IT Audit Process

Prof. Mike Romeu

September 9, 2015
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
COBIT® 5 – Principles: Meeting Stakeholder Needs

**Goals Cascade:**
Translates Stakeholder needs into specific, actionable and customized goals within the context of the enterprise, IT-related goals and enable goals.
IT Assurance and COBIT® 5 - Enablers

1. Principles, Policies and Frameworks

2. Processes

3. Organizational Structures

4. Culture, Ethics and Behaviour

5. Information

6. Services, Infrastructure and Applications

7. People, Skills and Competencies

Resources
IT Assurance and COBIT® 5

**Definition:** “Assurance Means that, pursuant to an accountability relationship between two or more parties, an IT audit and assurance professional may be engaged to issue a written communication expressing a conclusion about the subject matters to the accountable party” (ISACA Glossary).” (ISACA, COBIT® 5 for Assurance, USA, 2013)

1. Three-Party Relationship
   a. Accountable Party (Auditee)
   b. User of Assurance Report
   c. Assurance Professional
2. Subject Matter
3. Suitable Criteria
4. Assurance Process
5. Conclusions and Recommendations
IT Assurance and COBIT® 5 – Assurance Process

A. Determine Scope of the Assurance Initiative

B. Understand Enablers, Set Suitable Criteria and Perform the Assessment

C. Communicate the Results of the Assessment
A. Determine Scope of the Assurance Initiative

- **A-1** Determine the stakeholders of the assurance initiative and their stake.
- **A-2** Determine Assurance Objectives based on assessment of internal/external environment and of the relevant risk and opportunities
- **A-3** Determine the enablers in scope and the instance(s) of the enablers in scope:
  - Principles, Policies and Frameworks
  - Processes
  - Organisational Structures
  - Culture, Ethics and Behaviour
  - Information
  - Services, Infrastructure and Applications
  - People, Skills and Competencies
# IT Assurance and COBIT® 5 – Assurance Process

## B. Understand Enablers, Set Suitable Assessment Criteria and Perform Assessment

<table>
<thead>
<tr>
<th>B-1</th>
<th>Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-2</td>
<td>Obtain understanding of the Principles, policies and frameworks in scope. Assess principles, policies and frameworks in scope.</td>
</tr>
<tr>
<td>B-3</td>
<td>Obtain understanding of the processes in scope and set suitable assessment criteria. Assess the processes.</td>
</tr>
<tr>
<td>B-4</td>
<td>Obtain understanding of the organizational structures in scope. Assess the organizational structures.</td>
</tr>
<tr>
<td>B-5</td>
<td>Obtain understanding of culture, ethics and behavior in scope. Assess culture, ethics and behavior</td>
</tr>
<tr>
<td>B-6</td>
<td>Obtain understanding of the information items in scope. Assess information.</td>
</tr>
<tr>
<td>B-7</td>
<td>Obtain understanding of the services, infrastructure and applications in scope. Assess services, infrastructure and applications.</td>
</tr>
<tr>
<td>B-8</td>
<td>Obtain understanding of the people, skills and competencies in scope. Assess people, skills and competencies.</td>
</tr>
</tbody>
</table>
Process for Governance of Enterprise IT
Evaluate, Direct and Monitor

**Align, Plan and Organize**

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

**Build, Acquire and Implement**

- AP001 Manage the IT management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Innovation
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP009 Manage Suppliers
- AP010 Manage Innovation
- AP011 Manage Risk
- AP012 Manage Security

**Deliver, Service and Support**

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

**Monitor, Evaluate and Assess**

- AP008 Manage Budget and Costs
- AP009 Manage Human Resources
- AP010 Manage Innovation
- AP011 Manage Risk
- AP012 Manage Security
- AP013 Manage Innovation
- AP014 Manage Business Continuity
- AP015 Manage Risk Management
- AP016 Manage Compliance
- AP017 Manage Performance

**Processes for Management of Enterprise IT**

- BAI01 Monitor, Evaluate and Assess Performance and Conformance
- BAI02 Monitor, Evaluate and Assess the System of Internal Controls
- BAI03 Monitor, Evaluate and Assess Compliance With External Requirements