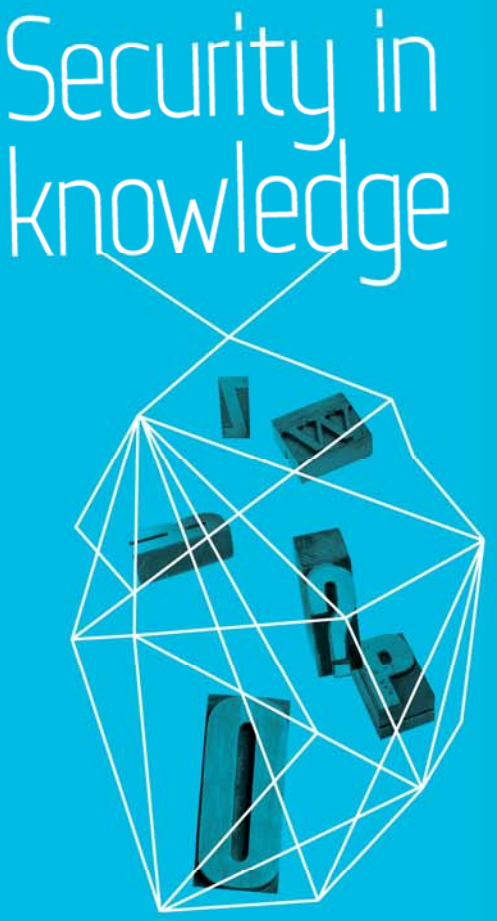
RSA CONFERENCE ASIA PACIFIC 2013



CLOUD SECURITY THROUGH COBIT, ISO 27001 ISMS CONTROLS, ASSURANCE AND COMPLIANCE

Indranil Mukherjee
Singapore ISC Pte Ltd

Session ID: CLD-T02

Session Classification: Intermediate

Cloud Computing – from a genealogy perspective (on the lighter side)

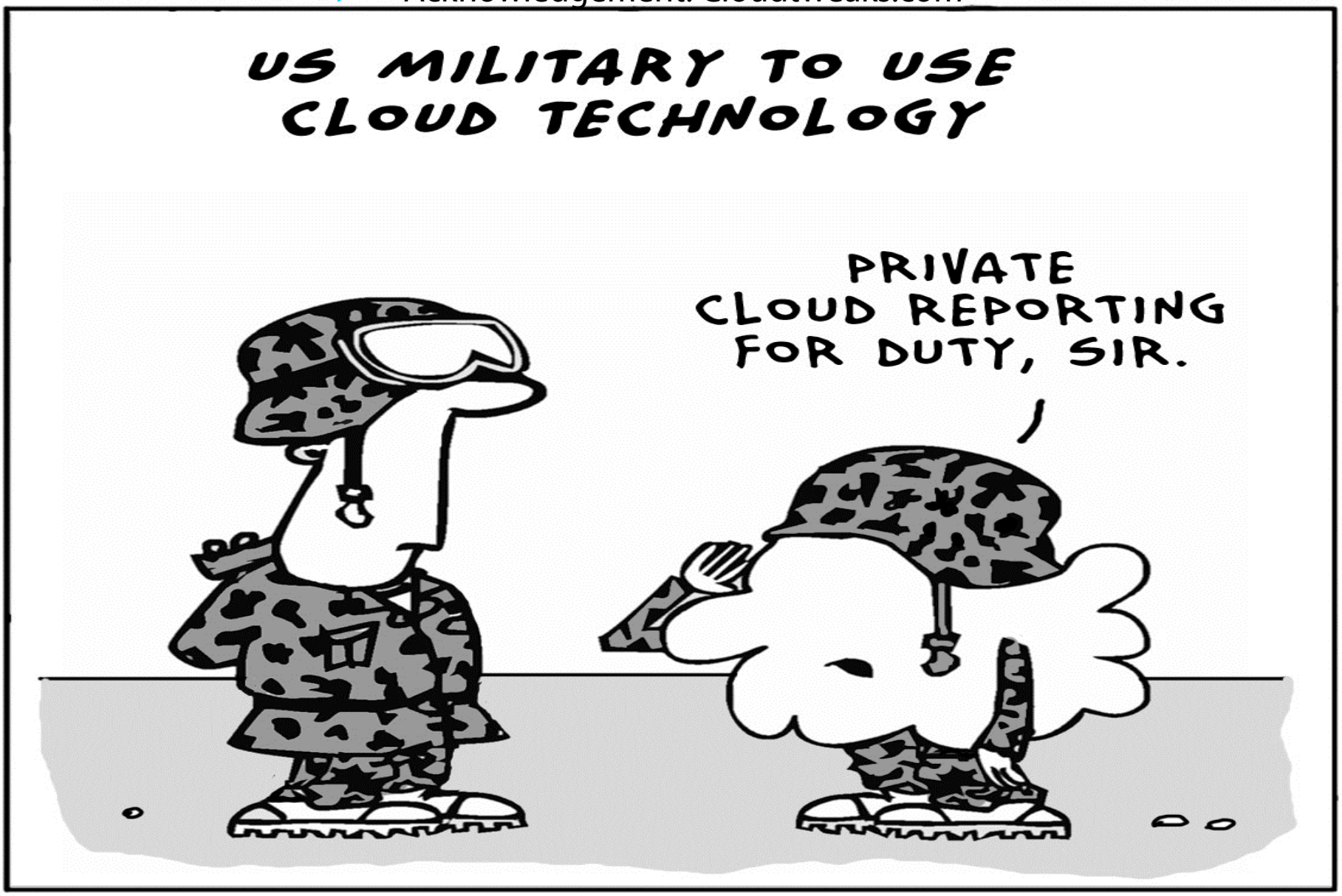
-Born for CLOUD Computing

"Indra" in India refers to the god of the Clouds, which supply rain and thunder, and the weather is at his command. As controller of the megha (cloud), he is master of the clouds and is also known as Maghavan.

"**Nil**" means Cloud or champion, in Gaelic

CLOUD TYPES (The Lighter Side)

- Acknowledgement: Cloudtweaks.com



DISCLAIMER

Any views or opinions presented in this Presentation are solely those of the author and do not necessarily represent those of his employers, past or present.

Any images used in this presentation are either

i) free of copyright

or

ii) ISACA , ISO or ISC Copyright materials , which are being used with permission with "All Rights reserved" by ISACA , ISO or ISC

Cloud Security-COBIT, ISO27001 ISMS Controls, Assurance and Compliance

1: What is COBIT , ISO 27001 / ISMS Controls?

2: COBIT 5 Principles

3:Cloud Computing and ISACA's Control Objectives for Cloud Computing

4: ISO 27001 ISMS Controls with COBIT Assessment Program

5. ISO 27000 Certification Process

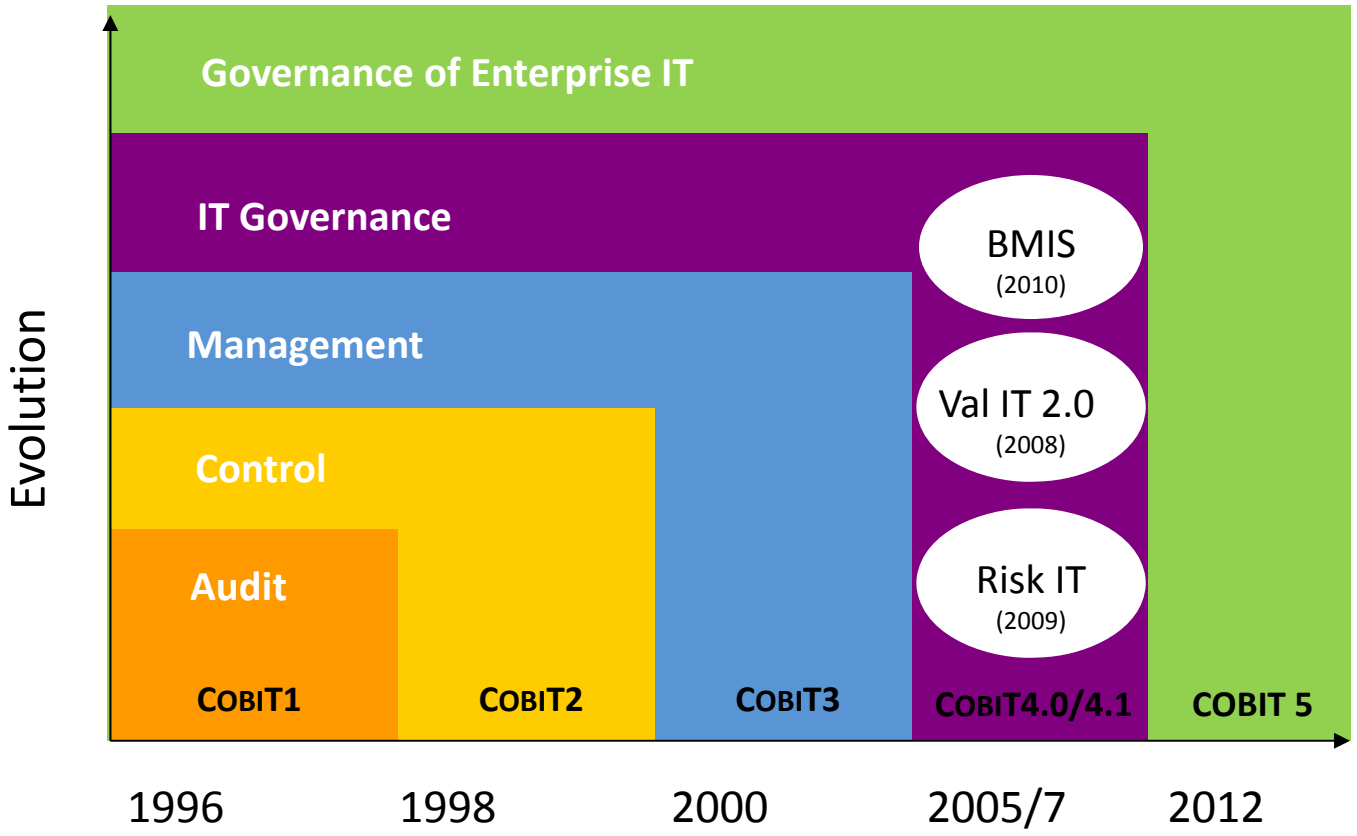
6. Summary/ Recommendations

1. What is COBIT 5

The only business framework for the governance & management of enterprise IT

- incorporates latest thinking in enterprise governance and management techniques
- provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from information systems

The Evolution of COBIT 5



Drivers for COBIT 5

- Provide guidance in:
  - Enterprise architecture
  - Asset and service management
  - Emerging sourcing and organization models
  - Innovation and emerging technologies
- End to end business and IT responsibilities
- Controls for user-initiated and user-controlled IT solutions

COBIT 5 Scope

- Not simply IT; not only for big business!
  - COBIT 5 is about ***governing and managing information***
    - Whatever medium is used
    - End to end throughout the enterprise
  - Information is *equally* important to:
    - Global, multinational business
    - National and local government
    - Charities and not for profit enterprises
    - Small to medium enterprises and
    - Clubs and associations

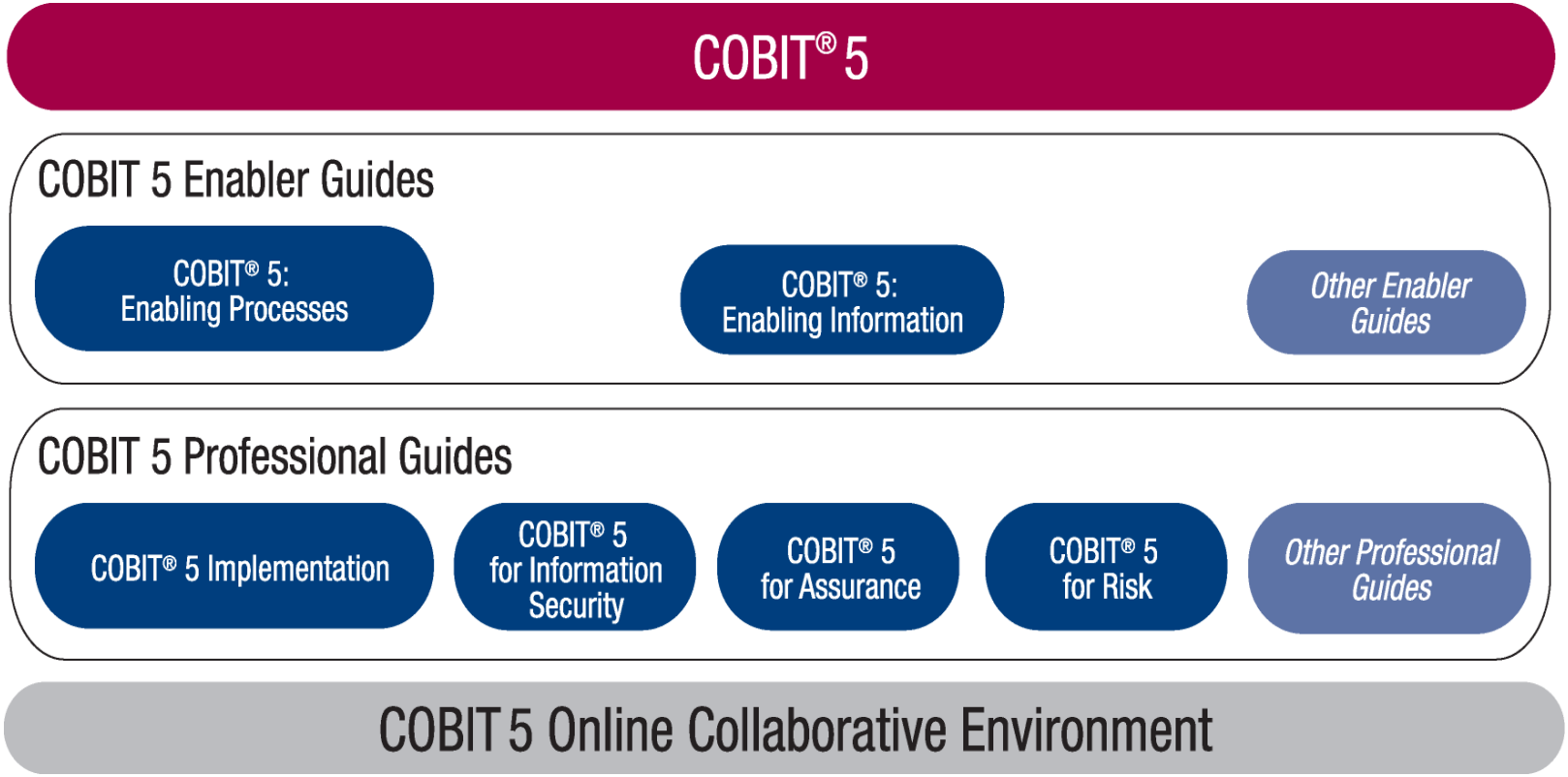
Business Needs

- Enterprises are under constant pressure to:
  - Increase benefits realization through effective and innovative use of enterprise IT
    - Generate business value from new enterprise investments with a supporting IT investment
    - Achieve operational excellence through application of technology
  - Maintain IT related risk include IT security risk at an acceptable level
  - Contain cost of IT services and technology
  - Ensure business and IT collaboration, leading to business user satisfaction with IT engagement and services
  - Comply with ever increasing relevant laws, regulations and policies

The COBIT 5 Format

- Simplified
  - COBIT 5 directly addresses the needs of the viewer from different perspectives
  - Development continues with specific practitioner guides
- COBIT 5 is initially in 3 volumes:
  - The Framework – Free Download
  - Process Reference Guide – Free to Members
  - Implementation Guide - Free to Members
- COBIT 5 is based on:
  - 5 principles and
  - 7 enablers

COBIT 5 Product Family

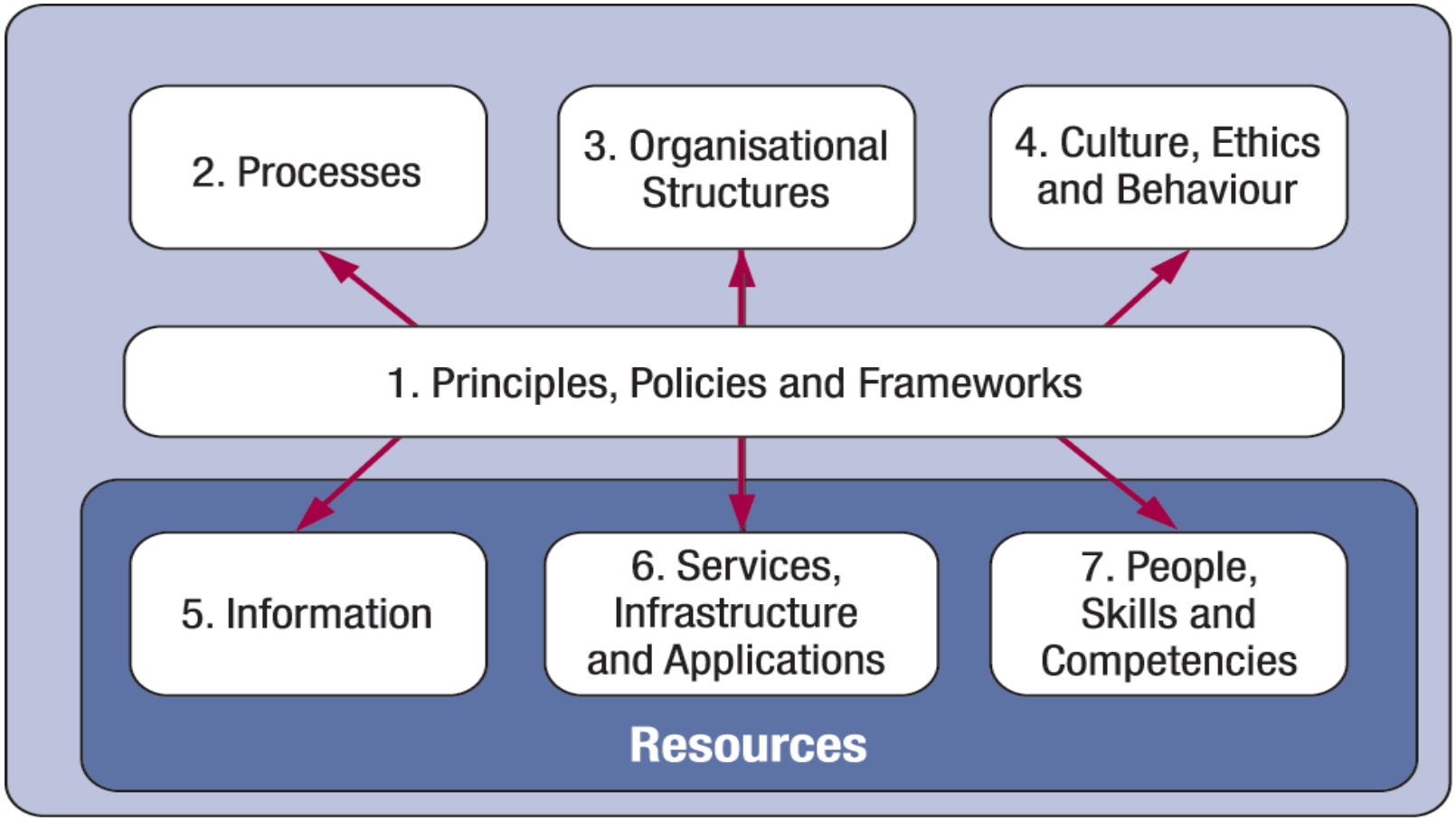


Areas of Change

- The major changes in COBIT 5 content and how they may impact GEIT* implementation/improvement are:
  - New GEIT principles – *introduced in detail later*
  - Increased **focus on enablers**
  - New and modified processes
  - Separated governance and management practices and activities
  - Revised and expanded goals and metrics
  - Defined inputs and outputs
  - More detailed RACI charts
  - Process Capability Assessment Model

(* Governance of Enterprise Information Technology)

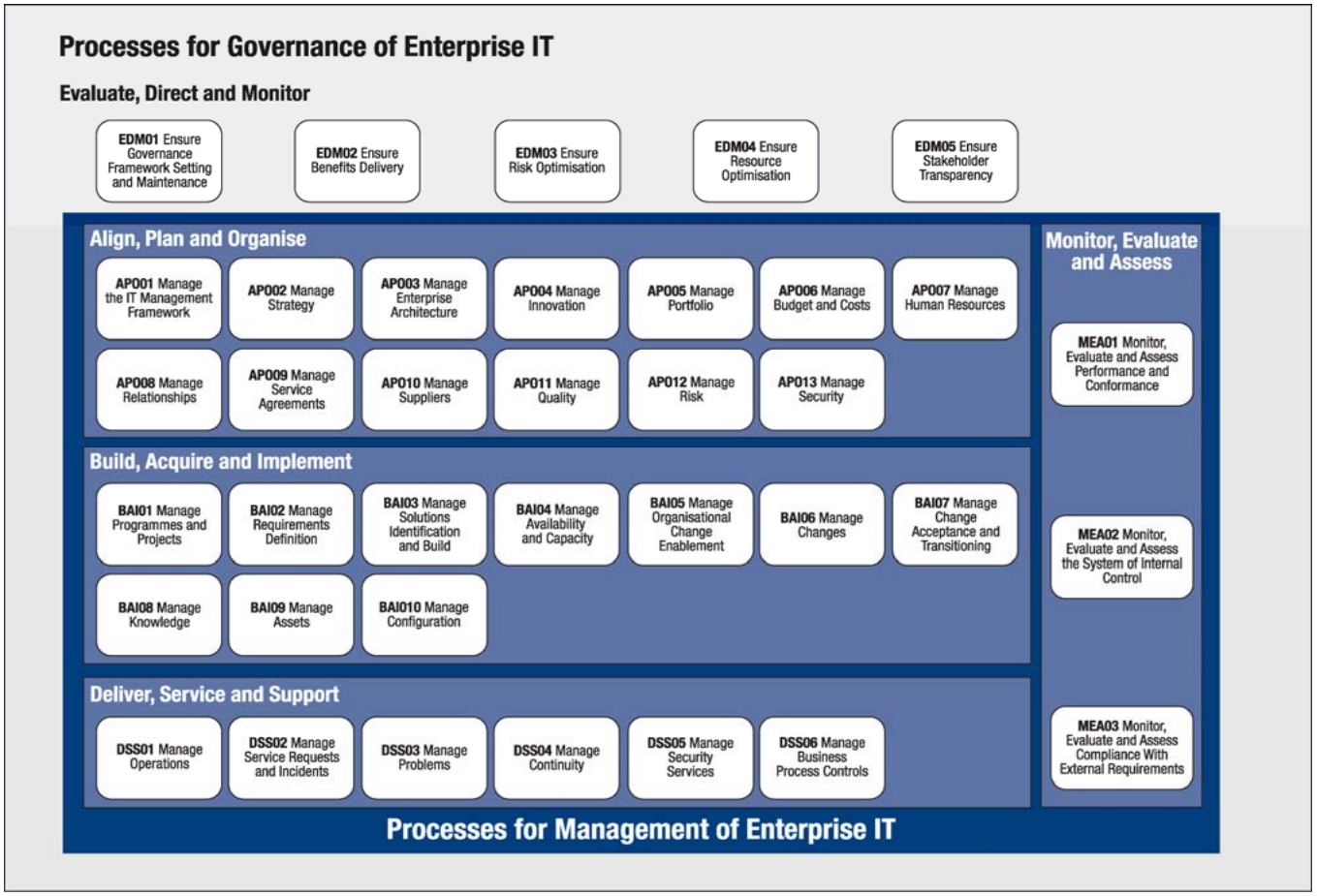
COBIT 5



New Process Reference Model

- The COBIT 5 process reference model
  - Introduces a governance domain
  - Several new and modified processes
  - Incorporate the principles of other, non-ISACA frameworks
  - Can be used as a guide for adjusting the enterprise's own process model (just like COBIT 4.1).
- COBIT 5 is still a generic framework

COBIT 5 Process Reference



New and Modified Processes

- COBIT 5 introduces five new **governance** processes
- 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

New & Modified Processes

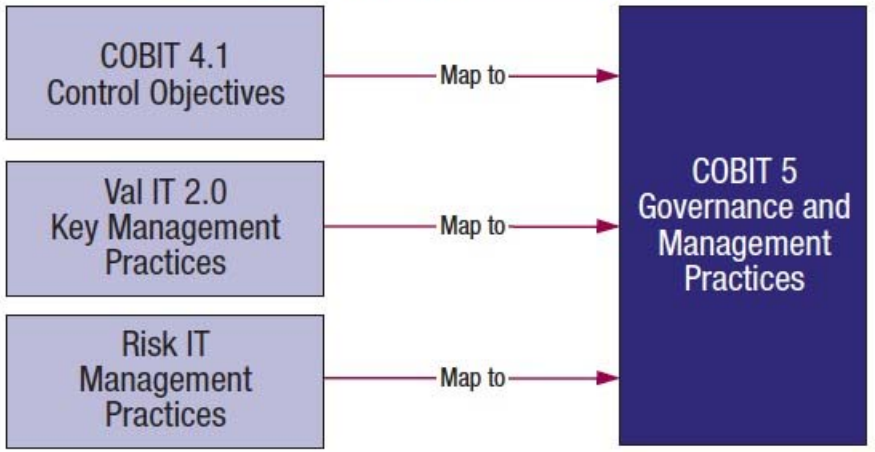
- There are several new and modified processes that reflect current thinking, in particular:
  - APO03 Manage enterprise architecture
  - APO04 Manage innovation
  - APO05 Manage portfolio
  - APO06 Manage budget and costs
  - APO08 Manage relationships
  - APO13 Manage security
  - BAI05 Manage organizational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

COBIT 5 and Legacy ISACA Frameworks

Appendix A
Mapping Between COBIT 5 and Legacy ISACA Frameworks

Figure 13 shows the ISACA frameworks included in COBIT 5.

Figure 13—ISACA Frameworks Included in COBIT 5



The mapping of COBIT 4.1, Val IT and Risk IT components to COBIT 5 is shown in **figures 14, 15** and **16**.

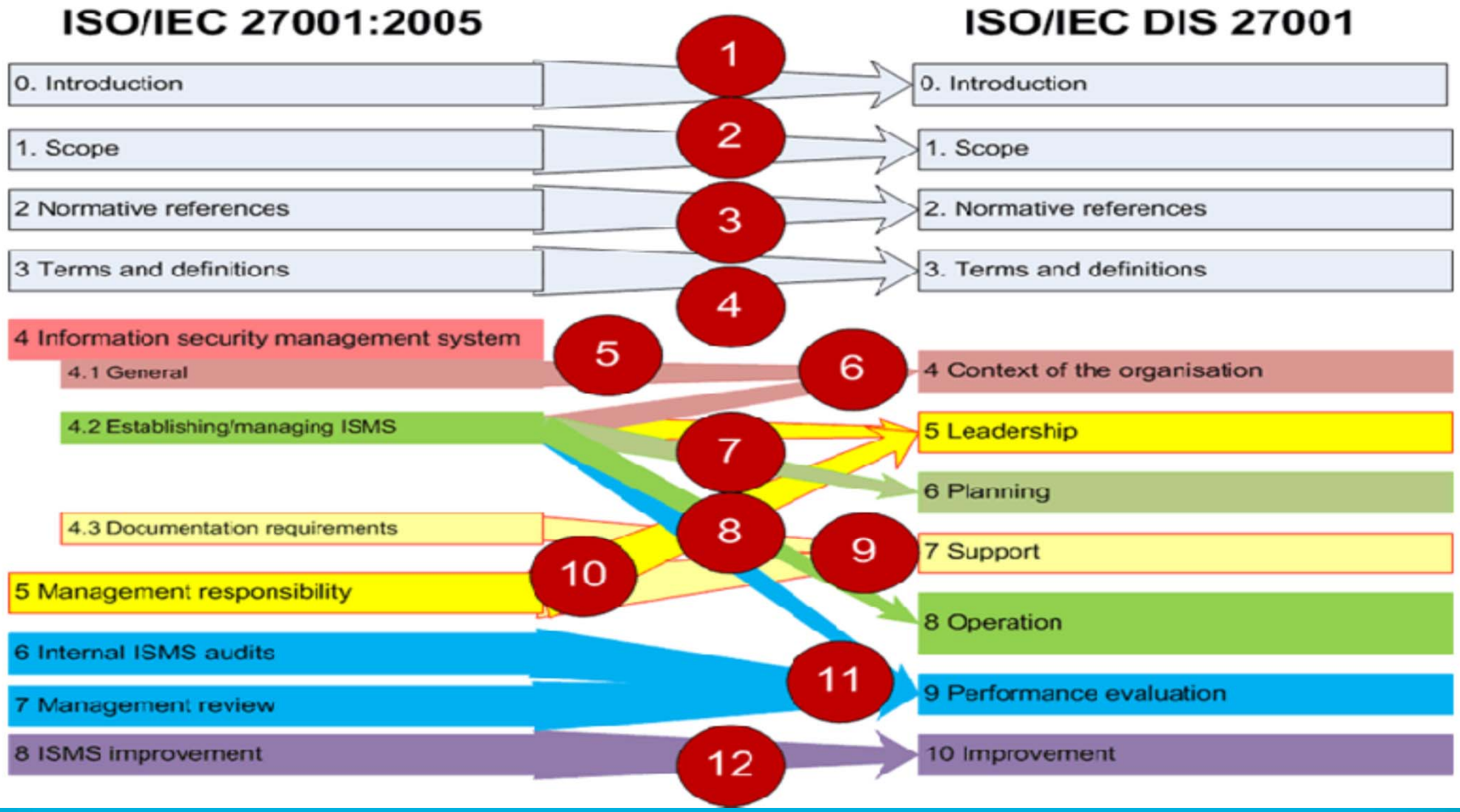
INTRODUCTION to ISO/IEC 27000

- ISO/IEC 27000 provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS)
- ISO 27001 Auditable standard on Information Security Management System (ISMS) requirements
- First version of the standard was in 2005
- Aligns with COBIT 5

Arriving soon

ISO/IEC 27018 — Data protection for cloud systems

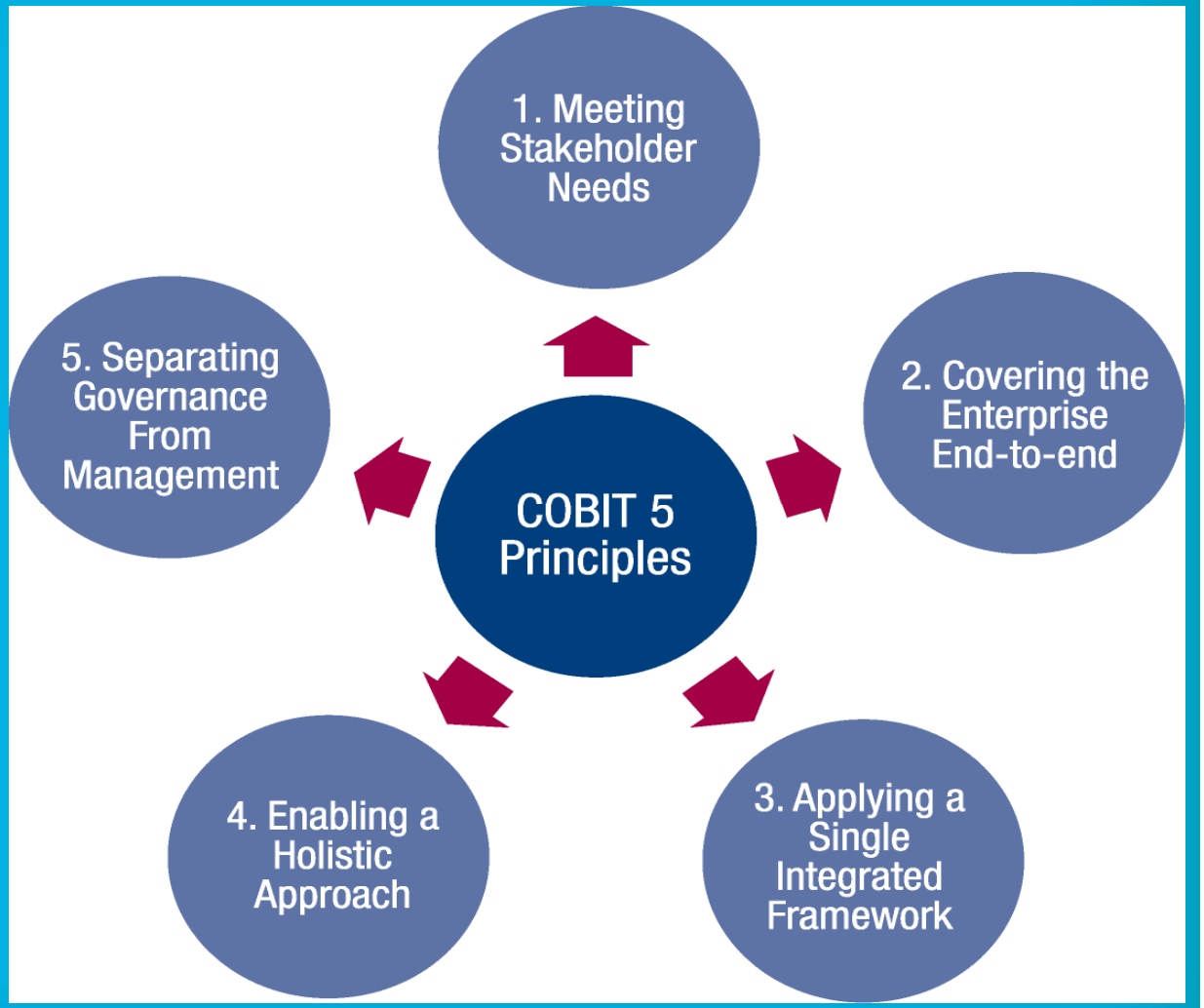
ISO27001 & ISMS Controls



COBIT 5 vs ISO 27001

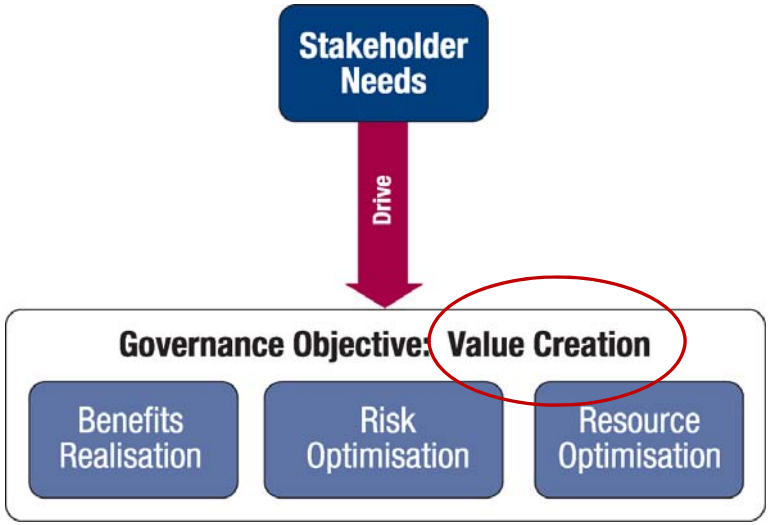
- COBIT 5 covers *end-to-end business and IT activities* whilst ISO 27001 focuses on IT Security Management
- COBIT 5 Provide a holistic Framework and complete coverage of practices whilst ISO 27001 provides guidelines and is a certifiable standard
- COBIT 5 makes the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more explicit and transparent and aligns with ISO 27001

2. COBIT 5 Principles



Principle 1:
Meeting Stakeholder Needs

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



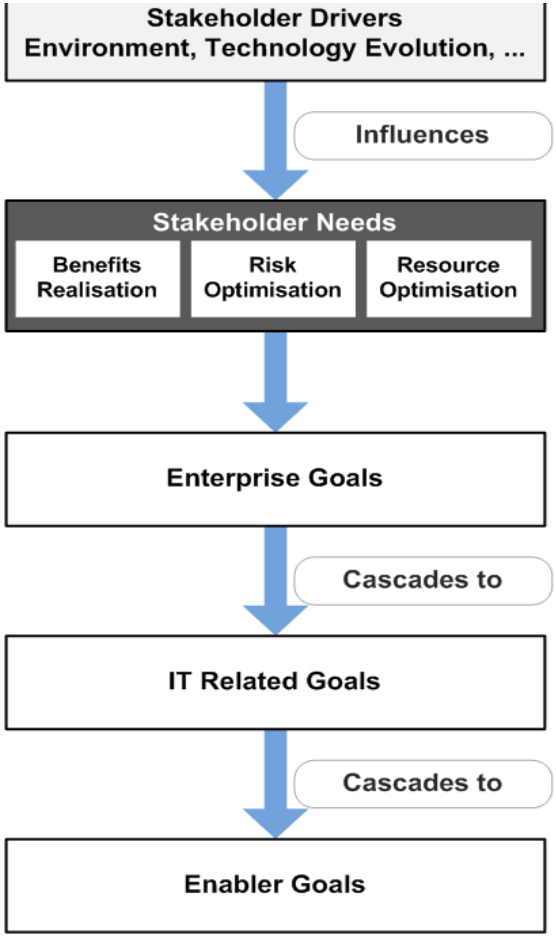
- **Value creation:** realizing benefits at an optimal resource cost while optimizing risk.

Principle 1:
Meeting Stakeholder Needs

- Enterprises have **many** stakeholders
- Governance is about:
  - Negotiating
  - Deciding amongst different stakeholders' value interests
  - Considering all stakeholders when making benefit, resource and risk assessment decisions
- For each decision, ask:
  - For whom are the benefits?
  - Who bears the risk?
  - What resources are required?

Principle 1:
Meeting Stakeholder Needs

- Stakeholder needs have to be transformed an enterprises' actionable strategy into specific, practical and customized goals for IT and its enablers



Principle 1:
Meeting Stakeholder Needs

- The COBIT 5 goals cascade allows the definition of priorities for
  - Implementation
  - Improvement
  - Assurance of enterprise governance of IT
- 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 enablers are used to achieve enterprise goals

Principle 1:
Meeting Stakeholder Needs

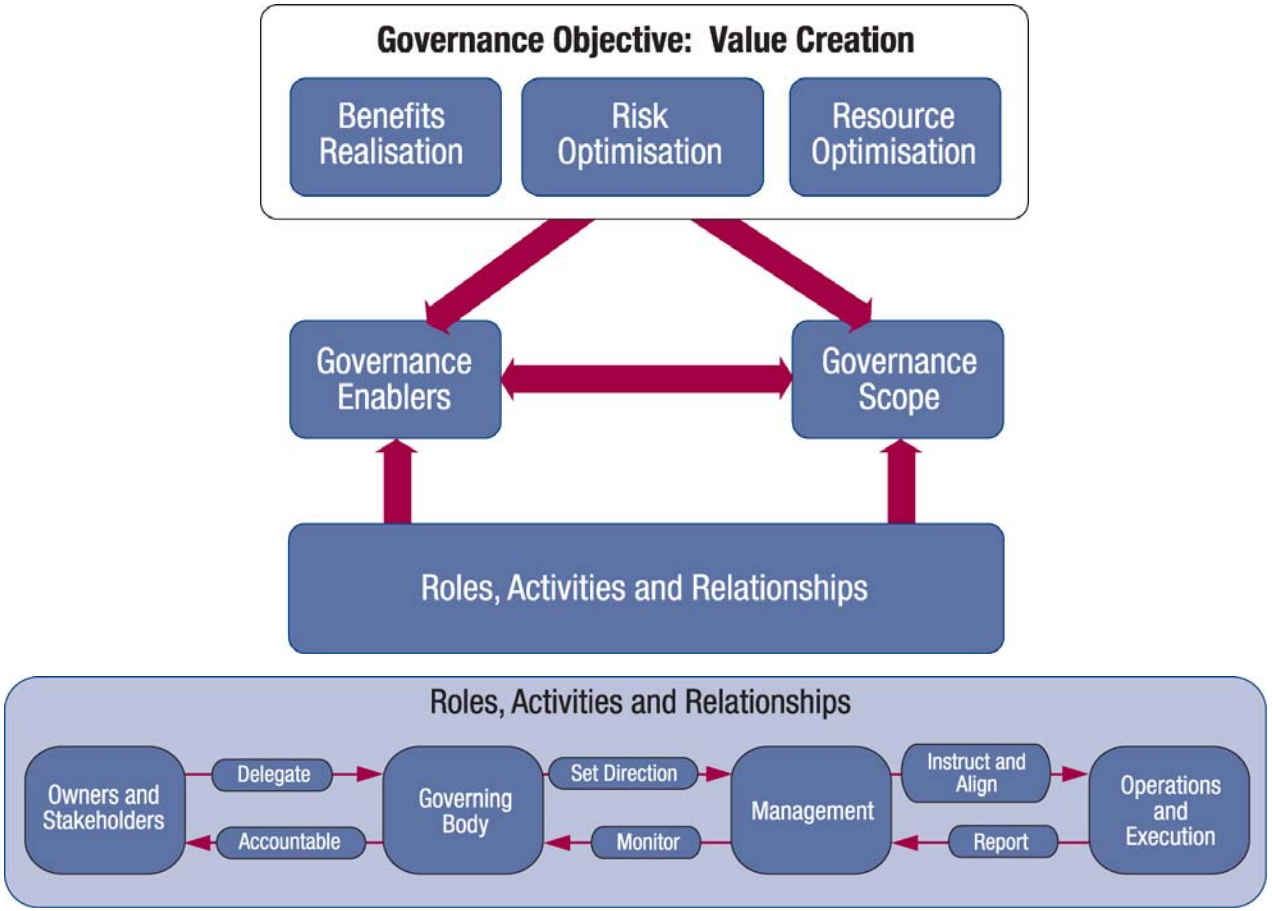
- **Internal** stakeholder concerns include:
  - How do I get value from the use of IT?
  - How do I manage performance of IT?
  - How can I best exploit new technology for new strategic opportunities?
  - How do I know whether I'm compliant with all applicable laws and regulations?
  - Am I running an efficient and resilient IT operation?
  - How do I control cost of IT?
  - Is the information I am processing adequately and appropriately secured?
  - How critical is IT to sustaining the enterprise?
  - What do I do if IT is not available?

Principle 1:
Meeting Stakeholder Needs

- COBIT 5 addresses the governance and management of information and related technology ***from an enterprise-wide, end-to-end perspective***

- COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance
  - Covers all functions and processes within the enterprise
  - **Does not focus only on the 'IT function'**

Principle 2:
Covering the Enterprise End–to–End



Principle 2:
Covering the Enterprise End–to–End

Main elements of the governance approach:

- **Governance Enablers** ***comprising***
  - ***The organizational resources for governance***
  - ***The enterprise's resources***
  - ***A lack of resources or enablers may affect the ability of the enterprise to create value***
- **Governance Scope** ***comprising***
  - ***The whole enterprise***
  - ***An entity, a tangible or intangible asset, etc.***

Principle 2:
Covering the Enterprise End–to–End

- Governance roles, activities and relationships
  - Define **Who** is involved in governance
  - **How** they are involved
  - **What** they do and
  - **How** they interact

- COBIT 5 defines the difference between governance and management activities in principle 5

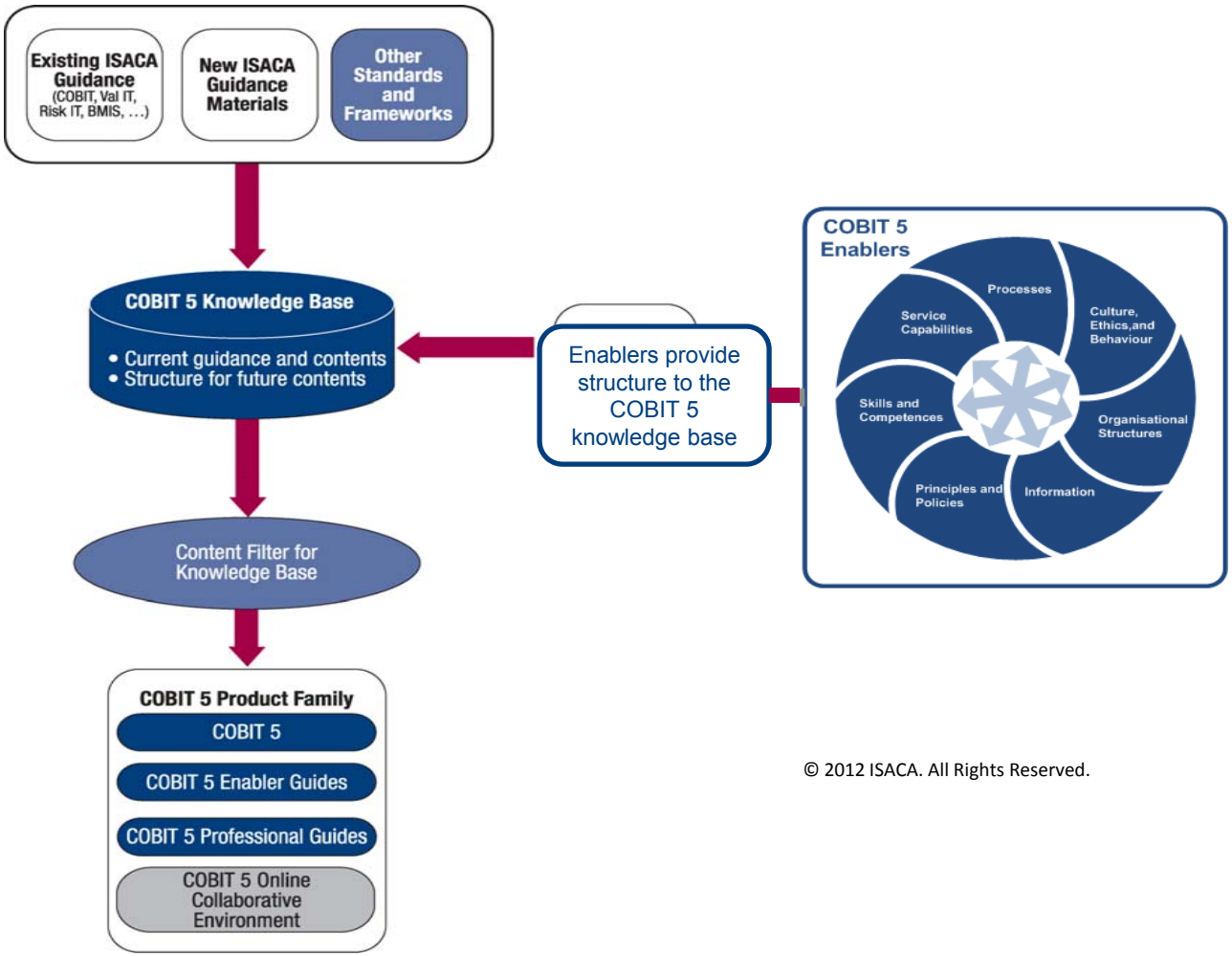
Principle 3:
Applying a Single Integrated Framework

- **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

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– Released April 10 2012*
  - *COBIT 5: Enabling Processes – Released April 10 2012*
  - *COBIT 5 Implementation Guide – Released April 10 2012*
  - COBIT 5 for Information Security – *Target 3rd Quarter, 2012*
  - COBIT 5 for Assurance – *Target 1st Quarter, 2013*
  - COBIT 5 for Risk – *Target 1st Quarter, 2013*
  - A series of other products is planned; they will be tailored for specific audiences or topics
  - COBIT 5 Online – *Currently under development*
- The perspective concept links the above to external sources for standards

Principle 3:
Applying a Single Integrated Framework



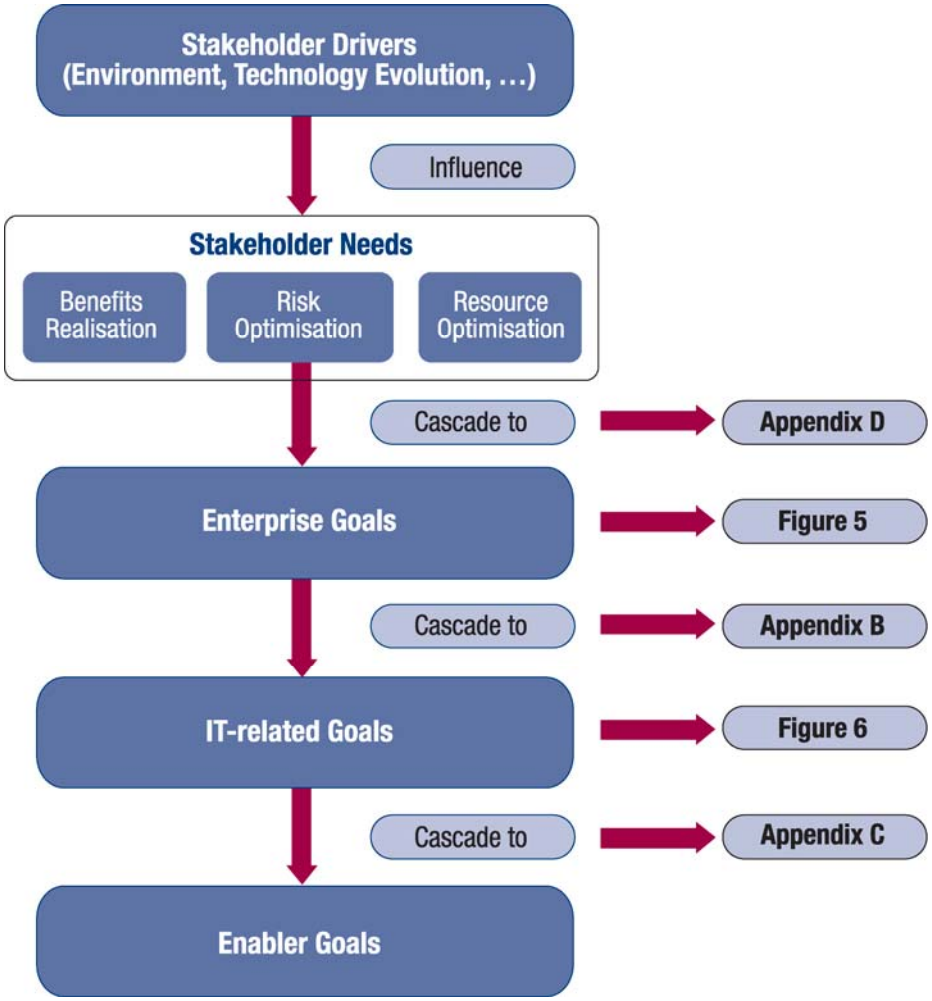
Principle 4:
Enabling a Holistic Approach

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

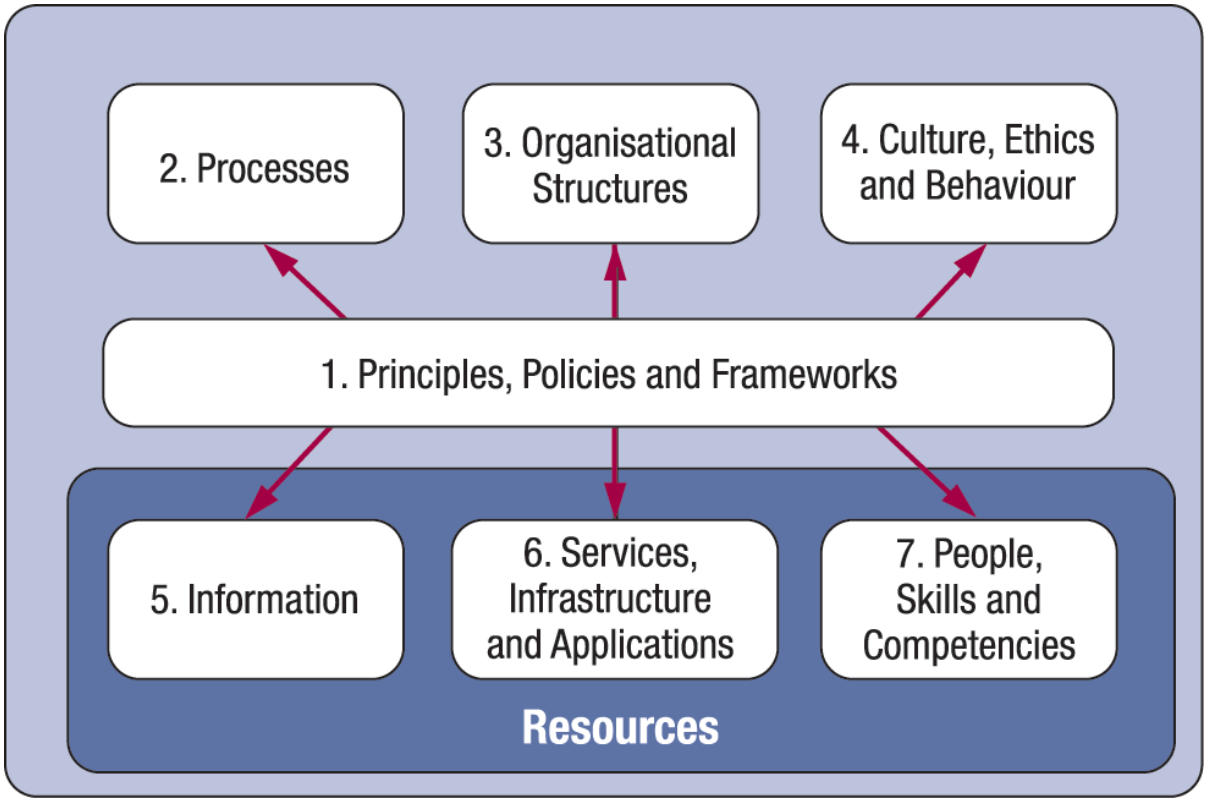
COBIT 5 enablers are:

- 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



Principle 4:
Enabling a Holistic Approach



Principle 4:
Enabling a Holistic Approach

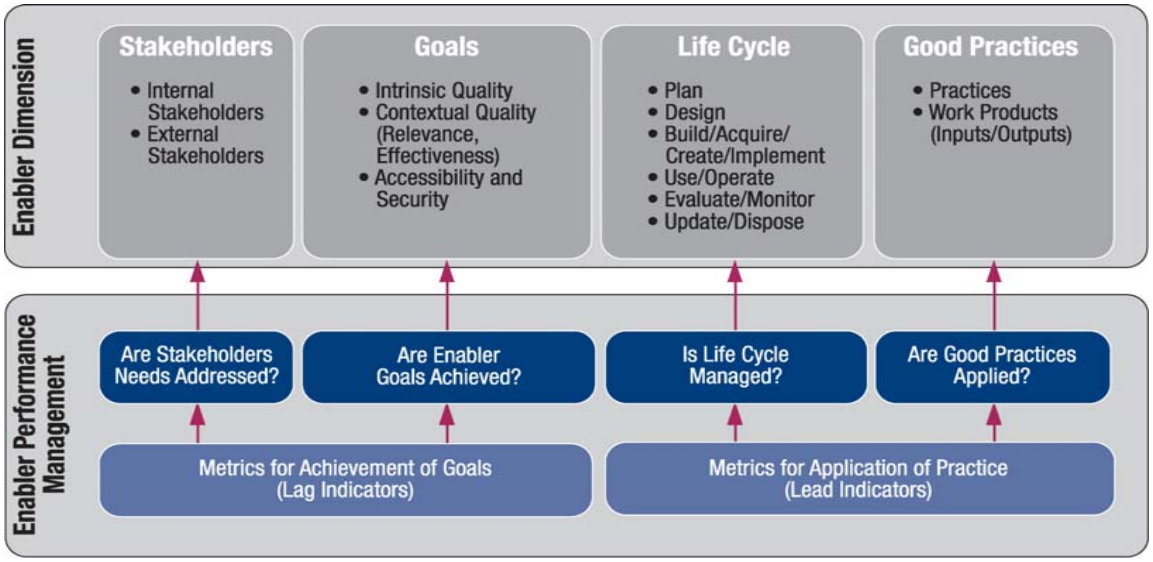
Enablers:

1. Principles, policies and frameworks
2. Processes
3. Organizational structures
4. Culture, ethics and behavior
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

Principle 4:
Enabling a Holistic Approach

COBIT 5 enabler dimensions:

- All enablers have a set of common dimensions that:
  - Provide a common, simple and structured way to deal with enablers & Allow an entity to manage its complex interactions
  - Facilitate successful outcomes of the enablers



Principle 5:
Separating Governance from Management

- The **COBIT 5** framework makes a clear distinction between **governance and management**

- **Governance and management**
  - Encompass different types of activities
  - Require different organizational structures
  - Serve different purposes

- ***COBIT 5: Enabling Processes*** differentiates the activities associated with each

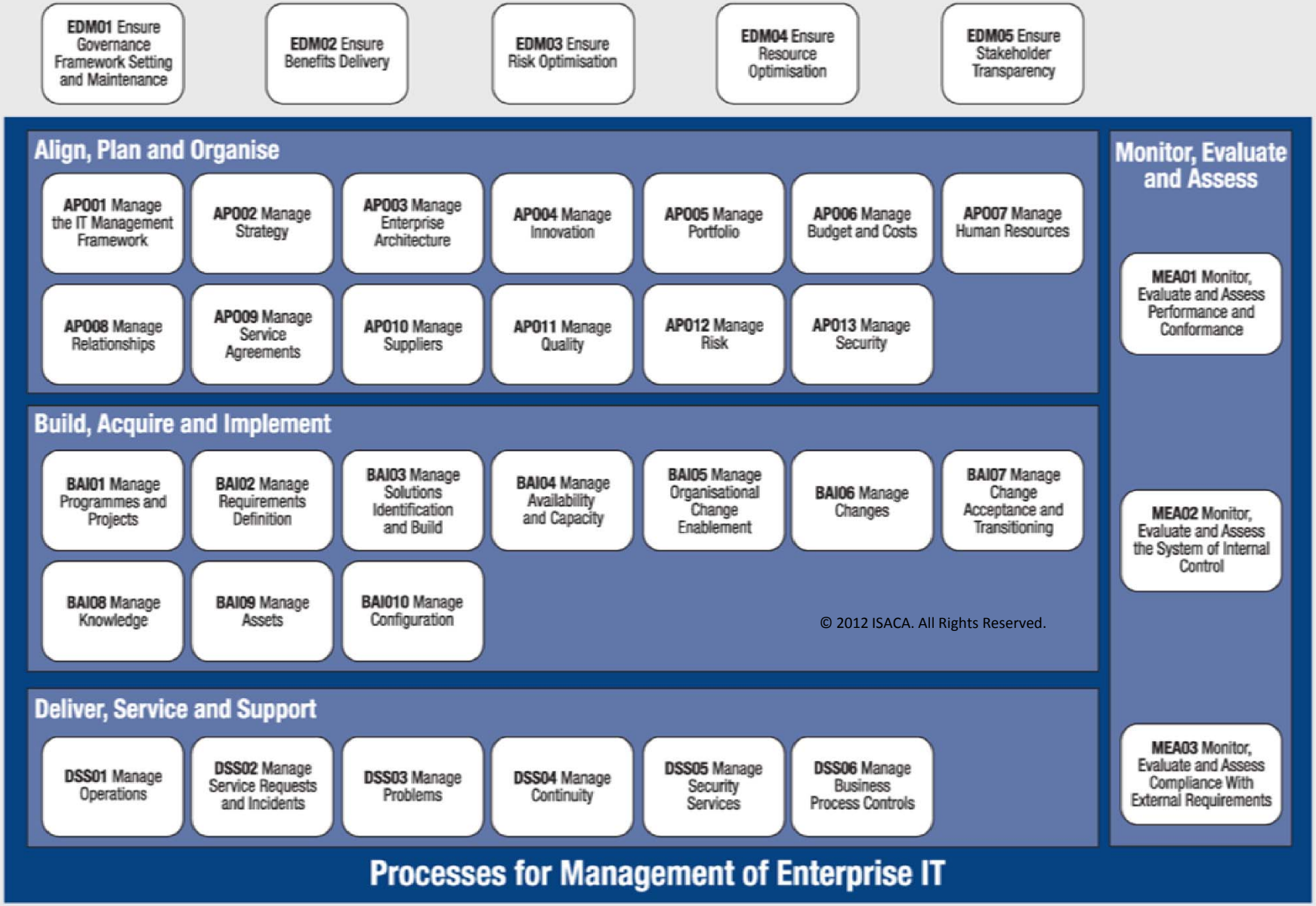
Principle 5:
Separating Governance from Management

- **Governance** ensures that stakeholder needs, conditions and options are:
  - **Evaluated** to determine balanced, agreed-on enterprise objectives to be achieved
  - Setting **direction** through prioritization and decision making
  - **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)**

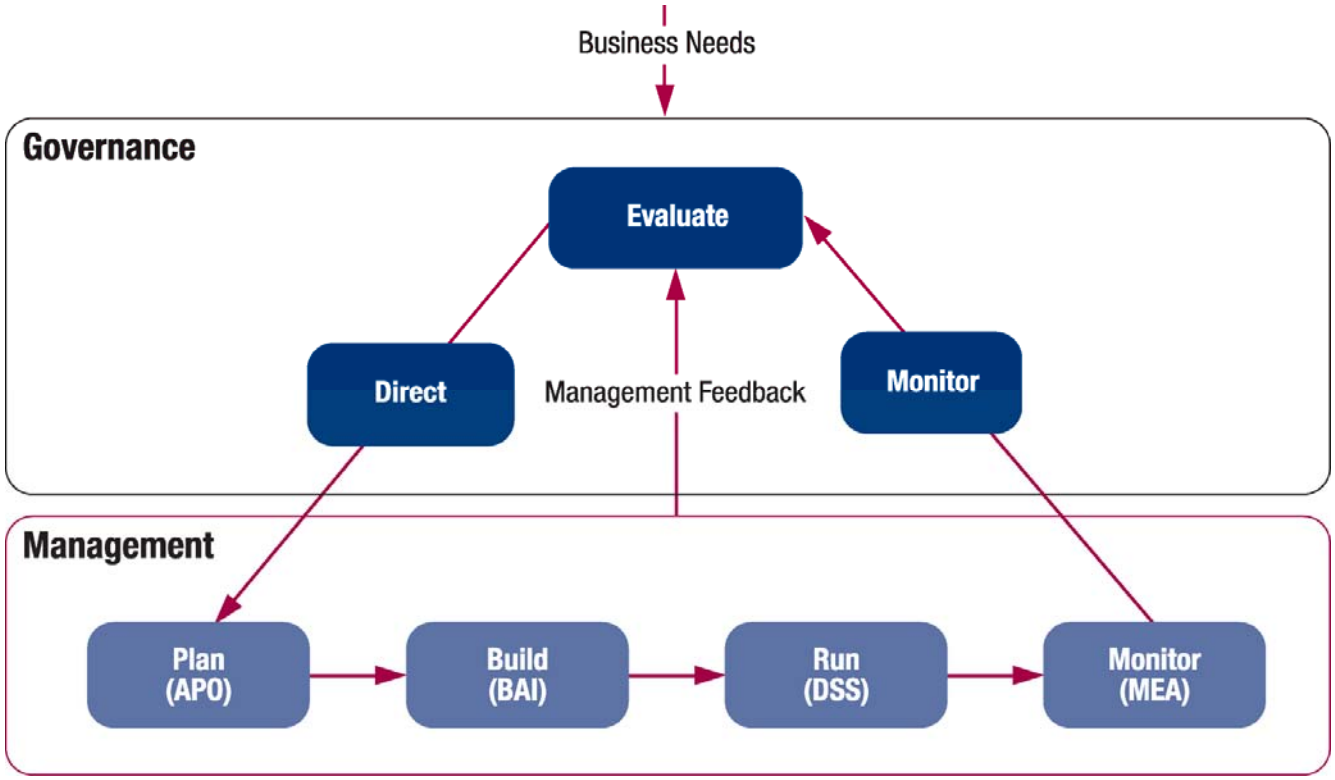
Processes for Governance of Enterprise IT

COBIT 5 Process Reference Model



Principle 5:
Separating Governance from Management

COBIT 5 Governance and Management Key Areas



COBIT 5 Principles – 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.

RSA CONFERENCE ASIA PACIFIC 2013

3:Cloud Computing and ISACA's Control Objectives for Cloud Computing

Control & Assurance Issues in Cloud Adoption

- 4,000 business and IT managers across 7 countries
- Cloud Survey by Ponemon Institute July 2012 survey
- Who is considered responsible for protecting this valuable and often regulated class of data – cloud service provider or consumer ?
- The findings are also significant in explaining data encryption applied inside / outside a cloud & management of associated encryption keys
- Encryption decision:
  - before data leaves the organization's environment ? OR
  - whether encryption is expected to be a cloud component?

Control & Assurance Issues in Cloud Adoption

Proportion of are already transferring sensitive data to the cloud?

- About 50% currently transfer sensitive or confidential data to cloud
- Another 33% to transfer sensitive/ confidential data within next 2 years

Has cloud computing usage (sensitive data)increased or decreased security?

- 39% believe cloud adoption has decreased their companies' security

Who is responsible for data security in the cloud?

- 64% that currently transfer sensitive or confidential data to the cloud believe the cloud provider has primary responsibility for protecting it

How much visibility do decision makers have regarding cloud security?

- Nearly two thirds of respondents say they do not know what cloud providers are actually to protect their sensitive confidential data

Control & Assurance Issues in Cloud Adoption

Where is data encryption applied?

- 50% applies data encryption before transfer to the cloud provider and the other 50% rely on encryption that is applied within the cloud environment.

Who manages encryption keys when data is transferred to a cloud?

- 36% say their organization has primary responsibility for managing the keys.
- 22% say the cloud provider has primary responsibility for encryption key management.
- Even in cases where encryption is performed inside the enterprise, more than 50% hand over control of the keys to the cloud provider.
  - Encryption used for protecting stored data & application-based encryption
- Nearly 2/3rd do not know what cloud providers do to protect sensitive confidential data

CLOUD QUIZ

Which Cloud Framework is named after the Creator's son's toy elephant?

Wh

HADOOP after Doug Cutting's son's toy elephant

IT CONTROL OBJECTIVES for the Cloud : Introduction

- 5 Sections, 2 Appendices, only 193 pages !
- Glossary updated to introduce "Community Cloud" concept

The 5 Sections are

- Preface - Cloud Computing Service Models (IaaS/ PaaS/ SaaS) and the Cloud Deployment Models.
- Key updates – include the Community Cloud model which could be Business-process Specific, Industry -specific
- Cloud Computing Fundamentals discusses cloud evolution, provides technical building blocks, Cloud characteristics, cloud drivers & cloud computing challenges

IT CONTROL OBJECTIVES for

Cloud Computing:Governance & Frameworks

The third Section covers

- **Governance** -which has the Cloud Computing IT Benefits/ Value Enablement Risk and how to leverage Risk IT / Val IT/ COBIT for the Cloud.

- Key updates – "Outcome of Good Governance" & Mapping of ISACA's COBIT ,

  Risk IT and Val IT Frameworks

  to Cloud Governance

IT CONTROL OBJECTIVES for

Cloud Computing: Risk,Applicability & Compliance

Section 4 covers whether Businesses are Cloud ready , Risk Considerations, graduated Risk Responsibilities, IAM (Identity and Access management),Physical security, Operational Risk, Security concerns and Secure Code

Section 5 includes

1) Common Framework CSP Applicability for Third-party Certification/Examination

2) Key elements of a Unified IT Compliance program

3) Assurance through the Vendor management

Appendix A contains IT Control objectives for Cloud Computing

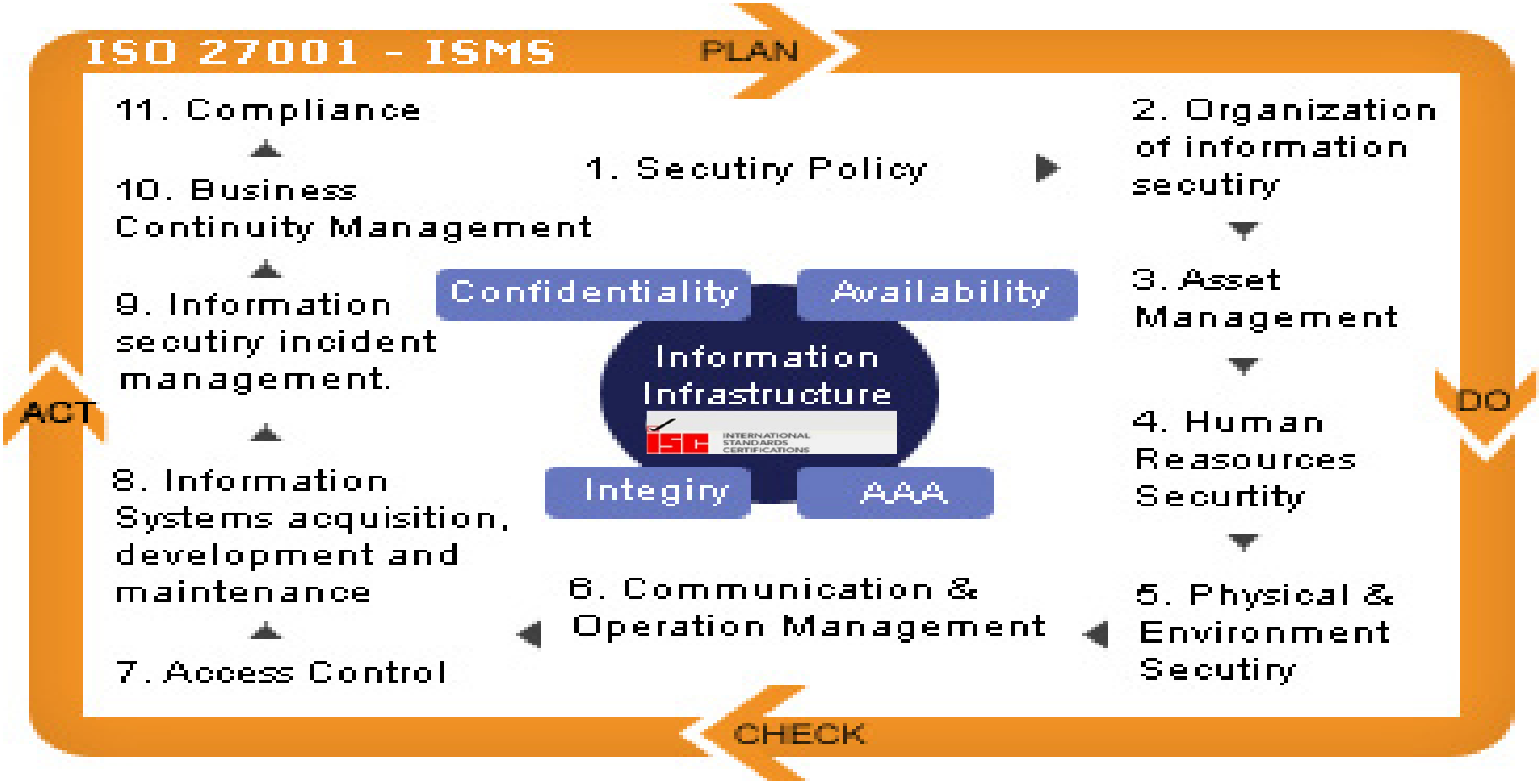
Appendix B –8 useful Templates/Frameworks for Audit & Assurance

RSA CONFERENCE ASIA PACIFIC 2013

4: ISO 27001 ISMS Controls with COBIT Assessment Program

ISO 27001 ISMS Controls

133 ISMS Controls Risk based IT Audit and certification



CLOUD SPECIFIC RISKS- I

Policy and Organizational Risks

- Lock –in with a single Provider
- Loss of Governance
- Compliance Challenges e.g MAS Circular dated 14th July 2011
  http://www.nortonrose.com/knowledge/publications/54960/monetary-authority-of-singapore-circular-regarding-its-outsourcing-and-cloud-computing
- Loss of Business Reputation due to co-tenant activities
- Cloud service termination or failure
- Cloud Provider acquisition
- Supply Chain Failure

Legal Risks

- Sub-poena and e-discovery
- Risk from changes in jurisdiction
- Data Protection risks
- Licensing risks

CLOUD SPECIFIC RISKS- II

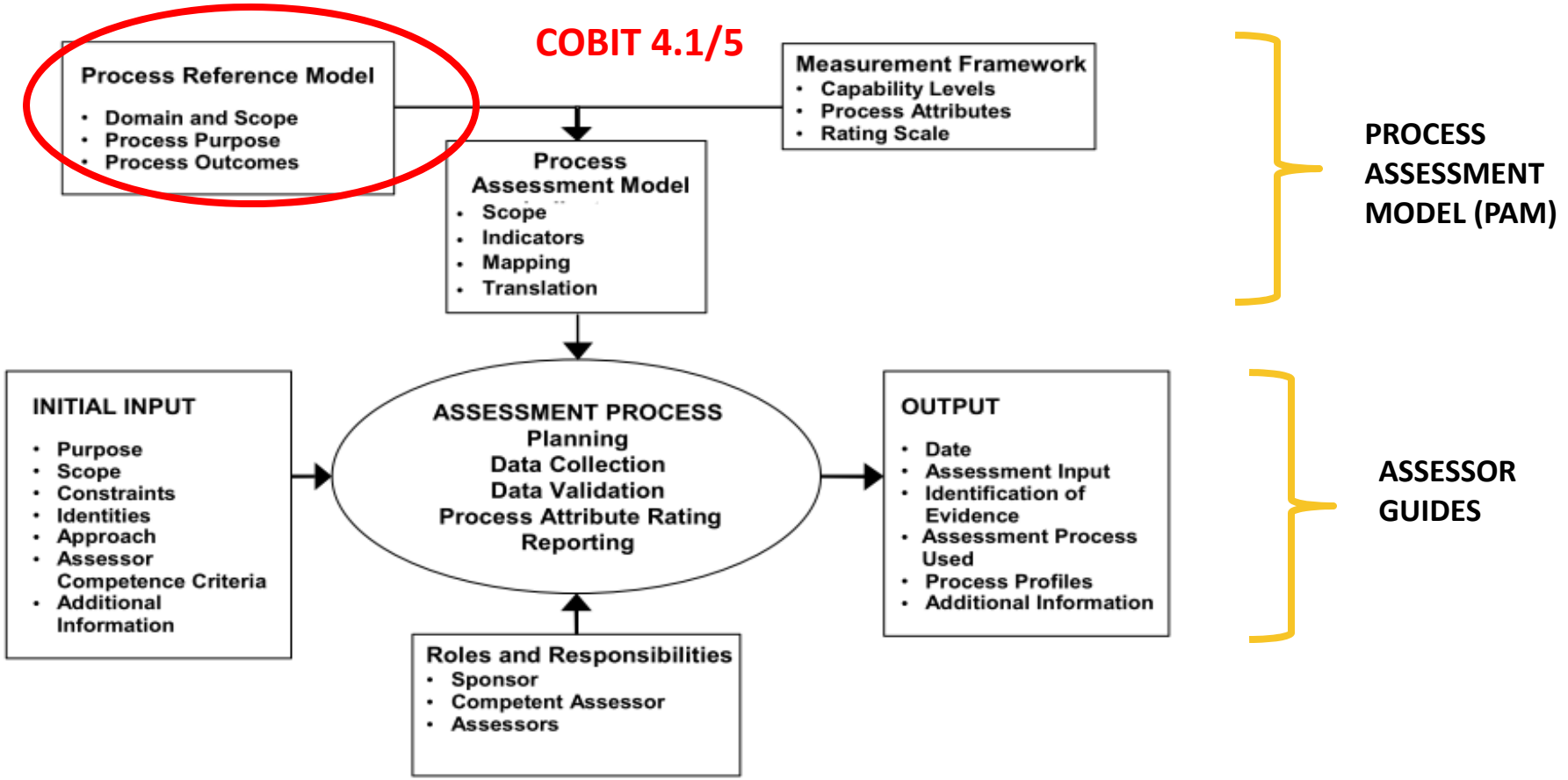
Technical Risks

- Resource exhaustion (under or over provisioning)
- Isolation Failure – resulted the first documented Cloud security hack
- Cloud provider malicious insider-abuse of high privilege roles
- Management interface compromise (manipulation, availability of infrastructure)
- Intercepting data in transit or Data leakage on up/download, intra-cloud
- Insecure or ineffective deletion of data
- Distributed Denial of Service (DDOS)
- Economic Denial Of Service (EDOS)
- Loss of Encryption keys
- Undertaking Malicious probes or scans
- Compromise service engine
- Conflicts between customer hardening procedures & cloud environment

What is the new COBIT Assessment Programme?

- The COBIT Assessment Programme includes:
  - *COBIT Process Assessment Model (PAM): Using COBIT 5*
  - *COBIT Assessor Guide: Using COBIT 5*
  - *COBIT Self Assessment Guide: Using COBIT 5*
- *Identical COBIT 4.1 versions also available*
- The COBIT 5 PAM is based on the ISO 15504 compliant process assessment model

Process Capability Model and Assessments



COBIT 5 Revised Process Capability Levels

Optimizing
The process is continuously improved to meet relevant current and projected business goals

Predictable
The process is enacted consistently within defined limits

Established
A defined process is used based on a standard process

Level 5	Optimizing process
PA 5.1	Process innovation attribute
PA 5.2	Process optimization attribute

Level 4	Predictable process
PA 4.1	Process measurement attribute
PA 4.2	Process control attribute

Level 3	Established process
PA 3.1	Process definition attribute
PA 3.2	Process deployment attribute

Level 2	Managed process
PA 2.1	Performance management attribute
PA 2.2	Work product management attribute

Managed
The process is managed and work products are established, controlled and maintained

Level 1	Performed process
PA 1.1	Process performance attribute

Performed
The process is implemented and achieves its process purpose

Level 0 Incomplete process

Incomplete
The process is not implemented or fails to achieve its purpose

COBIT 5-New Process Attribute Rating Scale

COBIT 5 assessment process measures the extent to which a given process achieves the process attributes:

N Not achieved → 0 to 15% achievement

P Partially achieved → 15% to 50% achievement

L Largely achieved → 50% to 85% achievement

F Fully achieved → 85% to 100% achievement

COBIT 5- Process Attribute Ratings and Capability Levels

		1	2	3	4	5
Level 5 - Optimizing	PA 5.2 Optimization PA 5.1 Innovation					L / F
Level 4 - Predictable	PA 4.2 Control PA 4.1 Measurement				L / F	F
Level 3 - Established	PA 3.2 Deployment PA 3.1 Definition			L / F	F	F
Level 2 - Managed	PA 2.2 Work product management PA 2.1 Performance management		L / F	F	F	F
Level 1 - Performed	PA 1.1 Process performance	L / F	F	F	F	F
Level 0 - Incomplete						

L/F = Largely or Fully F= Fully

RSA CONFERENCE ASIA PACIFIC 2013

5: ISO 27001 Certification Process

5. ISO 27001 Certification Process

RSA CONFERENCE ASIA PACIFIC 2013

6: Summary/ Recommendations

Cloud Controls-Summary/Recommendations

- Requests for third party Cloud Audits would get more common
- IT Control Objectives for Cloud Computing from ISACA serves as a useful reference guide
- Risk assessment / Risk based IT Audit aligned to COBIT 5
- Aligned to ISO 27001 Certification
- Check Compliance with local standards and guidelines (MAS)

e.g MAS Circular dated 14th July 2011– Risk Mitigation of Cloud Computing Risks through multi-tier cloud security (MTCS) standard .

Cloud ready Trade Finance & Biometric ATMs (in Retail Banking)

- Map Business Goals to IT Processes and the maturity of each Cloud deployment model against these attributes using the Templates in th Appendix of COBIT 5

References/ Acknowledgements

Author	Source
Samuel GreenGard	A Clear View of Cloud Security, August 2012
ISACA	IT Control Objectives for Cloud Computing, 2011 V 1.0 Controls and Assurance in the Cloud
ISACA	IT Audits for Clouds and SaaS, Information Systems Control Journal, Volume 3, 2010
ENISA (European Network and Information Agency)	Cloud Computing- Benefits, Risks and Recommendations for Information Security, November 2009

Questions

Contact

Indranil Mukherjee

Singapore ISC Pte Ltd

International Standards Certification

indranil@isc-singapore.com

(www.isc-worldwide.com)