COBIT ® 5 Foundation Workshop

COBIT is a trademark of the Information Systems Audit and Control Association and the IT Governance Institute
COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
Purpose -
COBIT 5 Foundation Certificate

- The purpose of the Foundation Certificate is to confirm that a candidate has sufficient knowledge and understanding of the COBIT 5 Guidance and Management of enterprise IT, create awareness with their business executives and senior IT Management; assess the current state of their Enterprise IT with the objective of scoping what aspects of COBIT 5 would be appropriate to implement.

- The Foundation level training and certificate is also a prerequisite for the following training and certificate courses
  - COBIT 5 Implementation Training & Certificate
  - COBIT 5 Assessor Training & Certificate
Target Audience for the COBIT 5 Foundation Level Training and Certificate

- Business Management
- Chief Executives
- IT/IS Auditors
- Information Security and IT Practitioners
- Consultants
- IT/IS Management
  - Looking to gain an insight into the Enterprise Governance of IT and looking to be certified as a COBIT Implementer or Assessor
High Level Learning Outcomes

- The candidate should understand the key principals and terminology within COBIT 5. Specifically the candidate should know and understand:
  - The major drivers for the development of a Framework.
  - The business benefits of using COBIT 5.
  - The COBIT 5 Product Architecture.
  - The IT management issues and challenges that affect enterprises.
  - The 5 Key Principles of COBIT 5 for the governance and management of Enterprise IT
  - How COBIT 5 enables to be governed and managed in a holistic manner for the entire enterprise.
  - Understand the key concepts in a Process Capability Assessment and the key attributes of the COBIT 5 PAM (Process Assessment Model)
  - How the COBIT 5 Processes and the Process Reference Model (PRM) help guide the creation of the 5 Principles and the 7 Governance and Management Enablers.
Structure of the Material

- The material is structured in 5 Learning Area Modules
- Based on two specific COBIT 5 Guides
  - The COBIT 5 ‘Business Framework for the Governance and Management of Enterprise IT’.
  - Supplementary Guide on Process Capability with extracts from the COBIT 4.1 and COBIT 5 PAM’s (Process Assessment Model).
  - Some aspects of the Enabling Process Guide have been used as examples for more detailed ‘walk through’ where appropriate Tips and Notes have been provided in each guide.
- Tips and Notes have been provided in each guide
Exam Requirement and Preparation

➢ Exam requirements :
  ✓ 50 Questions
  ✓ 40 minutes
  ✓ Closed book
  ✓ 50% pass required

➢ Exam preparation :
  ✓ Approximately 2 hours
  ✓ Comprises syllabus review
  ✓ Test Questions
Questions ?
Chapter 1

Overview of COBIT 5
Major drivers for the development of COBIT 5

- Provide more stakeholders a say in determining what they expect from information and related technology
- Address the increasing dependency of enterprise success on external business and IT parties such as outsourcers, suppliers, consultants, clients, cloud and other service providers.
- Deal with the amount of information, which has increased significantly.
- Deal with much more pervasive IT; it is more and more an integral part of the business.
- Provide further guidance in the area of innovation and emerging technologies.
- Cover the full end-to-end business and IT functional responsibilities.
- Get better control over increasing user-initiated and user-controlled IT solutions
✓ Achieve enterprise:
  – Value creation through effective and innovative use of enterprise IT
  – Business user satisfaction with IT engagement and services
  – Compliance with relevant laws, regulations, contractual agreements and internal policies
  – Improved relations between business needs and IT objectives

✓ Connect to, and, where relevant, align with, other major frameworks and standards in the marketplace, such as Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®), Project, Management Body of Knowledge (PMBOK®), Projects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards.

✓ Integrate all major ISACA frameworks and guidance, with a primary focus on COBIT, Val IT and Risk IT as one single framework
Benefits

• Information is the business currency of the 21st Century
  - Information has a life cycle: it is created, used, retained, disclosed and destroyed
  - Technology plays a key role in these actions.
  - Technology is becoming pervasive in all aspects of business and personal life.
  - Every form of enterprise needs to be able to rely on quality information to support quality executive decisions!
Enterprise Benefits

Enterprise 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 realize 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.
• Optimize the cost of IT services and technology.

How can these benefits be realized to create enterprise stakeholder value?
Stakeholder Value

• Delivering enterprise stakeholder value requires good governance and maintenance 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 compliances 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.
Benefits

- **COBIT 5:**
  - Defines the starting point of governance and management activities with the *stakeholder needs* related to enterprise IT.
  - Creates a more holistic, integrated and complete view of enterprise governance and management of IT that is consistent, provides end to end view on all IT-related matters and provides a holistic view.
  - Creates a common language between IT and business for the enterprise governance and management of IT.
  - Is consistent with generally accepted corporate governance standards, and thus helps to meet regulatory requirements.
Business Needs

- Enterprises are under constant pressure to:
  - Increase benefits realization through effective and innovation of enterprise IT
    - Generate business value from new enterprise investment with a supporting IT investment.
    - Achieve operational excellence through application of technology.
  - Maintain IT related risk at an acceptable level
  - Contain cost of IT services and technology
  - Ensure business and IT collaboration, leading to business 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:
  1. The Framework
  2. Process Reference Guide
  3. Implementation Guide

• COBIT 5 is based on:
  – 5 principles and
  – 7 enablers
COBIT 5 Product Family

Figure 1—COBIT 5 Product Family

COBIT® 5

COBIT 5 Enabler Guides
- COBIT® 5: Enabling Processes
- COBIT® 5: Enabling Information
- Other Enabler Guides

COBIT 5 Professional Guides
- COBIT® 5 Implementation
- COBIT® 5 for Information Security
- COBIT® 5 for Assurance
- COBIT® 5 for Risk
- Other Professional Guides

COBIT 5 Online Collaborative Environment
The COBIT 5 product family includes the following products:

• COBIT 5 (the framework)

• COBIT 5 enabler guides, in which governance and management enablers are discussed in detail. These include:
  – COBIT 5: Enabling Processes
  – COBIT 5: Enabling Information (in development)
  – Other enabler guides (check www.isaca.org/cobit)

• COBIT 5 professional guides, which include:
  – COBIT 5 Implementation
  – COBIT 5 for Information Security (in development)
  – COBIT 5 for Assurance (in development)
  – COBIT 5 for Risk (in development)
  – Other professional guides (check www.isaca.org/cobit)

• A collaborative online environment, which will be available to support the use of COBIT 5
COBIT 5 Mapping Summary
COBIT 5 Mapping Specifies

- **ISO/IEC 38500**
  - ISO’s 6 principles map to COBIT 5

- **ITIL v3** the following 5 areas and domains are covered by ITIL v3:
  - A subset of processes in the DSS domain
  - A subset of processes in the BAI domain
  - Some processes in the APO domain

- **ISO/IEC 27000**
  - Security and IT-related processes in domains EDM, APO, and DSS
  - Some monitoring of security activities in MEA

- **ISO/IEC 31000**
  - Risk management related activities in EDM and APO
➢ TOGAF (The Open Group Architecture Framework)
  ✓ TOGAF components of the architecture board and governance areas.
  ✓ Resource related processes in EDM
  ✓ Enterprise architecture processes of APO

➢ PRINCE2
  ✓ Programme and project management processes in the BAI domain
  ✓ Portfolio related processes in the APO domain

➢ CMM1
  ✓ Some organizational and quality related processes in the APO domain
  ✓ Application building and acquisition related processes in BAI
Questions ?
Chapter 2

COBIT 5 PRINCIPLES
COBIT 5 Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

Figure 2—COBIT 5 Principles
Principle 1: Meeting Stakeholder Needs

- Enterprises have many stakeholders
- Governance is about
  - Negotiating
  - Deciding amongst different stakeholder’s 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?
Enterprises exist to create value for their stakeholders

Value Creation: realizing benefits at an optimal resource cost while optimizing risk.
Stakeholder Needs have to be transformed into an enterprises actionable strategy

- The COBIT 5 Goals Cascade is the mechanism to translate Stakeholder Needs into specific, practical, and customized goals
- The COBIT5 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
COBIT 5
Goals Cascade
Step 1. Stakeholder Drivers Influence Stakeholder Needs
Step 2. Stakeholder Needs Cascade to Enterprise Goals
Step 3. Enterprise Goals Cascade to IT-related Goals
Step 4. IT-related Goals Cascade to Enabler Goals
Step 1. Stakeholder Drivers Influence Stakeholder Needs

- Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.

Step 2. Stakeholder Needs Cascade to Enterprise Goals

- Stakeholder needs can be related to a set of generic enterprise goals. These enterprise goals have been developed using the balanced scorecard (BSC) dimensions, and they represent a list of commonly used goals that an enterprise may define for itself. Although this list is not exhaustive, most enterprise-specific goals can be mapped easily onto one or more of the generic enterprise goals.

COBIT 5 defines 17 generic goals, which includes the following information:

- The BSC dimension under which the enterprise goal fits
- Enterprise goals
- The relationship to the three main governance objectives—benefits realization, risk optimization and resource optimization. (‘P’ stands for primary relationship and ‘S’ for secondary relationship, i.e., a less strong relationship.)
Step 3. Enterprise Goals Cascade to IT-related Goals

- Achievement of enterprise goals requires a number of IT-related outcomes, which are represented by the IT-related goals. IT-related stands for information and related technology, and the IT-related goals are structured along the dimensions of the IT balanced scorecard (IT BSC). COBIT 5 defines 17 IT-related goals.

Step 4. IT-related Goals Cascade to Enabler Goals

- Achieving IT-related goals requires the successful application and use of a number of enablers. Enablers include processes, organizational structures and information, and for each enabler a set of specific relevant goals can be defined in support of the IT-related goals.
## COBIT 5

### Internal Stakeholders

<table>
<thead>
<tr>
<th>Internal Stakeholders</th>
<th>Internal Stakeholder Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board</td>
<td>How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?</td>
</tr>
<tr>
<td>Chief executive officer (CEO)</td>
<td>How do I manage performance of IT?</td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>How can I best exploit new technology for new strategic opportunities?</td>
</tr>
<tr>
<td>Chief information officer (CIO)</td>
<td>How do I best build and structure my IT department?</td>
</tr>
<tr>
<td>Chief risk officer (CRO)</td>
<td>How dependent am I on external providers? How well are IT outsourcing agreements being managed?</td>
</tr>
<tr>
<td>Business executives</td>
<td>How do I obtain assurance over external providers?</td>
</tr>
<tr>
<td>Business process owners</td>
<td>What are the (control) requirements for information?</td>
</tr>
<tr>
<td>Business managers</td>
<td>Did I address all IT-related risk?</td>
</tr>
<tr>
<td>Risk managers</td>
<td>Am I running an efficient and resilient IT operation?</td>
</tr>
<tr>
<td>Security managers</td>
<td>How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options?</td>
</tr>
<tr>
<td>Service managers</td>
<td>Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance?</td>
</tr>
<tr>
<td>Human resource (HR) managers</td>
<td>How do I get assurance over IT?</td>
</tr>
<tr>
<td>Internal audit</td>
<td>Is the information I am processing well secured?</td>
</tr>
<tr>
<td>Privacy officers</td>
<td>How do I improve business agility through a more flexible IT environment?</td>
</tr>
<tr>
<td>IT users</td>
<td>Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy?</td>
</tr>
<tr>
<td>IT managers</td>
<td>How critical is IT to sustaining the enterprise? What do I do if IT is not available?</td>
</tr>
<tr>
<td>Etc.</td>
<td>What critical business processes are dependent on IT, and what are the requirements of business processes?</td>
</tr>
<tr>
<td></td>
<td>What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget?</td>
</tr>
<tr>
<td></td>
<td>How much of the IT effort goes to fighting fires rather than to enabling business improvements?</td>
</tr>
<tr>
<td></td>
<td>Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?</td>
</tr>
<tr>
<td></td>
<td>How long does it take to make major IT decisions?</td>
</tr>
<tr>
<td></td>
<td>Are the total IT effort and investments transparent?</td>
</tr>
<tr>
<td></td>
<td>Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?</td>
</tr>
</tbody>
</table>
## Figure 7—Governance and Management Questions on IT

<table>
<thead>
<tr>
<th>External Stakeholders</th>
<th>External Stakeholder Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business partners</td>
<td>How do I know my business partner’s operations are secure and reliable?</td>
</tr>
<tr>
<td>Suppliers</td>
<td>How do I know the enterprise is compliant with applicable rules and regulations?</td>
</tr>
<tr>
<td>Shareholders</td>
<td>How do I know the enterprise is maintaining an effective system of internal control?</td>
</tr>
<tr>
<td>Regulators/government</td>
<td>Do business partners have the information chain between them under control?</td>
</tr>
<tr>
<td>External users</td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td></td>
</tr>
<tr>
<td>Standardisation organisations</td>
<td></td>
</tr>
<tr>
<td>External auditors</td>
<td></td>
</tr>
<tr>
<td>Consultants</td>
<td></td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
</tr>
</tbody>
</table>
**Principle 2: Covering the Enterprise End-to-End**

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

- **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’.
This means that COBIT 5:

- Integrates the governance of enterprise IT into enterprise governance and
- Covers all functions and processes required to govern and manage enterprise information and related technologies wherever that information is processed.
- COBIT 5 addresses all relevant interval and external IT services as well as external and internal business processes.
Figure 8—Governance and Management in COBIT 5

Governance Objective: Value Creation

- Benefits Realisation
- Risk Optimisation
- Resource Optimisation

Governance Enablers

Governance Scope

Roles, Activities and Relationships
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.
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
  - Integrated all knowledge previously dispersed over different ISACA frameworks
  - Provides a simple architecture for structuring guidance materials and producing a consistent product set
Principle 4: Enabling a Holistic Approach
Enablers:
1. Principles, policies and framework
2. Processes
3. Organizational structure
4. Culture, ethics and behavior
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies
COBIT 5 defines a set of enablers to support the implementation of 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**
COBIT 5 Enabler Dimensions:

- All enablers have a set of common dimension 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
Figure 13—COBIT 5 Enablers: Generic

Enabler Dimension

Stakeholders
- Internal Stakeholders
- External Stakeholders

Goals
- Intrinsic Quality
- Contextual Quality (Relevance, Effectiveness)
- Accessibility and Security

Life Cycle
- Plan
- Design
- Build/Acquire/Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

Good Practices
- Practices
- Work Products (Inputs/Outputs)

Enabler Performance Management

Are Stakeholders Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)
The 4 Common Dimensions for Enablers:

- **Stakeholders**—Each enabler has stakeholders (parties who play an active role and/or have an interest in the enabler).
  - Stakeholders can be internal or external to the enterprise, all having their own, sometimes conflicting, interests and needs.
  - Stakeholders’ needs translate to enterprise goals, which in turn translate to IT-related goals for the enterprise.

- **Goals**—Each enabler has a number of goals, and enablers provide value by the achievement of these goals. Goals can be defined in terms of:
  - Expected outcomes of the enabler
  - Application or operation of the enabler itself.

The enabler goals are the final step in the COBIT 5 goals cascade. Goals can be further split up in different categories:

- **Intrinsic quality**—The extent to which enablers work accurately, objectively and provide accurate, objective and reputable results

- **Contextual quality**—The extent to which enablers and their outcomes are fit for purpose given the context in which they operate. For example, outcomes should be relevant, complete, current, appropriate, consistent, understandable and easy to use.

- **Access and security**—The extent to which enablers and their outcomes are accessible and secured, such as:
  - Enablers are available when, and if, needed.
  - Outcomes are secured, i.e., access is restricted to those entitled and needing it.
Life cycle—Each enabler has a life cycle, from inception through an operational/useful life until disposal. This applies to information, structures, processes, policies, etc. The phases of the life cycle consist of:

- Plan (includes concepts development and concepts selection)
- Design
- Build/acquire/create/implement
- Use/operate
- Evaluate/monitor
- Update/dispose

Good practices—For each of the enablers, good practices can be defined.

- Good practices support the achievement of the enabler goals. Good practices provide examples or suggestions on how best to implement the enabler, and what work products or inputs and outputs are required. COBIT 5 provides examples of good practices for some enablers provided by COBIT 5 (e.g., processes). For other enablers, guidance from other standards, frameworks, etc., can be used.
Enterprises expect positive outcomes from the application and use of enablers. To manage performance of the enablers, the following questions will have to be monitored and thereby subsequently answered—based on metrics—on a regular basis:

- Are stakeholder needs addressed?
- Are enabler goals achieved?
- Is the enabler life cycle managed?
- Are good practices applied?

The first two bullets deal with the actual outcome of the enabler. The metrics used to measure to what extent the goals are achieved can be called ‘lag indicators’.

The last two bullets deal with the actual functioning of the enabler itself, and metrics for this can be called ‘lead indicators’.
Principle 5: Separating Governance and 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 domain
Figure 15—COBIT 5 Governance and Management Key Areas

Business Needs

Governance

Evaluate

Direct

Monitor

Management Feedback

Management

Plan (APO) → Build (BAI) → Run (DSS) → Monitor (MEA)
Figure 16—COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Supplier
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programme and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablers
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance with External Requirements
 Governance

- Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

In most enterprises, governance is the responsibility of the board of directors under The leadership of the chairperson.

 Management

- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.
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)
Chapter 3

COBIT 5 IMPLEMENTATION GUIDANCE
COBIT 5 Implementation

- ISACA has developed the COBIT 5 Framework to help enterprises implement sound governance enablers. Indeed, implementing good GEIT almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT 5.

- However, frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.

- COBIT 5 implementation provides guidance on how to do this.
Enterprise Internal and External Environment

- Understanding the Enterprise Internal and External Environment as they apply to change management such as:
  - Ethics and culture
  - Applicable laws, regulations, policies
  - Mission, vision and values
  - Governance policies and practices
  - Business plans and strategic intentions
  - Operating model
  - Management style
  - Risk appetite
  - Capabilities and available resources
  - Industry practices
Key Success factors

- Top management providing the direction and mandate for the initiative as well as on-going commitment
- All parties supporting the governance and management processes to understand the business and IT objectives
- Ensuring effective communication and enablement of the necessary changes
- Tailoring COBIT and other supporting good practices and standard to fit the unique context of the enterprise and
- Focusing on quick wins and prioritizing most beneficial improvements that are easiest to implement.
Seven Phases –
Implementation Life Cycle

- 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?
Figure 17—The Seven Phases of the Implementation Life Cycle

1. What are the drivers?
2. Where are we now?
3. Where do we want to be?
4. What needs to be done?
5. How do we get there?
6. Did we get there?
7. How do we keep the momentum going?

- Programme management (outer ring)
- Change enablement (middle ring)
- Continual improvement life cycle (inner ring)
Phase 1 starts with recognizing and agreeing to the need for an implementation or improvement initiative. It identifies the current pain points and triggers and creates a desire to change at executive management levels.

Phase 2 is focused on defining the scope of the implementation or improvement initiative using COBIT’s mapping of enterprise goals to IT-related goals to the associated IT processes, and considering how risk scenarios could also highlight key processes on which to focus. An assessment of the current state is then performed, and issues or deficiencies are identified by carrying out a process capability assessment.

During phase 3, an improvement target is set, followed by a more detailed analysis leveraging COBIT’s guidance to identify gaps and potential solutions. Some solutions may be quick wins and others more challenging and longer-term activities. Priority should be given to initiatives that are easier to achieve and those likely to yield the greatest benefits.

Phase 4 plans practical solutions by defining projects supported by justifiable business cases. A change plan for implementation is also developed. A well-developed business case helps to ensure that the project’s benefits are identified and monitored.
In phase 5, the proposed solutions are implemented into day-to-day practices. Measures can be defined and monitoring established, using COBIT’s goals and metrics to ensure that business alignment is achieved and maintained and performance can be measured. Success requires the engagement and demonstrated commitment of top management as well as ownership by the affected business and IT stakeholders.

Phase 6 focuses on the sustainable operation of the new or improved enablers and the monitoring of the achievement of expected benefits.

During phase 7, the overall success of the initiative is reviewed, further requirements for the governance or management of enterprise IT are identified, and the need for continual improvement is reinforced.
Phase 1:
What are the Drivers?

- Initiate the programme
- Establish desire to change
- Recognize need to act
Need for new or improved IT governance organization is usually recognized by **pain points or trigger events**.

Board and executive management should:

- Analyze pain points to identify root cause
- Look for opportunities during trigger events

The goal of this phase of the lifecycle includes:

- Outlining the business
- Identification of stakeholders and roles & responsibilities
- IT governance program “wake-up call” and kick-off communications.
Typical Pain Points

✓ Failed IT initiatives
✓ Rising costs
✓ Perception of low business value for IT investments
✓ Significant incidents related to IT risk (e.g. data loss)
✓ Service delivery problems
✓ Failure to meet regulatory or contractual requirements
✓ Audit findings for poor IT performance or low service levels
✓ Hidden and /or rogue IT spending

✓ Resources waste through duplication or overlap in IT initiatives
✓ Insufficient IT resources
✓ IT staff burnout/ dissatisfaction
✓ IT enabled changes frequent falling to meet business needs (late deliveries or budget overruns)
✓ Multiple and complex IT assurance efforts
✓ Board members or senior managers that are reluctant engage with IT.
Relevant Trigger Events

- Merger, acquisition or divestiture
- Shift in market, economy or competitive position
- Change in business operating model or sourcing arrangements
- New regulatory or compliance requirements
- Significant technology change or paradigm shift
- An enterprise wise governance focus or project
- A new CIO, CFO, COO
- External audit or consultant assessments
- A new business strategy or priority

By using pain points or trigger events as the launching point for IT governance initiatives, the business case for GEIT improvements can be related to issues being experienced which will improve buy-in to the business case.
Phase 2:
Where are We now?

- Define the problems and opportunities [Programme management]
  - Understand the pain points that have been identified as governance problems
  - Take advantages of trigger events that provide opportunity for improvement

- Form a powerful guiding team [change enablement]
  - Knowledge of business environment
  - Insight into influencing factors

- Assess the current state [continual improvement life cycle attribute]
  - Identify the IT goals in respect to enterprise goals
  - Identify the most important processes
  - Understand management risk appetite
  - Understand the maturity of existing governance
  - Related processes
Phase 3: Where Do We Want To Be?

- Define the roadmap
  - Describe the high level change enablement plan and objectives

- Communicate desired vision
  - Develop a communication strategy
  - Communicate the vision
  - Articulate the rationale and benefits of the change
  - Set the tone at the top

- Define target state and perform gap analysis
  - Define the target for improvement
  - Analyze the gaps
  - Identify potential improvements
Phase 4: What Needs To Be Done?

- **Develop program plan**
  - Prioritize potential initiatives
  - Develop formal and justifiable projects
  - Use plans that include contribution and program objectives

- **Empower role players and identify quick wins**
  - High benefit, easy implementations should come first
  - Obtain buy-in by key stakeholders affected by the change
  - Identify strengths in existing processes and leverage accordingly.

- **Design and build improvements**
  - Plot improvements onto a grid to assist with prioritization
  - Consider approach, deliverables, resources needed, costs, estimated time scales, project dependencies and risks.
Phase 5: How Do We Get There?

- **Execute the plan**
  - Execute projects according to an integrated program plan
  - Provide regular update reports to stakeholders
  - Documents and monitor the contribution of projects while managing risks identified

- **Enable operation and use**
  - Build on the momentum and credibility of quick wins
  - Plan cultural and behavioral aspects of the broader transition
  - Define measures of success

- **Implement improvements**
  - Adopt and adapt best practices to suit the enterprise’s approach to policies and process changes
Phase 6: Did We Get There?

- **Realize benefits**
  - Monitor the overall performance of the program against business case objectives
  - Monitor and measure the investment performance

- **Embed new approaches**
  - Provide transition from project mode to business as usual mode
  - Monitor whether new roles and responsibilities have been taken on
  - Track and assess objectives of the change response plans
  - Maintain communication and ensure communication between appropriate stakeholders continues

- **Operated and measure**
  - Set targets for each metric
  - Measure metrics against targets
  - Communicate results and adjust targets as necessary
Phase 7: How Do We Keep Momentum

- Continual improvements – keeping the momentum is critical to sustainment of the lifecycle
- Review the program benefits
  - Review program effectiveness through a program review gathered
- Sustain
  - Conscious reinforcement (reward achievers)
  - Ongoing communication campaign (feedback on performance)
  - Continuous top management commitment
- Monitor and evaluate
  - Identify new governance objectives based on program experience
  - Communicate lessons learned and further improvement requirements for the next iteration of the cycle
Making the Business Case

The characteristics of a good business case:

- The importance of a business case cannot be overstated. An appropriate level of urgency needs to be instilled and the key stakeholders should be aware of the risk of not taking action. An initiative should be owned by a sponsor (senior), involve all key stakeholders, and be based on a business case.

- Initially this can be a high-level business case dealing with the strategic benefits and costs and then progress to a more detailed business case. It is a valuable tool available to management in guiding the creation of business value.
Characteristics of Good Business Case

- At a minimum a Business case should include:
  - The business benefits that will be realized
  - The business changes required
  - The investments needed
  - The on-going IT operating costs
  - Constraints and dependencies delivered from the risk assessment
  - Roles, responsibilities and accountabilities relative to other initiative.
  - How the investment will be monitored.
Chapter 3

COBIT 5 ENABLERS
The COBIT 5 Enterprise Enablers

Figure 12—COBIT 5 Enterprise Enablers

1. Principles, Policies and Frameworks
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Recap 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
Recap Principle 4 : Enabling a Holistic Approach

COBIT 5 enabler dimensions :

- All enablers have a set of common dimensions that:
  - Provides a common, simple and structured way to deal with enablers
  - Allow an entity to manage its complex interactions
  - Facilitate successful outcomes of the enablers
Enabler 1: Principles, Policies & Framework
The purpose of this enabler is to convey the governing body’s management direction and instructions. They are instruments communicate the rules of the enterprise, in support of the governance objectives and enterprise values as defines by the board and executive management.

Differences between principles and policies –

- Principles need to be limited in number
- Put in simple language, expressing as clearly as possible the core values of the enterprise
- Policies are more detailed guidance on how to put principles into practice
The characteristics of good policies; they should:
- Be effective – achieve their purpose
- Be efficient – especially when implementing them
- Non-intrusive – Should make sense and be logical to those who have to comply with them

Policies should have a mechanism (framework) in place where they can be effectively managed and users know where to go. Specifically, they should be:
- Comprehensive, covering all required areas
- Open and flexible allowing for easy adaptation and change.
- Current and up to date

The purpose of a policy life cycle is that it must support a policy framework in order to achieve defined goals.
The Good Practice Requirements for policies and frameworks, are important, specifically:

- Their Scope
- Consequences of falling to comply with the policy
- The means of handling exceptions
- How they will be monitored

The links and relationships between principles, policies and frameworks and other enablers:

- Principles, policies and frameworks reflect the culture, ethics and values of the enterprise
- Processes are the most important vehicle for executing policies
- Organizational structures can define and implement policies
- Policies are part of information
Enabler 2: Processes

Figure 29—COBIT 5 Enabler: Processes

- **Stakeholders**
  - Internal Stakeholders
  - External Stakeholders

- **Goals**
  - Intrinsic Quality
  - Contextual Quality (Relevance, Effectiveness)
  - Accessibility and Security

- **Life Cycle**
  - Plan
  - Design
  - Build/Acquire/Create/Implement
  - Use/Operate
  - Evaluate/Monitor
  - Update/Dispose

- **Good Practices**
  - Process Practices, Activities, Detailed Activities
  - Work Products (Inputs/Outputs)

**Enabler Performance Management**

- Are Stakeholders Needs Addressed?
- Are Enabler Goals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

**Metrics**

- Metrics for Achievement of Goals (Lag Indicators)
- Metrics for Application of Practice (Lead Indicators)
**Enabler 2 Process - Definitions**

- **A process is defined** as a collection of practices influenced by the enterprise's policies, and procedures that takes inputs from a number of sources (including other processes) manipulates the inputs and produces outputs (e.g., products and services).

- **Process Practices** are defined as the ‘guidance’ necessary to achieve process goals.

- **Process Activities** are defined as the ‘Guidance’ to achieve management practices for successful governance and management of enterprise IT.

- **Inputs and Outputs** are the process work products/artifacts considered necessary to support operation of the process.
Each process is divided into:

- Process description
- Process Purpose statement
- IT-related Goals (from the Goals cascade see example in the Appendix)
- Each IT-related goal is associated with a set of generic related metrics
- Process goals (Also from the goals cascade mechanism and is referred to as Enabler goals)
- Each process contains a set of Management Practices
- These are associated with a generic RACI chart (Responsible, Accountable, Consulted, Informed)
- Each management practice contains a set of inputs and outputs (called work products in module PC)
- Each management Practice is associated with a set of activities
Processes complements COBIT 5 and contains a detailed reference guide to the processes that are defined in the COBIT 5 process reference model:

- The COBIT 5 goals cascade is recapitulated and complemented with a set of example metrics for the enterprise goals and the IT related goals.
- The COBIT 5 process model is explained and its components defined.
- The Enabler process guide which is referenced in this module contains the detailed process information for all 37 COBIT 5 processes shown in the process reference model.
COBIT 5 : Enabling Processes

- The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas - governance and management – with management further divided into domains of processes:
  - The GOVERNANCE domain contains five Governance Processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
  - The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM)
Figure 30—COBIT 5 Governance and Management Key Areas

Business Needs

Governance

Evaluate

Direct

Management Feedback

Monitor

Management

Plan (APO)

Build (BAI)

Run (DSS)

Monitor (MEA)
The PRM is divided into a Governance Domain with 5 Processes titled EDM (Evaluate, Direct and Monitor)

Four management domains titled APO (Align, Plan and Organize); BAI (Build, Acquire and Implement) DSS (Deliver, Service and Support) and MEA (Monitor, Evaluate and Assess)

APO contains 13 processes, BAI 10 processes, DSS 6 processes and MEA 3 processes

This makes a total of 37 processes, 32 for management and 5 for Governance
Key Characteristics of Process Goals:

- Process Goals are defined as a statement describing the desired outcome of a process. An outcome can be an artifact, a significant change of a state or a significant capability improvement of other processes. They are part of the goals cascade in which process goals link to IT-related goals which link to enterprise goals.

- **Intrinsic Goals**
  - Does the process have intrinsic quality? Is it accurate and in line with good practice? Is it compliant with internal and external rules?

- **Contextual Goals**
  - Is the process customized and adapted to the enterprise’s specific situation? Is the process relevant, understandable, easy to apply?

- **Accessibility and Security Goals**
  - The process remains confidential, when required, and is known and accessible to those who need it.
Relationship between Process and other enablers:

- Processes need information as one form of input.
- Processes need organizational structure.
- Processes produce and require services, infrastructure and applications.
- Processes are dependent on other processes.
- Processes need policies and procedures to ensure consistent implementation.
Enabler 3: Organizational Structures

Figure 32—COBIT 5 Enabler: Organisational Structures

Enabler Dimension

- Stakeholders
  - Internal Stakeholders
  - External Stakeholders
- Goals
  - Intrinsic Quality
  - Contextual Quality (Relevance, Effectiveness)
  - Accessibility and Security
- Life Cycle
  - Plan
  - Design
  - Build/Acquire/Create/Implement
  - Use/Operate
  - Evaluate/Monitor
  - Update/Dispose
- Good Practices
  - Practices: Operating Principles, Span of Control (Scope), Level of Authority, Delegation of Authority, Escalation Procedures
  - Work Products (Inputs/Outputs): Decisions

Enabler Performance Management

- Are Stakeholders Needs Addressed?
- Are Enabler Goals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

- Metrics for Achievement of Goals (Lag Indicators)
- Metrics for Application of Practice (Lead Indicators)
A number of Good Practices of organizational structure can be distinguished such as:

- **Operating principles** – The practical arrangements regarding how the structure will operate, such as meeting frequency documenting and other rules.
- **Span of control** – The boundaries of the organization structure’s decision rights.
- **Level of authority** – the decisions that the structure is authorized to take.
- **Delegation of responsibility** – The structure can delegate a subset of its decision rights to other structures reporting to it.
- **Escalating procedures** – The escalating path for a structure describes the required actions in case of problems in making decisions.
Enabler 4: Culture, Ethics and Behavior

Figure 34—COBIT 5 Enabler: Culture, Ethics and Behaviour

- **Stakeholders**
  - Internal Stakeholders
  - External Stakeholders

- **Goals**
  - Intrinsic Quality
  - Contextual Quality (Relevance, Effectiveness)
  - Accessibility and Security

- **Life Cycle**
  - Plan
  - Design
  - Build/Acquire/Create/Implement
  - Use/Operate
  - Evaluate/Monitor
  - Update/Dispose

- **Good Practices**
  - Practices:
    - Communication
    - Enforcement
    - Incentives and Rewards
    - Awareness
    - Rules and Norms
    - Champions
  - Work Products (Inputs/Outputs)

- **Enabler Performance Management**
  - Are Stakeholders Needs Addressed?
  - Are Enabler Goals Achieved?
  - Is Life Cycle Managed?
  - Are Good Practices Applied?

- **Metrics**
  - Metrics for Achievement of Goals (Lag Indicators)
  - Metrics for Application of Practice (Lead Indicators)
Good practices for creating, encouraging and maintaining desired behavior throughout the enterprise include:

- Communication throughout the enterprise of desired behaviors corporate values. (This can be done via a code of ethics).
- Awareness of desired behavior, strengthened by senior manager. Example. This is one of the keys to a good governance environment when senior management and the executives walk the talk so to speak. It is sometimes a difficult areas and one that causes many enterprises to fail because it leads to poor governance. (Typically will be part of a training and awareness sessions around areas of ethics)
- Incentives to encourage and deterrents to enforce desired behavior. There is a clear link to HR payment and reward schemes.
- Rules and norms which provide more guidance and will typically be found in a Code of Ethics.
Relationship of Goals for culture, ethics and behavior

- Organizational Ethics determine by the values by which the enterprise to live (its code)

- Individual ethics determined by each person’s personal values and dependent to some extent on external factors not always under the enterprise’s control such as religion, ethnicity, etc.

- Individual behaviors which collectively determine the culture of the enterprise and is dependent on both organizational and individual ethics. Some examples are:
  - Behavior towards risk taking
  - Behavior towards the enterprise’s principles and policies.
  - Behavior towards negative outcomes, e.g. loss events
The relationship of this enabler is to other enablers

- Links to processes for execution process activities
- Links to organizational structures for the implementation of decisions and
- Links to principles and policies to be able to communicate the corporate values. (many organizations include their code of ethics with their policies)
Enabler 5: Information

Figure 36—COBIT 5 Enabler: Information

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Goals</th>
<th>Life Cycle</th>
<th>Good Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Stakeholders</td>
<td>Intrinsic Quality</td>
<td>Plan</td>
<td>Practices: Define Information Attributes</td>
</tr>
<tr>
<td>External Stakeholders</td>
<td>Contextual Quality (Relevance, Effectiveness)</td>
<td>Design</td>
<td>- Physical (Carrier, Media)</td>
</tr>
<tr>
<td></td>
<td>Accessibility and Security</td>
<td>Build/Acquire/Create/Implement</td>
<td>- Empirical (User Interface)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use/Operate</td>
<td>- Syntactic (Language, Format)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evaluate/Monitor</td>
<td>- Semantic (Meaning), Type, Currency, Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update/Dispose</td>
<td>- Pragmatic (Use), Includes Retention, Status, Contingency, Novelty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Social (Context)</td>
</tr>
</tbody>
</table>

Enabler Performance Management

- Are Stakeholders Needs Addressed?
- Are Enabler Goals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)

Metrics for Application of Practice (Lead Indicators)
Information Stakeholders

- Information producer - responsible for creating the information
- Information custodian - responsible for storing and maintaining the information
- Information consumer - responsible for using the information
Importance of the Information Quality categories and dimensions;

- The concept of information criteria was introduced in COBIT 4.1; these were very important to be able to show how to meet business requirements.

Importance of Information Criteria

- COBIT 4.1 introduces us to the concept of 7 Key information criteria to meet Business requirements. This concept has been retained but translated differently.
To satisfy business objectives, information needs to conform to certain control criteria which COBIT refers to as business requirements for information. Base broader quality, fiduciary and security requirements, seven distinct information criteria are defined. These are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability
The attributes required to assess the context and quality of information to the user, specifically

- Relevancy – The extent to which information is applicable and helpful for the task at hand.
- Completeness – the extent to which information is not missing and is of sufficient depth and breadth for the task at hand.
- Appropriateness – The extent to which the volume of information is appropriate for the task at hand.
- Conciseness – The extent to which the information is compactly represented.
- Consistency – The extent to which the information is presented in same format.
- Understandability – The extent to which the information is easily understandable.
- Ease of Manipulation – The extent to which information is easy to manipulate and to apply to different tasks.
COBIT 5 Enabler 5 Information – Meta data
Information Cycle

Figure 35—COBIT 5 Metadata—Information Cycle
Information attributes applied to the following layers:

- **Physical World Layer** – The world where all phenomena that can be empirically observed takes place.
  - The attribute that identifies the physical carrier of the information, e.g., paper, electric signals, sound waves

- **Empirical layer** – The empirical observation of the signs used to information and their distinction from each other.
  - The attribute that identifies the access channel of the information, e.g., user interfaces
- **Syntactical Layer** – The rules and principles for constructing sentence in natural or artificial language. Syntax refers to the form of information.
  - **Attribute that identifies the representational language/format used for encoding the information and the rules for combining the symbols of the language to form syntactic structures.**

- **Semantic layer** – The rules and principles for constructing meaning out of the syntax structures.
  - **Semantics refers to the meaning of information.**
    - **Information type**—The attribute that identifies the kind of information, e.g., financial vs. non-financial information, internal vs. external origin of the information, forecasted/predicted vs. observed values, planned vs. realized values
    - **Information currency**—The attribute that identifies the time horizon referred to by the information, i.e., information on the past, the present or the future
    - **Information level**—The attribute that identifies the degree of detail of the information, e.g., sales per year, quarter, month
Pragmatic layer – The rules and structures for constructing layer language structures that fulfill specific purposes in human communication. Pragmatics refers to the use of information.

- Retention period—The attribute that identifies how long information can be retained before it is destroyed
- Information status—The attribute that identifies whether the information is operational or historical
- Novelty—The attribute that identifies whether the information creates new knowledge or confirms existing knowledge, i.e., information vs. confirmation
- Contingency—The attribute that identifies the information that is required to precede this information (for it to be considered as information)

Social World layer – The world that is socially constructed the use of language structures at the pragmatic level of semi e.g. contracts, laws, culture.

- The possible used of the Information Model
  - Use for Information Specifications
  - Use to determine required protection
  - Used to determine ease of data Use.
Enabler 6: Services, Infrastructure and Applications
Five architecture principles that govern the implementation and use of IT-Related resources

This is part of the Good Practices of this enabler

Architecture Principles are overall guidelines that govern the implementation and use of IT-related resources within the enterprise. Examples of such principles:

- **Reuse** - Common components of the architecture should be used when designing and implementing solutions as part of the target or transition architectures.
- **Buy vs. build** – Solutions should be purchased unless there is an approved rationale for developing them internally.
- **Simplicity** – The enterprise architecture should be designed and maintained to be simple as possible while still meeting enterprise requirements.
- **Agility** – The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.
- **Openness** – The enterprise architecture should leverage open industry standards.
Relationship To other Enablers

- **Information** - is a service capability that is leveraged through processes to deliver internal and external services.

- Cultural and behavioral aspects – relevant when a service-oriented culture needs to be built

- Process inputs and outputs - Most of the inputs and outputs (work products) of the process management practices and activities in the PRM include service capabilities.
Enabler 7:
People, Skills and Competencies

Figure 38—COBIT 5 Enabler: People, Skills and Competencies

- Stakeholders:
  - Internal Stakeholders
  - External Stakeholders

- Goals:
  - Intrinsic Quality: Education and Qualifications, Technical Skill
  - Contextual Quality (Relevance, Effectiveness): Experience, Knowledge, Behavioural Skill, Availability, Turnover
  - Accessibility and Security

- Life Cycle:
  - Plan
  - Design
  - Build/Acquire/Create/Implement
  - Use/Operate
  - Evaluate/Monitor
  - Update/Dispose

- Good Practices:
  - Practices: Define Role Skill Requirements, Skill Levels, Skill Categories
  - Work Products (Inputs/Outputs): Skill Definitions

Enabler Performance Management

- Are Stakeholders Needs Addressed?
- Are EnablerGoals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)
Identify the good practices of People, Skills and Competencies, specifically:

- Described by different skill levels of different roles.
- Defining Skill categories requirements for each role.
- Mapping skill categories to COBIT 5 process domains (APO; BAI etc)
- These correspond to the with IT-related activities undertaken, e.g. Business analysis, information management etc.
- Using external sources for good practices
- There exist in frameworks such as ITIL 3; which contains extensive guidance on how to design and operate services.
- Consider also TOGAF (www.opengroup.org/togaf) which provides an integrated information infrastructure reference model.
Questions ?
Chapter 4

COBIT 4.1 Differences to COBIT 5
Transition Message

- COBIT 4.1, Val IT and Risk IT users who are already engaged in governance of enterprise IT (GEIT) implementation activities can transition to COBIT 5 and benefit from the latest and improved guidance that it provides during the next iterations of their enterprise’s improvement life cycle.

- 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.
Areas of Change

The following slides summaries the major changes in COBIT content and how they may impact GEIT implementation/improvement:

1. New GEIT Principles
2. Increase Focus on Enablers
3. New Process Reference Model
4. New and Modified processes separating Governance from Management
5. Practices and Activities
6. Revised and Expanded Goals and Metrics
7. Inputs and Outputs provided at Management verse process level in COBIT4.1
8. Expanded RACI charts at management process
9. New process Capability Maturity Model.
The goals cascaded 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 cascaded 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 cascaded 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 2\textsuperscript{nd} Edition (1998)
    - Focus on Control Objectives
  - An IT management framework?
    - COBIT 3\textsuperscript{rd} Edition (2000)
    - Management guidelines added.
  - An IT governance framework?
    - COBIT 4.0 (2005) and COBIT 4.1 (2007)
    - Governance and compliances process added
    - Assurance processes removed
What is the difference between governance and management?

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)
1. New GEIT Principles

- 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 divided 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!
• 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.
• Organizational structure was implied through the responsible, accountable, consulted or informed (RACI) roles and their definitions.
• Culture, ethics and behavior were mentioned in 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).
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 enterprise 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.

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

- COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives and Val IT and Risk IT processes.
- 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 one new model, making it easier for users to understand and use this material when implementing improvements.
6. Enhanced 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. Revised and Enhanced Inputs and Outputs

- COBIT 5 provides inputs and outputs for every management practice whereas COBIT 4.1 only provides 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. Expanded RACI Charts

- COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to COBIT 4.1, 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.
9. New Process Capability Assessment Model

- COBIT 5 discontinues the COBIT 4.1, Val IT and Risk IT CMM-based capability maturity modeling 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. COBIT 5 will be launched soon; a supplementary guide has been provided for ATO’s
  - [www.isaca.org/Knowledge-Center/cobit/Pages /COBIT-Assessment-Programme.aspx](http://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.
• 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 assessment by accredited assessors (assessor training is being developed)
  – Last 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 assessment aligned to the ISO/IEC standard.
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.
Questions ?
Chapter 5

COBIT 5 Process Capability Model
What is a Process Assessment

- ISO/IEC 15504 identifies process assessment as an activity that can be performed as part of a process improvement initiative or as part of a capability determination approach.
- The purpose of process improvement is to continually improve the enterprise’s effectiveness and efficiency.
- The purpose of process capability determination is to identify the strengths, weaknesses and risk of selected processes with respect to a particular specified requirement through the processes used and their alignment with the business need.
- It provides an understandable, logical, reputable, reliable and robust methodology for assessing the capability of IT processes.
Process Capability Assessment

• 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 assessment by accredited assessors
  – Less rigorous self-assessment for internal gap analysis and process improvement planning

• The COBIT Assessment Programme potentially enables an enterprise to obtain an independent and certified assessments aligned to the ISO/IEC standards.
What is the COBIT Assessment Program?

- The COBIT Assessment Program includes:
  - COBIT Process Assessment Model (PAM) – using COBIT 4.1
  - COBIT Process Assessment Model (PAM) – using COBIT 5
  - COBIT Assessor’s Guide – using COBIT 4.1
  - COBIT Assessor’s Guide – using COBIT 5.0
  - COBIT Self Assessor’s Guide – using COBIT 4.1
  - COBIT Self Assessor’s Guide – using COBIT 5.0

- The COBIT Process Assessment Model (PAM) brings together two proven heavyweights in the IT arena, ISO and ISACA.

- The COBIT PAM adapts the existing COBIT 4.1 & COBIT 5.0 content into an ISO 15504 compliant process assessment model.
Process Capability Assessment

- **COBIT Process Assessment Model (PAM): Using COBIT 4.1 & COBIT 5.0**
  - Serves as a base reference document for the performance of a capability assessment of an organization's current IT processes against COBIT

- **COBIT Assessors Guide : Using COBIT 4.1 & COBIT 5.0**
  - Provides details on how to undertake a full ISO-compliant assessment

- **COBIT Self-Assessment Guide : Using COBIT 4.1 & COBIT 5.0**
  - Provides guidance on how to perform a basic self-assessment against COBIT processes.
Differences Between a Capability & Maturity Assessment

- Historically most frameworks from COBIT, ITIL to PRINCE2 have adopted the SEI (Software Engineering Institute) CMMI approach which combines a Capability and a Maturity Assessment into a single assessment.

- ISO 15504 argues that they are two separate assessments:
  - **A Maturity Assessment** is done at an Enterprise or Organizational level and uses a different measurement scale than a capability assessment and different criteria and attributes.
  - **A Capability Assessment** is done at a Process Level and is done for purpose of process improvement. You cannot ‘role up’ an assessment of many different processes mathematically to an enterprise level. It works for SEI’s CMMI because they are assessing a single process, software engineering development or application development. Most frameworks like COBIT contain 34 and 37 processes respectively for COBIT 4.1 and COBIT 5.
  - So the concept of a Maturity Assessment has been redeveloped in COBIT 5 to the ISO 15504 Process Capability Assessment.
Differences to a CMM Model?

- But don’t we already have maturity models for COBIT 4.1 processes?
- The new COBIT Assessment Program
  - A robust assessment process based on ISO 15504
  - Aligns COBIT’s maturity model scale with ISO 15504 standard
  - New capability based assessment model includes:
    - Specific process requirements derived from COBIT 4.1
    - Ability of process to achieve process attributes based on 15504
    - Evidence requirements
    - Assessors qualifications and experiential requirements.
- Results in a more robust, objective and reputable assessment.
- Assessment results will likely vary from existing COBIT maturity models.
- COBIT 5 only adopts the ISO 15504 approach
Process Capability Assessment Differences COBIT 4.1 & 5

- The key difference to note from the above definitions:
  - A Maturity Assessment is done at an Enterprise organizational level and uses a different measurement scale than a capability Assessment different criteria and attributes.
  - A Capability Assessment is done at a process level and is done for purposes of process improvement.
Advantages of the ISO 15504 Approach

- A robust assessment process based on ISO 15504
- An alignment of COBIT’s maturity model scale with the internal standard
- A new capability-based assessment model which includes:
  - Specific process requirements derived from COBIT 4.1 & COBIT 5
  - Ability to achieve process attributes based on ISO 15504
  - Evidence requirements
- Assessors qualifications and experiential requirements
- Results in a more robust, objective and reputable assessment.
Key ISO 15504 definitions

- ISO 15504 defines the following key terms:
- **Process purpose** – The high-level measurable objectives of performing the process and the likely outcomes of effective implementation of the process.
- **Process Outcomes** - an observable result of a process (Note: An outcome is an artifact, a significant change of state or the meeting of specified constraints.)
- **Base practices** – the activities that, when consistently performed, contribute to achieving the process purpose
- **Work product** – an artifact associated with the execution of a process – defined in terms of process ‘inputs’ and process ‘outputs’.
COBIT 5 Process Reference Model

Figure 16—COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Security Transparency

Align, Plan and Organise

- AP001 Manage the IT Governance Framework
- AP002 Manage Relationships
- AP003 Manage Service Agreements
- AP010 Manage Stakeholders
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security
- AP014 Manage Innovation
- AP015 Manage Portfolio
- AP016 Manage Budget and Costs
- AP017 Manage Human Resources

Build, Acquire and Implement

- BAO01 Manage Programmes and Projects
- BAO02 Manage Requirements Definition
- BAO03 Manage Solutions Identification and Build
- BAO04 Manage Availability and Capacity
- BAO05 Manage Organisational Change Management
- BAO06 Manage Change Management and Transitioning
- BAO07 Manage Knowledge Management
- BAO08 Manage Assets
- BAO09 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security
- DSS06 Manage Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Compliance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance with External Requirements
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
- Initiate a new set of assessments
The Process Assessment Model (PAM) Explained
PAM Scope

- A Process Assessment Model is related to one or more Process Reference Models. It forms the basis for the collection of evidence and rating of process capability. A Process Assessment Model shall relate to at least one process from the specified Process Reference Model(s).

- A Process Assessment Model shall address, for a given process, all, or a continuous subset of the levels (starting at level 1) of the measurement framework for process capability for each of the processes within its scope.

- Note It would be permissible for a model, for example, to address solely level 1, or to address levels 1, 2 and 3, but it would not be permissible to address levels 2 and 3 without level 1.
- Level 0, Incomplete process—The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.

- Level 1, Performed process (one attribute)—The implemented process achieves its process purpose.

- Level 2, Managed process (two attributes)—The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

- Level 3, Established process (two attributes)—The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.

- Level 4, Predictable process (two attributes)—The previously described established process now operates within defined limits to achieve its process outcomes.

- Level 5, Optimizing process (two attributes)—The previously described predictable process is continuously improved to meet relevant current and projected business goals.
Each capability level can be achieved only when the level below has been fully achieved. For example, a process capability level 3 (established process) requires the process definition and process deployment attributes to be largely achieved, on top of full achievement of the attributes for a process capability level 2 (managed process).

There is a significant distinction between process capability level 1 and the higher capability levels. Process capability level 1 achievement requires the process performance attribute to be largely achieved, which actually means that the process is being successfully performed and the required outcomes obtained by the enterprise. The higher capability levels then add different attributes to it.
Mapping to PRM’s

- A Process Assessment Model shall provide an explicit mapping from the relevant elements of the model to the relevant process attributes of the measurement framework.

- The mapping shall be complete, clear and unambiguous. The mapping of the indicators within the Process Assessment Model shall be:
  - The purpose and outcomes of the processes in the specified Process Reference Model
  - The process attributes (including all of the results of achievements listed for each process attribute) in the measurement framework.
  - This enables Process Assessment Models that are structurally different to be related to the same Process Reference Model.
Measurement Framework

✓ COBIT Assessment Process measures the extent to which a given process achieves specific attributes relative to that process –

✓ COBIT Assessment Process defines 9 Process Attributes (based on ISO/IEC 15504-2)

- PA1.1- process performance
- PA2.1- work product management
- PA2.2- performance management
- PA 3.1- process definition
- PA 4.1- process deployment
- PA 4.2- process control
- PA 5.1- process innovation
- PA 5.2- continuous optimization
Process Attributes (example)

- PA 1.1 Process performance
  - The process performance attribute is a measure of the extent to which the process purpose is achieved.
  - As a result of full achievement of this attribute the process achieves its defined outcomes.
PA 2.1 Performance Management

- A measure of the extent to which the performance of the process is managed. As a result of full achievement of this attribute:
  a. objectives for the performance of the process are identified
  b. performance of the process is planned and monitored
  c. performance of the process is adjusted to meet plans
  d. Responsibilities and authorities for performing the process are defined, assigned and communicated
  e. resources and information necessary for performing the process are identified, made available, allocated and used
  f. interfaces between the involved parties are managed to ensure effective communication and clear assignment of responsibility

PA 2.2 Work Product Management

- A measure of the extent to which the work products produced by process are appropriately managed. As a result of full achievement of this attribute:
  a. Requirements for the work products of the process are defined.
  b. Requirements for documentation and control of the work products are defined.
  c. work products are appropriately identified, documented and controlled
  d. work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet Requirements
COBIT Assessment Process measures the extent to which a given process achieves the “Process Attributes”

N, Not achieved - 0 to 15% achievement
There is little or no evidence of achievement of the defined attributes in the assessed process.

P, Partially achieved - >15 to 50% achievement
There is some evidence of an approach to and some achievement of the defined attributes in the assessed process. Some aspects of achievement of the attribute may be unpredictable.

L, Largely achieved - >50 to 85% achievement
There is evidence of a systematic approach to and significant achievement of the defined attributes in the assessed process. Some weakness related to this attribute may be exist in the process.

F, Fully achieved - >85 to 100% achievement
There is evidence of a complete & systematic approach to and full achievement of the defined attributes in the assessed process. No significant weakness related to this attribute exist in the assessed process.
Chapter 5

Assessor Assessment Steps
Assessment Process Activities

- Initiation
- Planning the Assessment
- Briefing
- Data Collection
- Data Validation
- Process Attribute Rating
- Reporting the Results
1: Initiation

- Identify the sponsor and define the purpose of the assessment - why it is being carried out.
- Define the scope of the assessment - which processes are being assessed - what constraints, if any, apply to the assessment
- Identify any additional information that needs to be gathered
- Select the assessment participants, the assessment team and define the roles of team members
- Define assessment inputs and outputs - Have them approved by the sponsor
2: Planning the Assessment

- An assessment plan describing all activities performed in conducting the assessment is developed and documented together with an assessment schedule.
- Identify the project scope.
- Secure the necessary resources to perform the assessment.
- Determine the method of collecting, reviewing, validating and documenting the information required for the assessment.
- Co-ordinate assessment activities with the organizational unit being assessed.
3: Briefing

- The assessment Team Leader ensures that the assessment team understands the assessment
  - input
  - process and
  - output
- Brief the Organizational Unit on the performance of the assessment
  - PAM, assessment scope, scheduling, constraints, roles and responsibilities,
    resource requirements, etc
4: Data Collection

- The assessor obtains (and documents) an understanding of the process(es) including process purpose, inputs, outputs, and work products, sufficient to enable and support the assessment.
- Data required for evaluating the processes within the scope of the assessment is collected in a systematic manner.
- The strategy and techniques for the selection, collection, analysis of data and justification of the ratings are explicitly identified and demonstrable.
- Each process identified in the assessment scope is assessed on the basis of objective evidence.
  - The objective evidence gathered for each attribute of each process assessed must be sufficient to meet the assessment purpose and scope.
  - Objective evidence that supports the assessor's judgment of process attribute rating is recorded and maintained in the assessment record.
    - This record provides evidence to substantiate the ratings and to verify compliance with the requirements.
5: Data Validation

- Actions are taken to ensure that the data is accurate and sufficiently covers the assessment scope, including:
  - Seeking information from first hand, independent sources
  - Using past assessment results; and
  - Holding feedback sessions to validate the information collected.

- Some data validation may occur as the data being collected.
Process Attribute Rating

- For each process assessed, a rating is assigned for each process attribute up to and including the highest capability level defined in the assessment scope.
- The rating is based on data validated in the previous activity.
- Traceability shall be maintained between the objective evidence collected and the process attribute ratings assigned.
- For each process attribute rated, the relationship between the indicators and the objective evidence is recorded.
7: Reporting the Results

- The results of the assessment are analyzed and presented in a report.
- The report also covers any key issues raised during the assessment such as:
  - Observed areas of strength and weakness
  - Findings of high risk
    - i.e. magnitude of gap between assessed capability and desired/required capability
Assessor Certification

- **COBIT process Assessment roles:**
  - Lead Assessor-a “competent” assessor responsible for overseeing the assessment activities
  - Assessor- an individual, developing assessor competencies, that performs the assessment activities

- **Assessor Competencies:**
  - **Knowledge, skills and Experience**
    - With the process Reference Model; Process Assessment Model, methods and tools; and rating processes
    - With the processes/domains being assessed
    - Personal attributes which contribute to effective performance

- An assessor’s training and certificate course for assessors is being developed for COBIT 4.1 and COBIT 5.0 Availability Q1 2013
Questions?