Using COBIT 5 for Assurance as Framework for your IT Audit

Hans Henrik Berthing, CPA, CGEIT, CRISC, CISA, CIA, Verifica & Aalborg University
Hans Henrik Berthing

Married with Louise and dad for Dagmar and Johannes

CPA, CRISC, CGEIT, CISA and CIA

Expert reviewer Cobit 5 for Sarbannes Oxley

Partner and owner for Verifica

Financial Audit, since 1994 and IT Assurance since 1996

Member of FSR IT Advisory Board & ISACA IT Assurance Task Force

CISA, CRISC & CISM review instructor (>80% passing)

Instructor, facilitator and speaker

Associated professor Aalborg University (Auditing, Risk & Compliance)
Learning Objective

After this presentation you will have learned how to use Cobit 5 for assurance as a framework for your planning and reporting of your IT Audit. You will learn how you will be able as an audit to use Cobit 5 for assurance as a framework and reference for your IT audit reporting for those who are accountable for IT Governance

Subhead

- Cobit 5 for Assurance
- IT Assurance Framework
- Cobit Assurance Workprogram
Cobit 5 for Assurance

An ISACA Framework
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
COBIT 5 for Assurance Overview

**Question**

- What is assurance?
- How do COBIT 5 enablers relate to providing assurance?
- How do I set up and maintain an efficient assurance function?
- How does COBIT 5 help me to provide assurance?

**Where to Find Guidance**

Section 1 defines *assurance*, and describes briefly how the COBIT 5 principles can be applied to assurance-specific needs.

In general, two perspectives on how to use COBIT 5 in an assurance context can be identified:

1. The *assurance function perspective*, describing what is needed in an enterprise to build and sustain an efficient and effective assurance function.
2. The *assessment perspective*, describing how different types of assurance engagements or assessments can be supported by the COBIT 5 enablers.

Section 2A provides guidance on what is needed to set up and maintain an effective and efficient assurance function. It lists and briefly describes the COBIT 5 enablers required, e.g., processes, organizational structures. Putting these enablers in place will result in an effective and efficient assurance function that adds value to the enterprise.

*Appendix B.1-7* includes detailed descriptions for each enabler listed in section 2A.

**COBIT 5 helps to provide assurance in several ways:**

1. COBIT 5 includes an enabler model, after which all seven COBIT 5 enablers are structured. Part of this enabler model is the performance assessment dimension, which is used to structure any assessment of any enabler. This is explained in *Section 2B*.
2. COBIT 5, and especially the COBIT 5 process reference model as described in the *COBIT 5: Enabling Processes* publication, provides a comprehensive reference model for all governance and management aspects of IT. As such, it constitutes the perfect set of suitable criteria on which to base any assessment.
COBIT 5 for Assurance Overview

- What does a COBIT 5-based audit/assurance programme look like?
  - Section 2B explains the audit/assurance process in detail, and it describes a generic, skeleton audit/assurance programme. This programme builds on the COBIT 5 enablers, which results in a comprehensive and holistic programme.

- Are there any examples of COBIT 5-based audit/assurance programmes?
  - Yes. Section 2B explains the generic structure of an audit/assurance programme. Appendix D contains a set of example audit/assurance programmes based on this template. More sample audit/assurance programmes will be published separately by ISACA.

- Does COBIT 5 align with assurance standards?
  - Yes. A detailed comparison, in the form of a mapping or qualitative description, is included in section 3. The following related standards are referred to in this section: ITAF, IPPF and ISAE 3402/SSAE 16.

- Does COBIT 5 for Assurance include detailed instructions on how to perform an assessment?
  - No. COBIT 5 for Assurance assumes that the reader is familiar with, and can apply, basic auditing and assessment techniques. A brief overview of auditing techniques is included in section 2B, chapter 4.1, but details are not provided.
Prerequisite Knowledge

COBIT 5 for Assurance builds on COBIT 5. Most key concepts of COBIT 5 are repeated and elaborated on in this publication, making it a fairly standalone book—in essence, not requiring any prerequisite knowledge. However, an understanding of COBIT 5 at the foundation level will accelerate comprehension of this publication.

Should readers wish to know more about COBIT 5 concepts beyond what is required for assurance purposes, they are referred to the COBIT 5 framework publication.

COBIT 5 process details described therein. If readers wish to know more about the process capability assessment approach, they are referred to the COBIT Assessment Programme guides.
Assurance proces

Three-party relationship involving an accountable party for the subject matter, an assurance professional and an intended user.

Assurance Professional

Accountable Party

User

Assurance Process that the assurance professional will undertake:

A. Determine Scope of the Assurance Initiative
   Subject Matter over which the assurance is to be provided

B. Understand the Subject Matter, Set Suitable Assessment Criteria and Assess
   Suitable Criteria against which the subject matter will be assessed

C. Communication
   Execute the assurance engagement
   Conclusion issued by the assurance professional

Provides Comfort to
Scope of COBIT 5 for Assurance

COBIT® 5 for Assurance

COBIT 5 Enablers for the Assurance Function
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Principles, Policies and Frameworks
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Assurance Function Perspective

Assurance

COBIT 5 framework and COBIT® 5: Enabling Processes

Audit/Assurance Programmes for Subject Matter

ISACA Audit/Assurance Programmes

ITAF
## Comparison of Assurance Engag. Types

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Self-assessment</th>
<th>Internal Audit/Compliance Review</th>
<th>External Audit</th>
</tr>
</thead>
</table>
| Independence requirements      | • Not required or guaranteed  
                                   • Objectivity of self-assessors should be encouraged by defining clear responsibilities and correct follow-up. | Should be optimised by the correct composition of the internal audit/compliance department members | Independence of the external auditors should be established, verified and maintained. |
| Interested party (user)        | Enabler owners                                                                | Executive management, audit committee, operational management and enabler owners involved         | Primarily directed toward the board/shareholders, but of importance to the enterprise in general |
| Responsible party (accountable party) | Enabler owners                                                              | Management and business enabler owners involved                                                  | The board and executive management involved                                          |
| Assurance provider (assurance professional) | Enabler owners                                                              | Internal audit/compliance department                                                              | External auditor                                                                    |
| Reporting format and requirements | • Free format  
                                   • Internal consistency required                                                              | Internal consistency required, in line with professional standards                              | Highly regulated/standardised                                                          |
| Governing rules/standards      | Standardised approaches based on good practices required                    | • Standardised approaches based on good practices required  
                                   • Professional standards and code of ethics to be respected                                      | Adherence to applicable codes of ethics and standards should be established, verified and maintained. |
| Level of trust (reliability)   | • Lowest  
                                   • Depends on the skill and objectivity of the assessor                                       | • Medium  
                                   • Depends on the skill and expertise of the internal audit/compliance department and on co-operation of the accountable party | Maximal                                                                          |

**Regulated and Standardised**
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

Resources
## Principles, Policies and Frameworks in ITAE

<table>
<thead>
<tr>
<th>Principles, Policies and Frameworks Area</th>
<th>Covered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code of professional ethics</td>
<td>ITAF, 2nd Edition, Section 1</td>
</tr>
<tr>
<td>General standards</td>
<td>1001 Audit Charter 1002 Organisational Independence 1003 Professional Independence 1004 Reasonable Expectation 1005 Due Professional Care 1006 Proficiency 1007 Assertions 1008 Criteria</td>
</tr>
<tr>
<td>Performance standards</td>
<td>1201 Engagement Planning 1202 Risk Assessment in Audit Planning 1203 Performance and Supervision 1204 Audit Materiality 1205 Audit Evidence 1206 Using the Work of Other Experts 1207 Irregularities and Illegal Acts</td>
</tr>
<tr>
<td>Reporting standards</td>
<td>1401 Reporting 1402 Follow-up Activities</td>
</tr>
</tbody>
</table>
ISACA Code of Professional Ethics

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.

3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the association.

4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.

7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
# Processes for Gov. of Enterprise IT

<table>
<thead>
<tr>
<th>Process Identification</th>
<th>Reasoning</th>
<th>Assurance-specific Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM01 Ensure governance framework setting and maintenance.</td>
<td>The assurance function requires the establishment of a governance structure.</td>
<td>• Stakeholder requirements with regards to governance of assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assurance guiding principles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assurance function and audit committee mandate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Formal documentation on assurance decisions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Formal meeting minutes of assurance management meetings</td>
</tr>
<tr>
<td>EDM02 Ensure benefits delivery.</td>
<td>The enterprise must ensure that the assurance function generates value.</td>
<td>• Formal documentation of stakeholder requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Formal documentation of assurance function’s contribution to business objectives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Feedback on delivery of assurance initiatives</td>
</tr>
<tr>
<td>EDM03 Ensure risk optimisation.</td>
<td>The enterprise must ensure that assurance-related risk is managed.</td>
<td>Remedial actions to address assurance deviations noted</td>
</tr>
<tr>
<td>EDM05 Ensure stakeholder transparency.</td>
<td>The assurance function is an important provider of overall stakeholder transparency.</td>
<td>• Evaluation of assurance reporting requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assurance summary of activities to audit committee</td>
</tr>
</tbody>
</table>
## Align, Plan and Organise

<table>
<thead>
<tr>
<th>Process Identification</th>
<th>Reasoning</th>
<th>Assurance-specific Outputs</th>
</tr>
</thead>
</table>
| AP002 Manage strategy.         | The assurance function must develop a strategy for providing assurance. The strategy should be aligned with the business strategy. | • List of potential assurance function coverage gaps  
• Assurance function capabilities  
• Criteria for prioritizing gaps in assurance coverage  
• Assurance function requirements in target IT capabilities  
• Assurance function gaps to be closed  
• Assurance function capability benchmark  
• Assurance strategic plan  
• Updated IT strategic plan and road map taking into account the assurance function requirements  
• Annual assurance function plan |
| AP006 Manage budget and costs. | The assurance function must budget for its activities and supporting systems.                                      | • Assurance activity prioritization  
• Assurance function budget |
| AP007 Manage human resources.  | The assurance function requires the right number of people and skills.                                                  | • Assurance function requirements for the staffing process  
• Assurance function training plan  
• Assurance function personnel evaluations  
• Resource performance tracking plan and indicators, resource allocation plan |
| AP008 Manage relationships.    | Relationships between the assurance function and business are critical.                                                   | • Understanding of business processes of the enterprise  
• Strategy to obtain stakeholder commitment  
• Assurance communication strategy  
• Assurance action plans for the business |
# APO and Build, Acquire and Implement

<table>
<thead>
<tr>
<th>Process Identification</th>
<th>Reasoning</th>
<th>Assurance-specific Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP011 Manage quality.</td>
<td>Quality improvement is an essential component of effective assurance provisioning.</td>
<td>• Relevant assurance good practices and standards&lt;br&gt;• Assurance function quality standards&lt;br&gt;• Assurance function quality metrics agreed upon&lt;br&gt;• Results of external quality peer reviews of the assurance functions&lt;br&gt;• Assurance function quality metrics implemented in line with industry good practices&lt;br&gt;• Documented root causes for assurance issues with quality metrics</td>
</tr>
<tr>
<td>AP012 Manage risk.</td>
<td>Assurance risk (audit risk) must be managed.</td>
<td>• Data for assurance risk analysis&lt;br&gt;• Assurance function risk analysis results&lt;br&gt;• Enterprise risk profile that includes assurance-related aspects&lt;br&gt;• Risk evaluation and assessment strategies&lt;br&gt;• Updated enterprise risk profile</td>
</tr>
<tr>
<td>BAI08 Manage knowledge.</td>
<td>Assurance function must be provided with the knowledge required to support assurance staff in their work activities.</td>
<td>• Updated classification of assurance function information&lt;br&gt;• Published knowledge repositories&lt;br&gt;• Updated access control over assurance information&lt;br&gt;• Updated rules for assurance information disposal</td>
</tr>
</tbody>
</table>
## Core Organisational Structures

<table>
<thead>
<tr>
<th>Structure</th>
<th>Definition/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board/audit committee</td>
<td>The governance body that is charged with evaluating, directing and monitoring the organisation's audit, risk management and control functions. The board (or the equivalent function that is charged with the governance of the enterprise) often delegates responsibility for providing assurance to the audit committee, whose members are usually drawn from the board (non-executives). Final accountability, however, stays with the board.</td>
</tr>
<tr>
<td>Audit department</td>
<td>The function in the enterprise responsible for provision of internal audits³</td>
</tr>
</tbody>
</table>
| Compliance department: | • Regulatory — The function in the enterprise responsible for guidance on legal, regulation and statutory requirements, and contractual compliance  
                     • Internal — The group responsible for verifying compliance with organisational policies and standards |
| External audit       | The function responsible for provision of external audit and associated services       |
Generic COBIT 5-based Assurance Engagement Approach

A. Determine Scope of the Assurance Initiative
   
   A-1 Determine the **stakeholders** of the assurance initiative and their **stake**.
   
   A-2 Determine the **objectives** based on assessment of the internal and external environment/context and of the relevant **risk** and related **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

B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment
   
   B-1 Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.
   
   B-2 Obtain understanding of the **principles, policies and frameworks** in scope. Assess principles, policies and frameworks.
   
   B-3 Obtain understanding of the **processes** in scope and set suitable assessment criteria. Assess the processes.
   
   B-4 Obtain understanding of the **organisational structures** in scope. Assess the organisational structures.
   
   B-5 Obtain understanding of the culture, ethics and behaviour in scope. Assess culture, ethics and behaviour.
   
   B-6 Obtain understanding of the **information items** in scope. Assess information.
   
   B-7 Obtain understanding of the services, infrastructure and applications in scope. Assess services, infrastructure and applications.
   
   B-8 Obtain understanding of the **people, skills and competencies** in scope. Assess people, skills and competencies.

C. Communicate the Results of the Assessment
   
   C-1 Document exceptions and gaps.
   
   C-2 Communicate the work performed and findings.
Determine scope of the assurance initiative (phase A)

- Stakeholders? And their stakes?
- "Overall enterprise objectives?"
- Business requirements and associated risk and opportunities?
- Organisational structure? - Roles and responsibilities?
- Governing policies and procedures?
- Applicable laws, regulations and contractual agreements?
- Management practices and associated activities are in place?
- Mgmt reporting (status, performance, actions) is in place?
- Past issues have arisen and corrective actions have been taken?
- Management hope to obtain as a result of the assurance initiative?
- Current issues and concerns?
## Phase A-1 to A-3

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Determine scope of the assurance initiative.</strong></td>
<td></td>
</tr>
<tr>
<td>A-1</td>
<td>Determine the <em>stakeholders</em> of the assurance initiative and their <em>stake</em>, i.e., the drivers for the assurance engagement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Identify the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Identify the interested parties accountable and responsible for the subject matter over which assurance needs to be provided.</strong></td>
<td></td>
</tr>
<tr>
<td>A-2</td>
<td><strong>Determine the assurance <em>objectives</em> based on assessment of the internal and external environment/context and of the relevant <em>risk</em> and related <em>opportunities</em> (i.e., not achieving the enterprise goals).</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimising the risk that strategic objectives are not achieved and optimising resource levels required to achieve the strategic objectives.</strong></td>
<td></td>
</tr>
</tbody>
</table>
Example: Audit of an Internet banking system

3.2.1 Assurance Topic: The topic covered by this document is: Internet banking.

3.2.2 Goals of the Assurance Engagement: The goal of the review is to provide assurance over whether Internet banking is secure, i.e., are the bank and its clients protected against fraudulent transactions and is client confidentiality maintained?

3.2.3 Scoping: The scope of the assurance engagement is expressed in function of the seven COBIT 5 enablers, as per the following table.

Some enabler instances are standard COBIT 5, i.e., they are described in varying degrees of detail in the COBIT 5 framework or COBIT 5: Enabling Process. This would include COBIT 5 processes mainly, but also the enabler examples included in this or similar publications.
## Example: Scope

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><strong>Determine scope of the assurance initiative.</strong></td>
<td>Board/audit committee: Provide the board/audit committee with assurance that the Internet banking process is secure in all aspects.</td>
</tr>
<tr>
<td>A-1</td>
<td><strong>Determine the stakeholders</strong> of the assurance initiative and their stake, i.e., the drivers for the assurance engagement.**</td>
<td></td>
</tr>
<tr>
<td>A-1.1</td>
<td><strong>Identify</strong> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.</td>
<td><strong>Intended user(s) of the assurance report</strong></td>
</tr>
<tr>
<td>A-1.2</td>
<td><strong>Identify</strong> the interested parties accountable and responsible for the subject matter over which assurance needs to be provided.</td>
<td><strong>Accountable and responsible parties for the subject matter</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Executive management</strong> (includes business executives and CIO): The individuals accountable for the establishment of a secure Internet banking process that is controlled, monitored and compliant with good practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Business process owners</strong>: The individuals responsible for identifying Internet banking process requirements, approving the process design and managing process performance. These people are, together with IT management, responsible for the complete security of the Internet banking process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IT management</strong> (includes head of development, head of IT operations, and service managers): The individuals responsible for managing the Internet banking applications (together with the business process owners) and ensuring the security, privacy and confidentiality aspects of the process</td>
</tr>
</tbody>
</table>
## Example: Scope

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Determine scope of the assurance initiative. <em>(cont.)</em></td>
<td>Guiding principles and policies include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internet banking policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Risk policies</td>
</tr>
<tr>
<td>A-3</td>
<td>Determine the enablers in scope and the instance(s) of the enablers in scope <em>(cont.)</em></td>
<td><strong>COBIT 5: Enabling Processes</strong> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customisation. The resulting list contains key processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</td>
</tr>
<tr>
<td>A-3.1</td>
<td>Define the <strong>principles, policies and frameworks</strong> in scope.</td>
<td><strong>Key Processes</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EDM03 Ensure risk optimisation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• APO10 Manage suppliers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• APO12 Manage risk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• APO13 Manage security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BAI01 Manage programmes and projects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BAI06 Manage changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All DSS processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All MEA processes</td>
</tr>
<tr>
<td>A-3.2</td>
<td>Define which <strong>processes</strong> are in scope of the review.</td>
<td><strong>Key Organisational Structures</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Risk management department</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT security department</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Architecture board</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT development department</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT operations department</td>
</tr>
</tbody>
</table>
Assurance Engagement Scoping Summary

A. Determine Scope of the Assurance Initiative

A-1. Determine the **stakeholders** of the assurance initiative and their **stake**.

A-2. Determine the assurance **objectives** based on assessment of the internal and external environment/context and of the relevant **risk** and related **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

1. Define the assurance objective in simple language.

2. Identify the **enterprise goals** that are most related to the high-level assurance objective.

3. Refine the list of potential enterprise goals to a manageable set of key goals and additional goals.

4. Use the **mapping table** between enterprise goals and IT goals to identify potential **IT goals** that need to be achieved.

5. Refine—taking into account the specific environment—the set of potential IT goals to a manageable set of key IT goals and additional IT goals.

6. Use the **mapping table** between IT goals and COBIT 5 processes to identify potential **processes** that support the IT goals.

7. Refine the list of selected processes to a manageable list.

8. Use the **RACI charts** of the selected processes to identify potential **organisational structures** in scope, and refine the list.

9. Use the **RACI charts** of the selected processes to identify potential **people, skills and competencies** in scope, and refine the list.

10. Use the **input/output tables** of the selected processes to identify potential **information items** in scope, and refine the list.

11. Identify which other **enablers** support the achievement of the selected IT goals.

12. Consolidate the list of enablers in scope and remove redundancies.
Understand enablers, set suitable Assessment criteria and perform the Assessment (phase b)

- Reference all seven enablers. Building an understanding of the subject matter over which assurance needs to be provided. The subject matter is expressed in terms of the COBIT 5 enablers.
- Obtaining agreement over the assessment criteria that will be used during the assurance engagement
- Assessing the design and outcomes of the enablers
Appropriate auditing techniques

- **Enquire and confirm:**
  - eg: Search for exceptions/deviations and examine them.

- **Observe:**
  - eg: Observe and describe the processes.

- **Reperform and/or recalculate:**
  - eg: Reperform transactions, control procedures, etc.

- **Review automated evidence collection:**
  - eg: Collect sample data.
Understand enablers, set suitable Assessment criteria and perform the Assessment (phase b)

- Reference all seven enablers. Building an understanding of the subject matter over which assurance needs to be provided. The subject matter is expressed in terms of the COBIT 5 enablers.

- Obtaining agreement over the assessment criteria that will be used during the assurance engagement

- Assessing the design and outcomes of the enablers
Understand enablers, set suitable Assessment criteria and perform the Assessment (phase b)

4.1 Introduction
4.2 Achievement of Goals
4.3 Enabler: Principles, Policies and Frameworks
4.4 Enabler: Processes
4.5 Enabler: Organisational Structures
4.6 Enabler: Culture, Ethics and Behaviour
4.7 Enabler: Information
4.8 Enabler: Services, Infrastructure and Applications
4.9 Enabler: People, Skills and Competencies
4.2 Achievement of Goals

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Understand the enablers, set suitable assessment criteria and perform the assessment.</td>
<td></td>
</tr>
<tr>
<td>B-1</td>
<td>Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.</td>
<td></td>
</tr>
<tr>
<td>B-1.1</td>
<td>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics.</td>
<td>Leverage the list of suggested metrics for the enterprise goals(^6) to define, discuss and agree on a set of relevant, customised metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative. Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</td>
</tr>
<tr>
<td></td>
<td>Assess whether enterprise goals in scope are achieved.</td>
<td>Enterprise goals were defined in the first part of step B-1.1, and for each goal the related metrics and assessment criteria were defined. In this part of the step, the related metrics for each goal are reviewed and an assessment is made whether the defined criteria are achieved or not.</td>
</tr>
</tbody>
</table>
4.3 Enabler: Principles, Policies and Frameworks

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Understand the enablers, set suitable assessment criteria and perform the assessment.</td>
<td></td>
</tr>
<tr>
<td>B-2</td>
<td>Obtain understanding of the <strong>principles, policies and frameworks</strong> in scope. Assess principles, policies and frameworks.</td>
<td></td>
</tr>
<tr>
<td>B-2.1</td>
<td>Understand the principles, policies and frameworks context.</td>
<td>Obtain understanding of the overall system of internal control and the associated principles, policies and frameworks.</td>
</tr>
<tr>
<td>B-2.2</td>
<td>Understand the stakeholders of the principles, policies and frameworks.</td>
<td>Understand the stakeholders in the policies. These include those setting the policies and those who need to be in compliance with the policies.</td>
</tr>
</tbody>
</table>
Generic approach for communicating on an Assurance initiative (phase c)

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Communicate the results of the assessment.</td>
<td></td>
</tr>
<tr>
<td>C-1</td>
<td>Document exceptions and gaps.</td>
<td></td>
</tr>
</tbody>
</table>
| C-1.1| Understand and document weaknesses and their impact on the achievement of enabler goals. | • Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse.  
  • Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.                                                                                                                                             |
| C-1.2| Understand and document weaknesses and their impact on enterprise goals.      | • Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry, and leverage industry benchmarks.  
  • Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc.  
  • Point out the consequence of non-compliance with regulatory requirements and contractual agreements.  
  • Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost). |
COBIT 5 Process Assurance Programs

Example
COBIT 5 Process Assurance Programs

Conducting assurance over a process.

Aligned with generally accepted auditing standards and practices and are based upon the overall assurance engagement approach.

Divided into three phases:

- Determining the scope of the assurance initiative
- Understanding enablers, setting suitable assessment criteria and performing the assessment
- Communicating and reporting the results of the assessment
COBIT 5 Process Assurance Programs

Fully aligned with COBIT 5:

- Reference all seven enablers.
- COBIT 5 goals are cascaded to ensure that detailed objectives of the assurance engagement can be put into the enterprise and IT context
- Enable linkage of the assurance objectives to enterprise and IT risk and benefits.
- Comprehensive yet flexible.
- The assurance professional can decide to not cover a set of enablers or some enabler instances
- Issue of what is or is not covered will be quite transparent to the assurance engagement user.
- For each step, a short description is included
- Assurance professionals will have to use their own professional judgment
Evaluate, Direct and Monitor

Provide assurance over the EDM01 process:

**Ensures:**

- A consistent and integrated approach aligned with the enterprise governance approach is provided.
- IT-related decisions are made in line with the enterprise’s strategies and objectives.
- IT-related processes are overseen effectively and transparently.
- Compliance with legal and regulatory requirements is confirmed.
- The governance requirements for board members are met.
## Phase A—Determine Scope of the Assurance Initiative

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Step</th>
<th>Guidance</th>
<th>Issue Cross-reference</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>Determine the <strong>stakeholders</strong> of the assurance initiative and their <strong>stake</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-1.1</td>
<td>Identify the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.</td>
<td>Intended user(s) of the assurance report. <strong>Describe the users of the assurance report and their stakes.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-1.2</td>
<td>Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.</td>
<td>Accountable and responsible parties for the subject matter. <strong>Describe the accountable and responsible parties for the subject matter over which assurance is to be provided; COBIT 5 includes a summary description of a comprehensive set of roles that can be used as starting point for this audit step (COBIT 5 framework, appendix 6, p. 76); COBIT 5 for Assurance also provides a summary description of a comprehensive set of assurance roles; see section 2A, chapter 4, p. 37.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-2</td>
<td><strong>Determine the assurance objectives</strong> based on assessment of the internal and external environment/context and of the relevant <strong>risk</strong> and related <strong>opportunities</strong> (i.e., not achieving the enterprise goals).</td>
<td>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement. Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically. Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-2.1</td>
<td>Understand the enterprise strategy and priorities.</td>
<td>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them to the extent the process under review is relevant.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-2.2</td>
<td>Understand the internal context of the enterprise.</td>
<td>Identify all internal environmental factors that could influence the performance of the process under review.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A-2.3</td>
<td>Understand the external context of the enterprise.</td>
<td>Identify all external environmental factors that could influence the performance of the process under review.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Assurance Steps and Guidance</th>
<th>Issue Cross-reference</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-1</td>
<td>Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B-1.1</td>
<td>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics and assess whether enterprise goals in scope are achieved. Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative. Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4:

<table>
<thead>
<tr>
<th>Enterprise Goal</th>
<th>Metric</th>
<th>Expected Outcome (Ex)</th>
<th>Assessment Step</th>
</tr>
</thead>
</table>
| EG01 Stakeholder value of business investments | • Percent of investments where value delivered meets stakeholder expectations  
• Percent of products and services where expected benefits are realised  
• Percent of investments where claimed benefits are met or exceeded | Agree on the expected values for these metrics, i.e., the values against which the assessment will take place. | In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved. |
| EG02 Portfolio of competitive products and services | • Percent of products and services that meet or exceed targets in revenues and/or market share  
• Ratio of products and services per life-cycle phase  
• Percent of products and services that meet or exceed customer satisfaction targets  
• Percent of products and services that provide competitive advantage | Agree on the expected values for these metrics, i.e., the values against which the assessment will take place. | In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved. |
Question