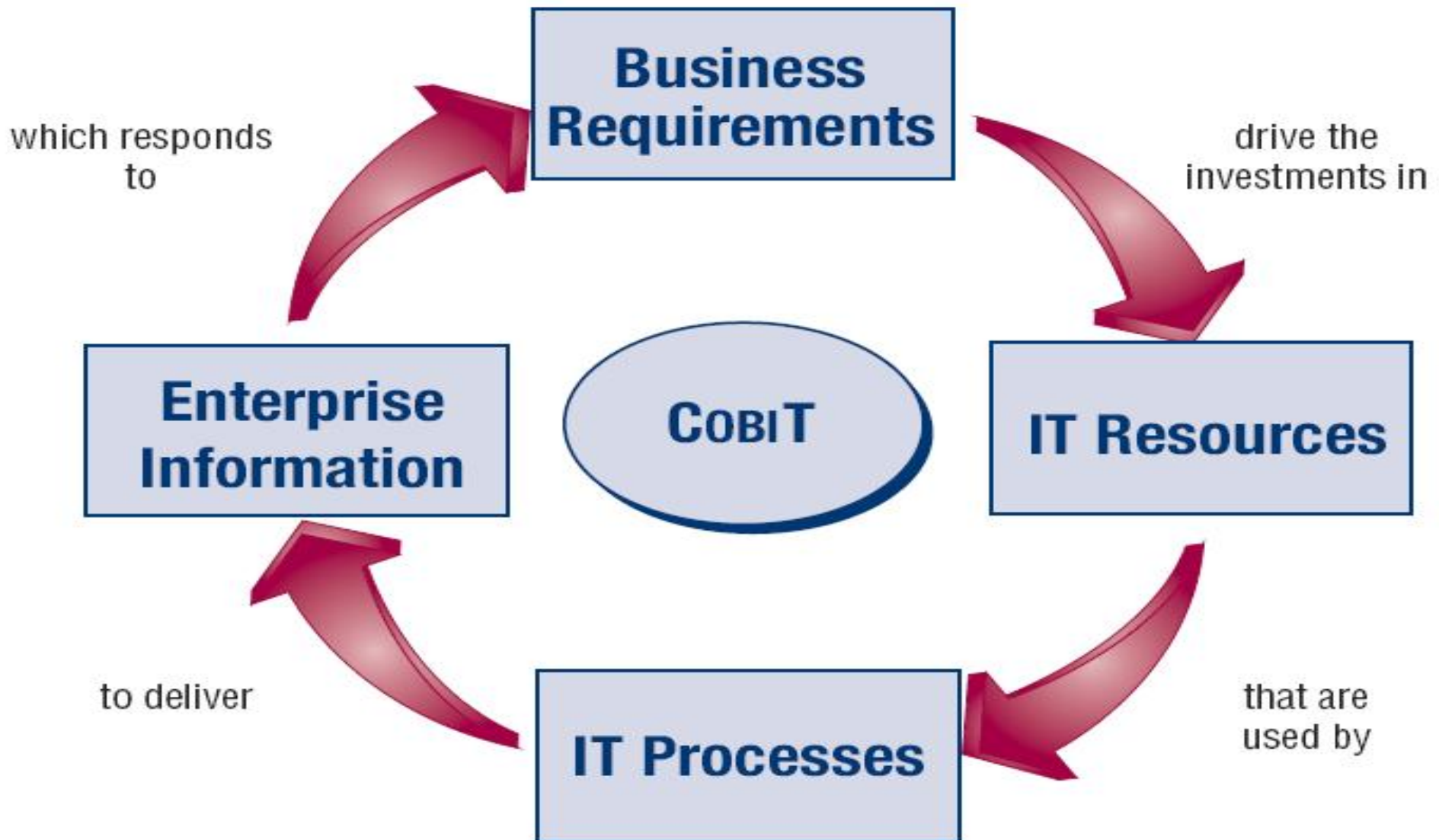
- Globally accepted set of tools that ensures IT is working effectively
- Provides common language to communicate goals, objectives, expected results
- Based on industry standards and good practices in:
 - Strategic alignment of IT with business goals
 - Value delivery of services and new projects
 - Risk management
 - Resource management
 - Performance measurement

The COBIT logo, consisting of the word 'COBIT' in a bold, blue, sans-serif font with a red oval behind the letter 'O'. The logo is set against a background of a dotted pattern.

Harmonizing IT Governance



Governance Lifecycle





COBIT® and mapping to other Frameworks (i.e. ITIL V3)

COBIT Mapping Project



Mapping of ITIL®
With COBIT® 4.0



LEADING THE IT GOVERNANCE COMMUNITY

- TOGAF (Architecture)
- COSO ERM
- GBPM
- FFEIC (US banking)
- NIAC (Insurance)
- NIST SP800-53
- FISMA
- IAIS Framework (Solvency II)
- HIPAA (Health Insurance)
- GLBA (Privacy)
- ISO19770-1 (SW Asset Mgmt)
- ISO 20000 (Service Mgmt)
- ISO 27005 (Risk Mgmt)
- ISO 27002 (ISO17799)

COBIT Mapping with ITIL V3



COBIT MAPPING

Mapping of ITIL v3
With COBIT® 4.1



LEADING THE IT GOVERNANCE COMMUNITY

COBIT and ITIL V3 mapping



Figure 7 is an overview of ITIL V3 and COBIT and highlights the differences of the guidance.

Figure 7—ITIL V3 Processes Mapped to High-level COBIT Processes

COBIT 4.1 Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise	o	-	-	o	o	-	-	o	o	-	/	/	/
Acquire and Implement	o	o	o	o	o	+	+	/	/	/	/	/	/
Deliver and Support	+	o	+	o	o	+	-	+	+	+	o	o	o
Monitor and Evaluate	o	-	-	-	/	/	/	/	/	/	/	/	/
Process Controls	-	o	-	o	+	/	/	/	/	/	/	/	/
Application Controls	o	o	o	o	o	+	/	/	/	/	/	/	/

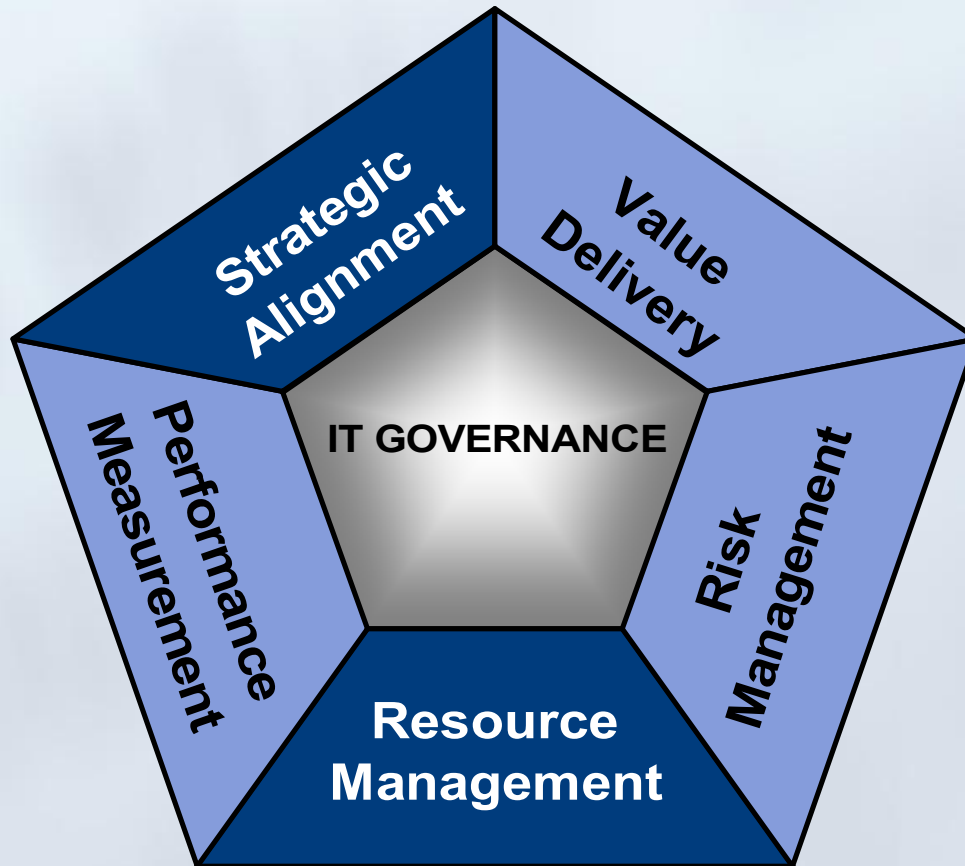
- (+) Significant match (more than two objectives were mapped to a COBIT process)
- (o) Minor match (one or two objectives were mapped)
- (-) Unrelated focus (no objective was mapped)
- (/) COBIT IT process does not exist




COBIT and ITIL Mapping



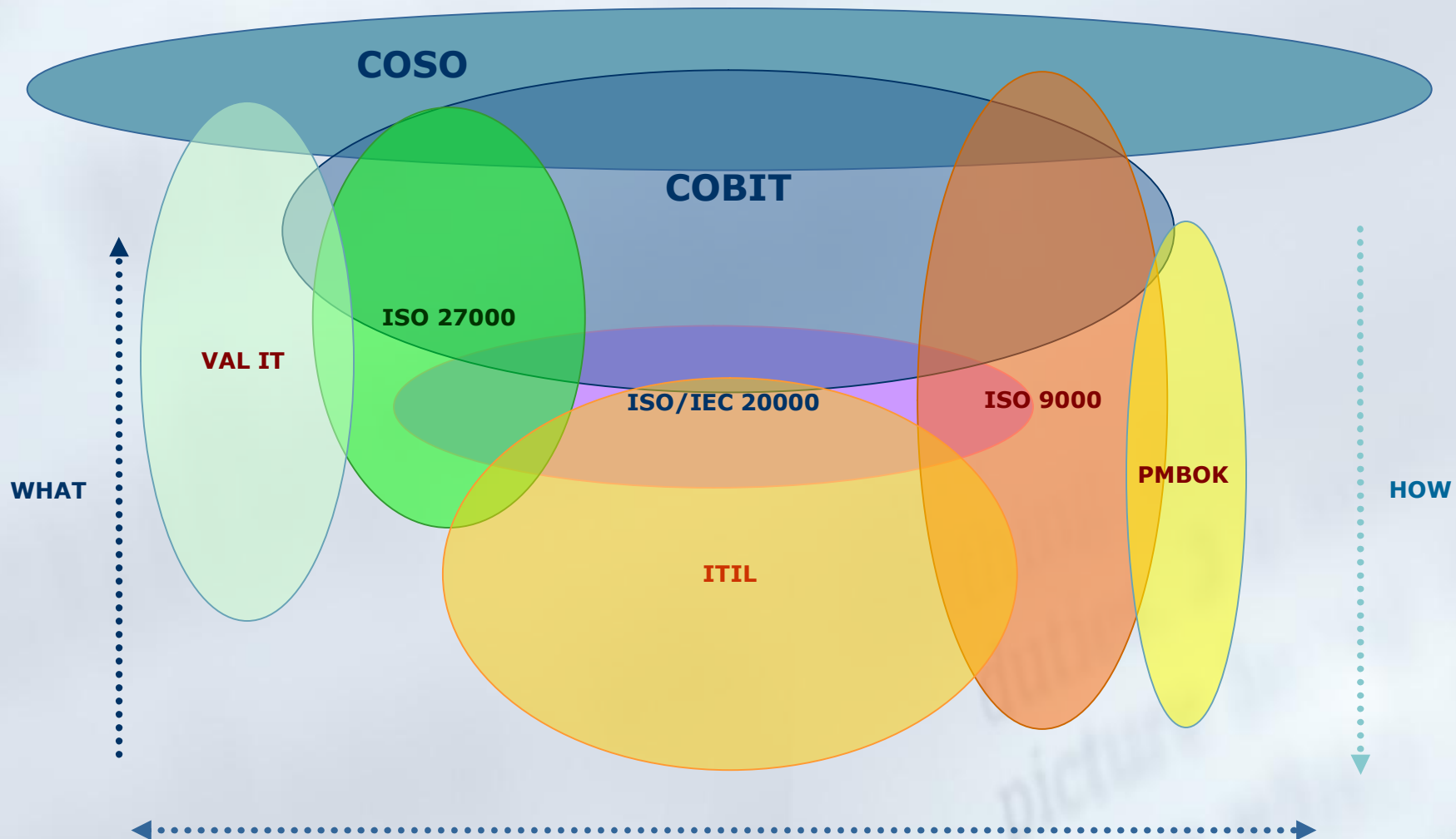
COBIT		ITIL	Coverage
Control Objective	Name		
PO1	Define a Strategic IT Plan	SS 1 Introduction SS 2 Service management as a practice SS 3 Service Strategy principles SS 3.5 Service Strategy fundamentals SS 4 Service strategy ...	A+
PO1.1	IT Value Management	SS 2.2 What are services? SS 3.1 Value creation SS 3.4 Service structures SS 4.4 Prepare for execution SS 5.1 Financial Management SS 5.2 Return on Investment SS 5.3 Service Portfolio Management	C
PO1.2	Business-IT Alignment	SS 2.1 What is service management SS 2.3 The business process SS 2.4 Principles of service management	C
PO1.3	Assessment of Current Capability and Performance	SS 4.4 Prepare for execution CSI 5.2 Assessments	C
PO1.4	IT Strategic Plan	SS 3.3 Service provider types SS 3.5 Service Strategy fundamentals SS 4.1 Define the market SS 4.2 Develop the offerings SS 4.3 Develop strategic assets ...	C
PO1.5	IT Tactical Plans	SS 4.4 Prepare for execution SS 7.1 Implementation through the lifecycle SS 7.2 Strategy and Design ...	C

Focus Area's addressed with COBIT and ITIL

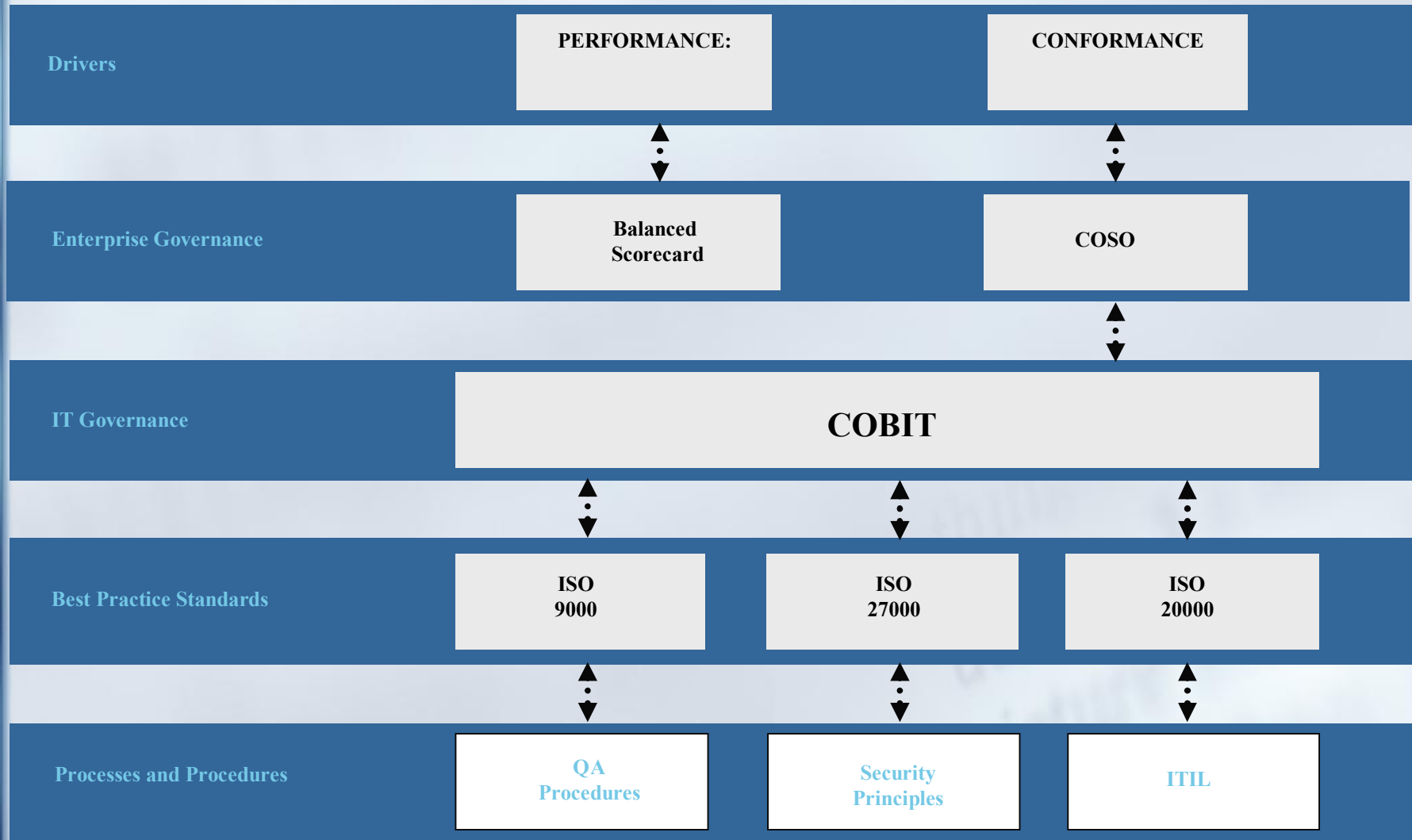


-  Primary
-  Secondary
-  Not Addressed

Governance and Frameworks



Governance Mapping



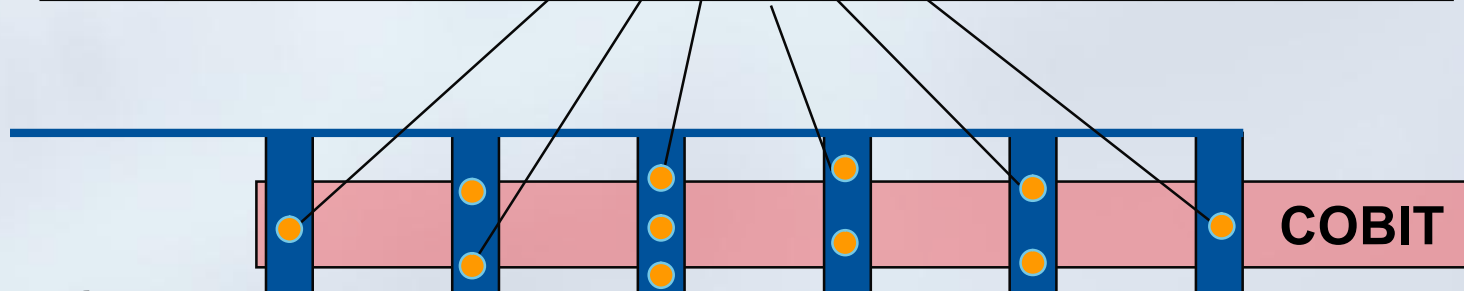
Comprehensive Approach



Governance



Measurement

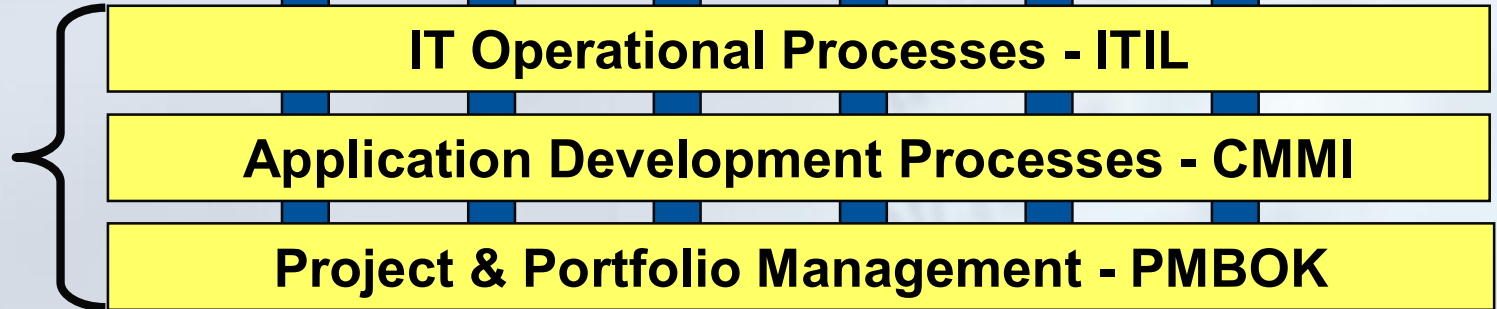


Align with roles

RACI
Responsible, Accountable, consulted and informed

Release Management: Roles/Responsibilities by Major Department/Work Group	Plan	Build	Test	Deploy	Operate	Monitor	Review
Program Management Office							
Applications Development	X						
Operations Infrastructure	X						
Operations Management							
Service Desk							
Change Mgmt Staff	X						
Production Ops							
Technical Ops							
System Admin							
System Support							

Establish the work





Overview of COBIT® Maturity Model (CMM)

Assessing IT Governance



Overview of the COBIT Maturity Model (CMM)

- Excellent approach to evaluating the current state environment against established criteria and developing a set of recommendations to achieve desired future state
- Uses a scale of 0 through 5 to measure the maturity level of the area being assessed
- Do not assume that the desired state is always 5

Maturity Levels in CobIT



Nonexistent

Initial

Repeatable

Defined

Managed

Optimised

0

1

2

3

4

5

0 - Management processes are not applied at all.

1 - Processes are *ad hoc* and disorganised.

2 - Processes follow a regular pattern.

3 - Processes are documented and communicated.

4 - Processes are monitored and measured.

5 - Best practices are followed and automated.

COBIT® Maturity Model



AI6 Acquire and Implement Manage Changes

MATURITY MODEL

AI6 Manage Changes

Management of the 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 is:

0 Non-existent when

There is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial/Ad Hoc when

It is recognised that changes should be managed and controlled. Practices vary and it is likely that unauthorised changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive when

There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change.

3 Defined Process when

There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, and compliance is emerging. Workarounds take place and processes are often bypassed. Errors may still occur and unauthorised changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

4 Managed and Measurable when

The change management process is well developed and consistently followed for all changes, and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation are becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process redesign. There is a consistent process for monitoring the quality and performance of the change management process.

5 Optimised when

The change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control. Tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.

Dimensions of Process Maturity in COBIT®



We capture process maturity data on each of six dimensions:

- **Awareness and communication**
- **Policies, standards and procedures**
- **Tools and automation**
- **Skills and expertise**
- **Responsibility and accountability**
- **Goal setting and measurement**



Sample CMM Deliverables/Reports

Capability Function



	Process Area	Current Capability	2008 Target
PO1	Define a Strategic IT Plan	2.33	3
PO2	Define the Information Architecture	1.83	2
PO5	Manage the IT Investment	2.83	3
PO10	Manage Projects	3.33	4
DS7	Educate and Train users	2.17	3
DS3	Manage Performance and Capacity	2.50	3
DS11	Manage Data	3.00	4
ME1	Monitor and Evaluate IT Performance	2.17	3

Conducting an IT Governance Assessment



Maturity Scorecard

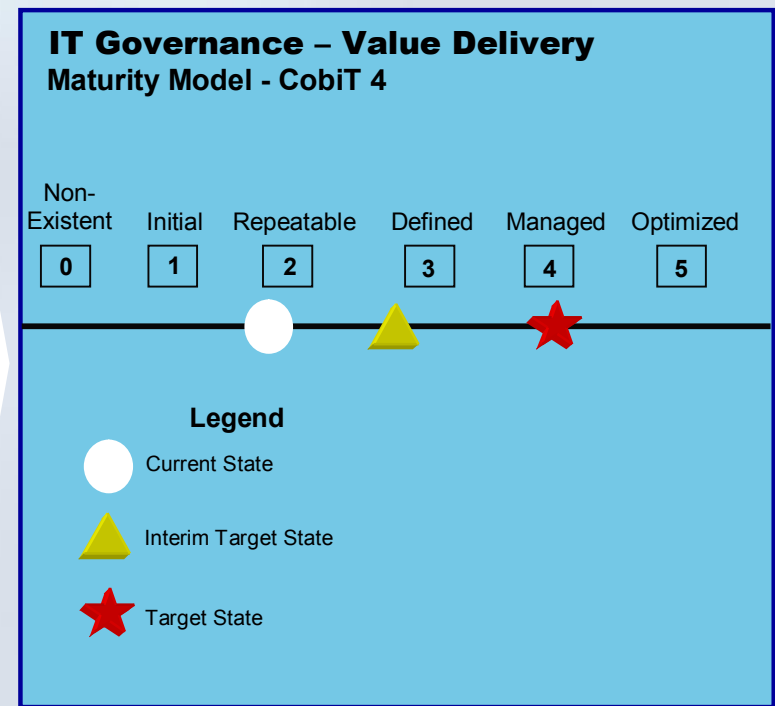
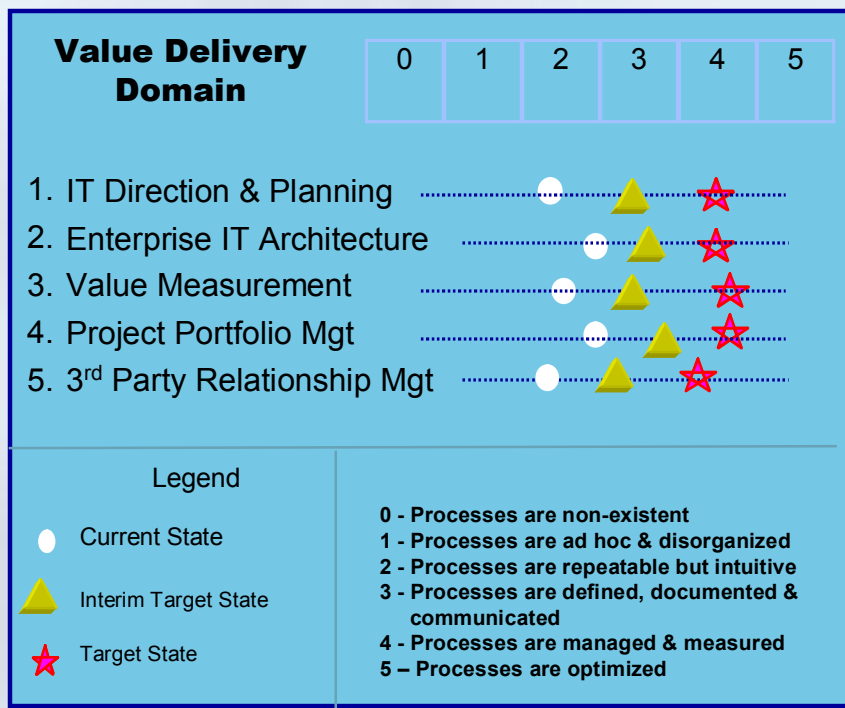
	Maturity Rating
o IT Governance Program and Framework	3.5*
Domains	
o Strategic Alignment	3.4
o Value Delivery	2.8
o Risk Management	3.4
o Resource Management	3.0
o Performance Management	3.2

- 0 - Processes are non-existent
- 1 - Processes are ad hoc & disorganized
- 2 - Processes are repeatable but intuitive
- 3 - Processes are defined, documented & communicated
- 4 - Processes are managed & measured
- 5 - Processes are optimized

Conducting an IT Governance Assessment

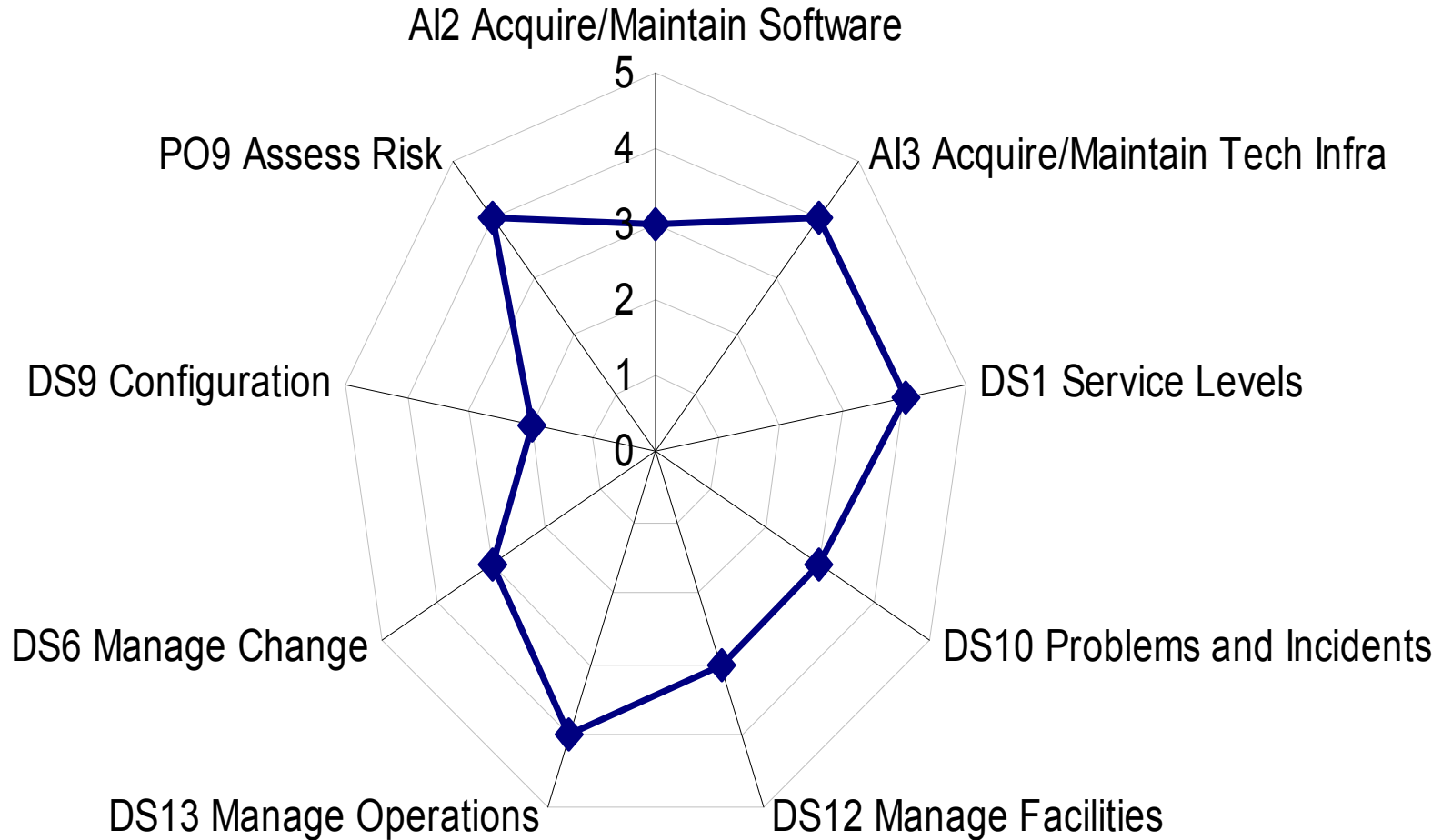


Sample Maturity Model for IT Governance - Value Delivery

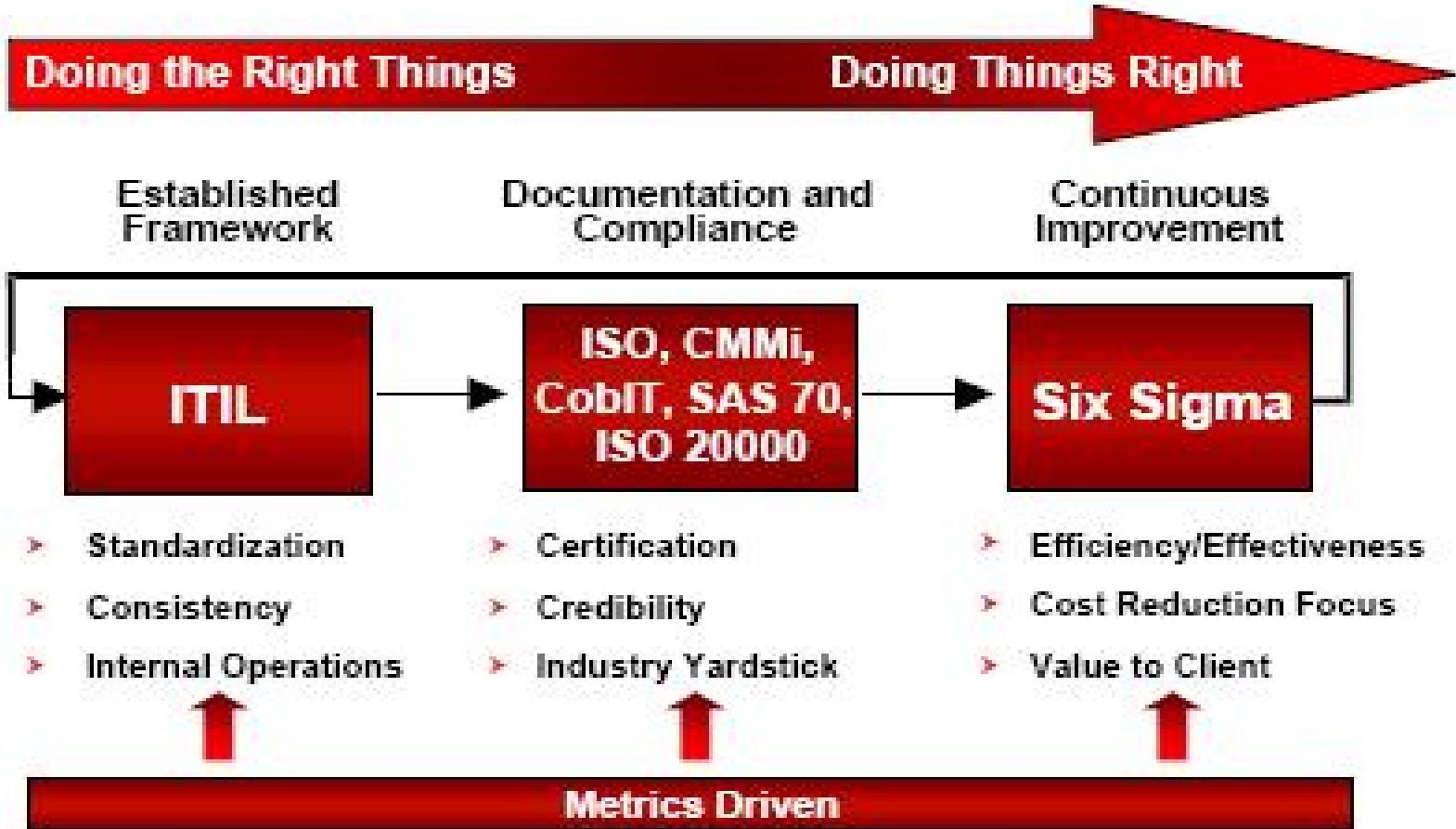


Example also in Appendix D (page 48) of Board Briefing on IT Governance booklet

COBIT Maturity Model



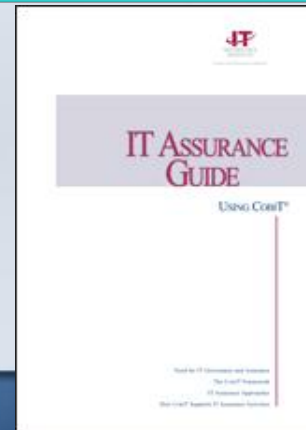
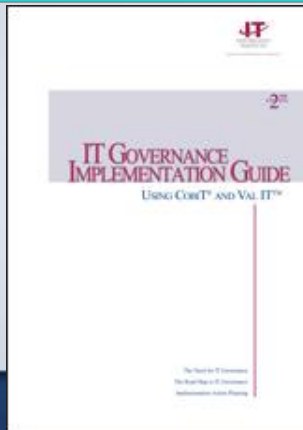
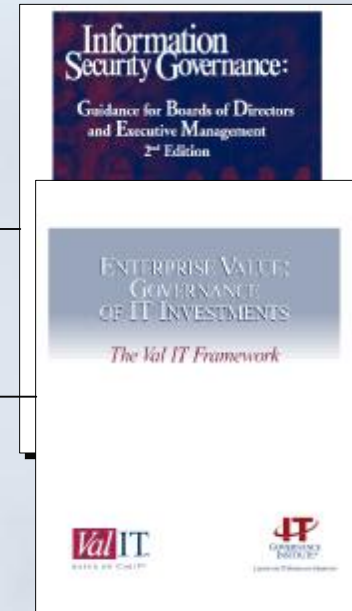
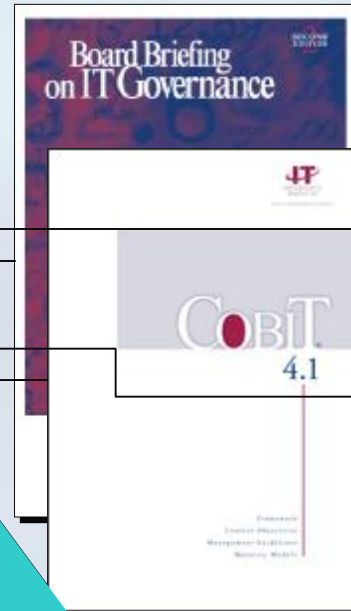
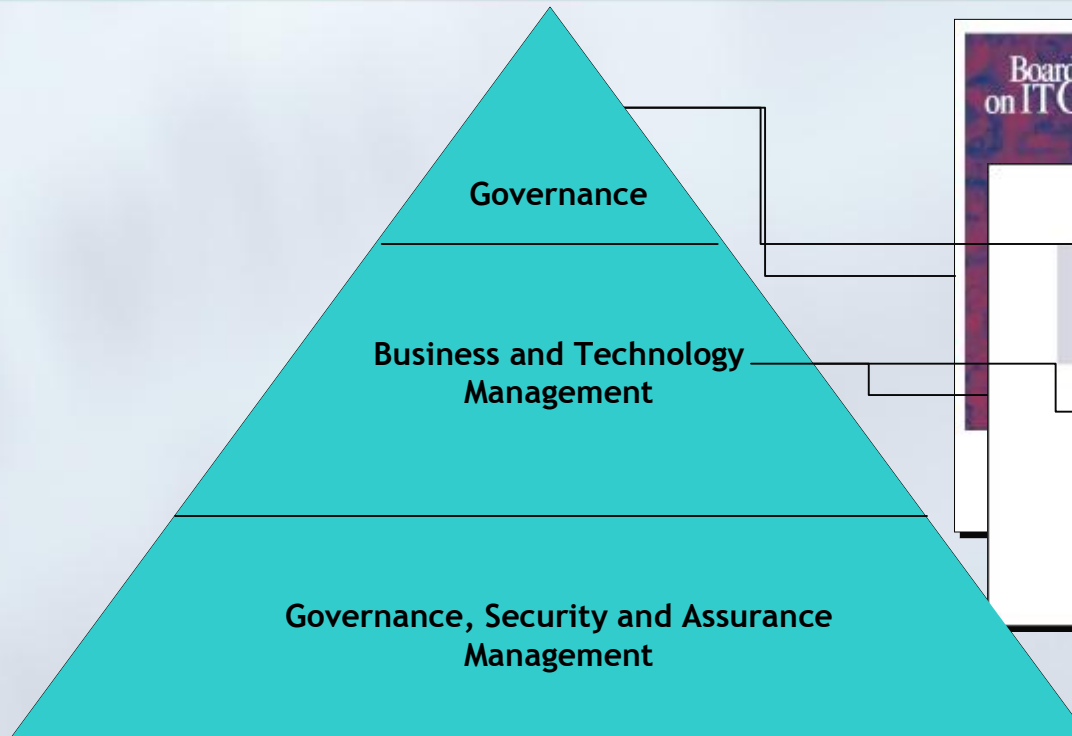
Moving forward





ISACA/ITGI References

IT Governance Product Suite

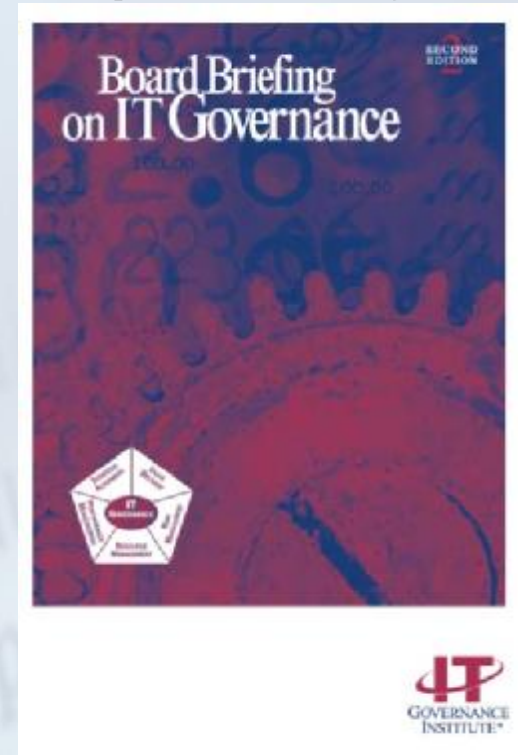


IT Governance
Board Briefing on
Implementation
Security Governance
Guide

Board Briefing on IT Governance



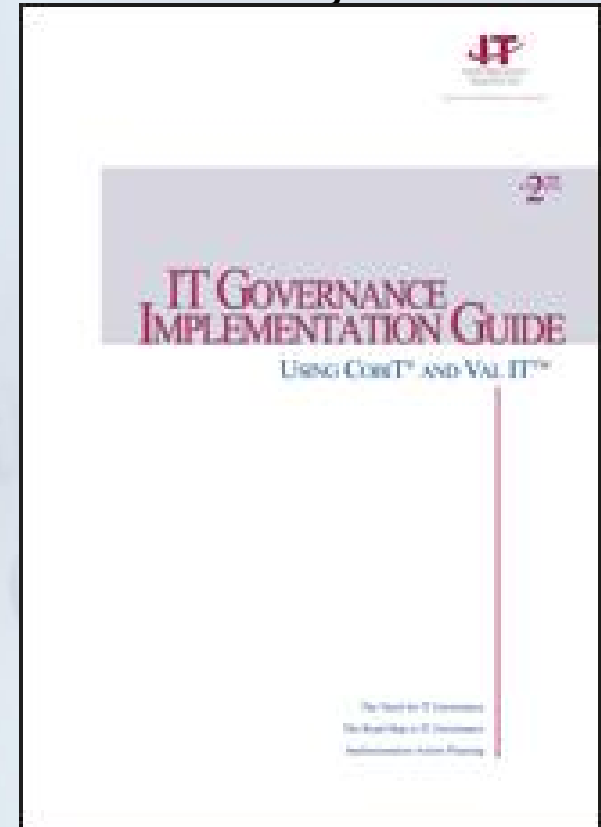
- Directed at boards of directors, supervisory boards, audit committees, chief executive officers, chief information officers and other executive management
- Details why IT governance is important, what the issues are and what boards' and executives' responsibility is for managing them.
- The document covers:
 - A summarized background on governance
 - Role of IT governance fits in the context of enterprise governance
 - Provides a simple framework with which to think about IT governance
 - Questions board members should ask
 - Good practices & critical success factors
 - Performance measures
 - Maturity model for benchmarking



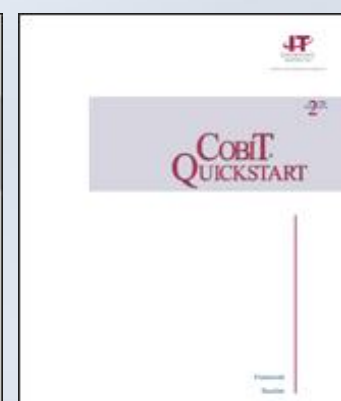
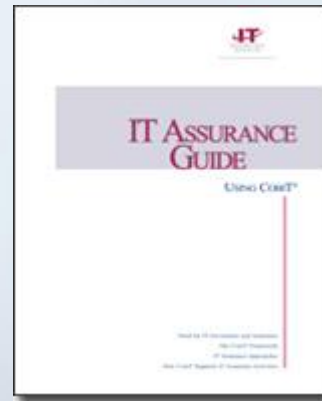
IT Governance Implementation Guide



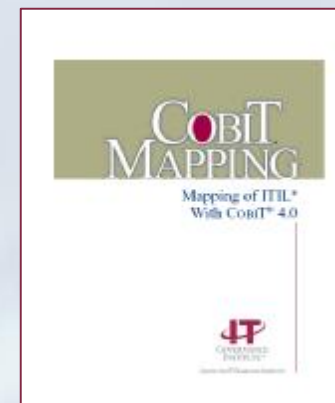
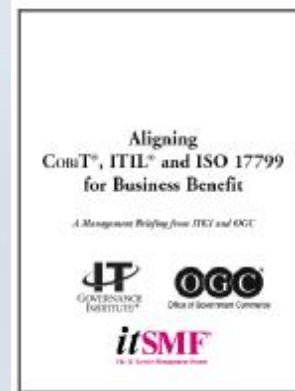
- Why IT governance is important and why organizations should implement it
- The IT governance life cycle
- The COBIT and Val IT frameworks
- How COBIT and Val IT are linked to IT governance and how they enable implementation
- Stakeholders who have an interest
- Road map for implementing IT governance using COBIT
- Implementation toolkit on CD-ROM, containing a variety of resources
 - Templates
 - Diagnostic tools
 - Reporting techniques
 - Mappings
 - Slide presentations
 - IT governance implementation activity templates
 - IT balanced scorecard example
 - Management awareness diagnostics
 - Maturity measurement information



Guidance and New Developments



- ITIL and COBIT Mapping
- COBIT Guidance for service managers
- Application controls
- Guidance for IT



Summary



- IT Governance is critical to most aspects of the business not just IT
- Control frameworks (COBIT) provide the guidance on the controls required to ensure good Governance
- ITIL processes allow for automation and repeatability of processes to deliver constantly
- Governance is not only mandatory it adds competitive edge to your organisation
- COBIT - Free download www.isaca.org
- V3 and COBIT 4.1 Mapping available
- Remember to download the Board Briefing document

Call To Action



- **After this session,**
 - Visit www.isaca.org and download the guidance
 - Review the mapping of COBIT and ITIL and identify “target” processes
 - Assess your current level of process maturity
 - Develop your metrics
 - Identify the gaps
 - Plan the implementation
 - Provide feedback to guide future development of COBIT - go to www.isaca.org/COBIT and click on Feedback.

For More Information:



Debbie Lew

Debbie.Lew@ey.com

Senior Manager,

**Assurance and Advisory Business Services,
Ernst & Young, LLP - Los Angeles**

COBIT Steering Committee

Office: 1 805 778 7049