Self-assessment Guide: Using COBIT® 5

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®
With more than 100,000 constituents in 180 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT® framework. COBIT helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created *COBIT® Self-assessment Guide: Using COBIT® 5* (the 'Work') primarily as an assessor guide. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assessors should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Copyright

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Feedback: *www.isaca.org/cobit*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join the COBIT conversation on Twitter: #COBIT
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

COBIT® Self-assessment Guide: Using COBIT® 5
ISBN 978-1-60420-266-3
1

Acknowledgements

ISACA wishes to recognise:

Development Team
Gary Allan Bannister, CGEIT, CGMA, FCMA, Austria
Barry Lewis, CISM, CGEIT, CRISC, CISSP, Cerberus ISC Inc., Canada

ISACA Board of Directors
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., (retired), USA, Past International President
John Ho Chi, CISA, CISM, CRISC,CBCP, CFE, Ernst & Young LLP, Singapore, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Salomon Rico, CISA, CISM, CGEIT, Deloitte LLP, Mexico

Framework Committee
Steven A. Babb, CGEIT, CRISC, Betfair, UK, Chairman
Charles Betz, Enterprise Management Associates, USA
David Cau, ISO, ITIL, MSP, Prince2, France
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Frank J. Cindrich, CGEIT, CIPP, CIPP/G, Deloitte & Touche LLP, USA
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Anthony P. Noble, CISA, Viacom, USA
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brazil
Paras Kesharichand Shah, CISA, CGEIT, CRISC, CA, Australia

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASI System Integration
Hewlett-Packard
IBM
Symantec Corp.

Page intentionally left blank

Table of Contents

Page intentionally left blank

1.0 Introduction

How capable are your IT processes? Do they meet the needs of the business?

1.1 The COBIT Assessment Programme

The COBIT assessment programme is designed to provide enterprises with a repeatable, reliable and robust methodology for assessing the capability of their IT processes. Such assessments will normally be used as part of an enterprise's process improvement programme and can then be used to report internally to an enterprise's executive management or board of directors on the current capability of its IT processes against a target for improvement based on business requirements. Such assessments can be used as part of the initiation of a programme of process improvement or to assess progress after a period of process improvement.

The COBIT assessment programme includes the:

- *COBIT® Process Assessment Model (PAM): Using COBIT® 5*:
  - Based on COBIT 5 and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15504, this model is the basis for the assessment of an enterprise's IT processes against COBIT 5. The assessment process is evidence-based to enable a reliable, consistent and repeatable assessment process in the area of governance and management of enterprise IT.
  - The assessment model enables internal assessments by enterprises to support process improvement.
- *COBIT® Assessor Guide: Using COBIT® 5*—This product supports those who want to undertake an assessment of a formal, evidence-based nature.
- *COBIT® Self-assessment Guide: Using COBIT® 5*—This product has been developed to support the performance of simpler, less rigorous self-assessments.
- *COBIT® Assessment Programme Tool Kit: Using COBIT® 5*—The tools support process assessment activities and include scoping templates. The tools support *COBIT® Assessor Guide: Using COBIT® 5* and *COBIT® Self-assessment Guide: Using COBIT® 5* and include mappings to:
  - Business goals
  - IT goals

  An assessment training and certification programme scheme is currently being explored for COBIT 5 to be established in the future.

The full details of the COBIT assessment programme are outlined in the *COBIT Process Assessment Model (PAM): Using COBIT 5* and the *COBIT Assessor Guide: Using COBIT 5*. A full and detailed assessment requires an evidenced-based assessment of selected IT processes led by competent assessors to provide a reliable, repeatable assessment. An overview of the model is outlined in chapter 2.

1.2 Purpose of the COBIT Self-assessment

The self-assessment guide is provided as a 'stand-alone' publication, which can be used by enterprises to perform a less rigorous assessment of the capability of their IT processes. This may be a precursor to undertaking a more rigorous, evidenced-based assessment. The approach is based on the COBIT PAM used in the COBIT assessment programme, but does not require evidentiary requirements in support of the self-assessment, nor does it require use of the COBIT PAM. Sufficient information from the COBIT PAM and a full self-assessment template have been provided to simplify the process, eliminating the need to reference the other two publications in the COBIT assessment programme. However, users are encouraged to refer to the COBIT PAM, the assessor guide and the tool kit.

Chapter 3 of this guide outlines how self-assessments of the IT processes can be performed, and a complimentary tool kit has been provided with a specific self-assessment template, together with a copy of the scoping template outlined in the tool kit.

A detailed template with all of the process attributes and content required to perform a self-assessment has also been provided in the tool kit accompanying this guide, and an example has been provided in appendix B.

1.3 Frequently Asked Questions

We know where our strengths and weaknesses lie. Why undertake a COBIT process assessment?
Many enterprises believe they have some idea of their strengths and weaknesses. However, they can often be surprised to find that a particular process fails to perform as expected because it is not robust enough to deal with either enterprise change or different circumstances.

A structured assessment provides a clear and objective understanding of the strengths and weakness of an enterprise's IT processes against its business needs. This can be used to determine where and how resources should be used for process improvement and defines a baseline to measure whether process improvements have been successful.

My enterprise has not adopted COBIT, so how can I use COBIT for an assessment?
It is not expected that an enterprise's processes will align exactly with the COBIT processes or that the same terminology will be used. COBIT terminology will not always be in general use within enterprises. An early phase in any assessment may involve mapping in-house processes and terminology to the COBIT processes to be assessed. In respect to a self-assessment, this would be a relatively informal process.

Why do I need a more rigorous assessment? Is the self-assessment process not sufficient?
A self-assessment is based more on the judgement of the individual or individuals making the assessment. It will be subjective without a requirement for evidence. As a result, the assessment will be indicative of the process capability. Experience has shown that such assessments are often optimistic, showing a better result than would be shown in a more formal, evidence-based assessment. They are generally not repeatable or objective. For a repeatable, objective assessment, a full assessment using the COBIT PAM and assessor guide (with training) is required.

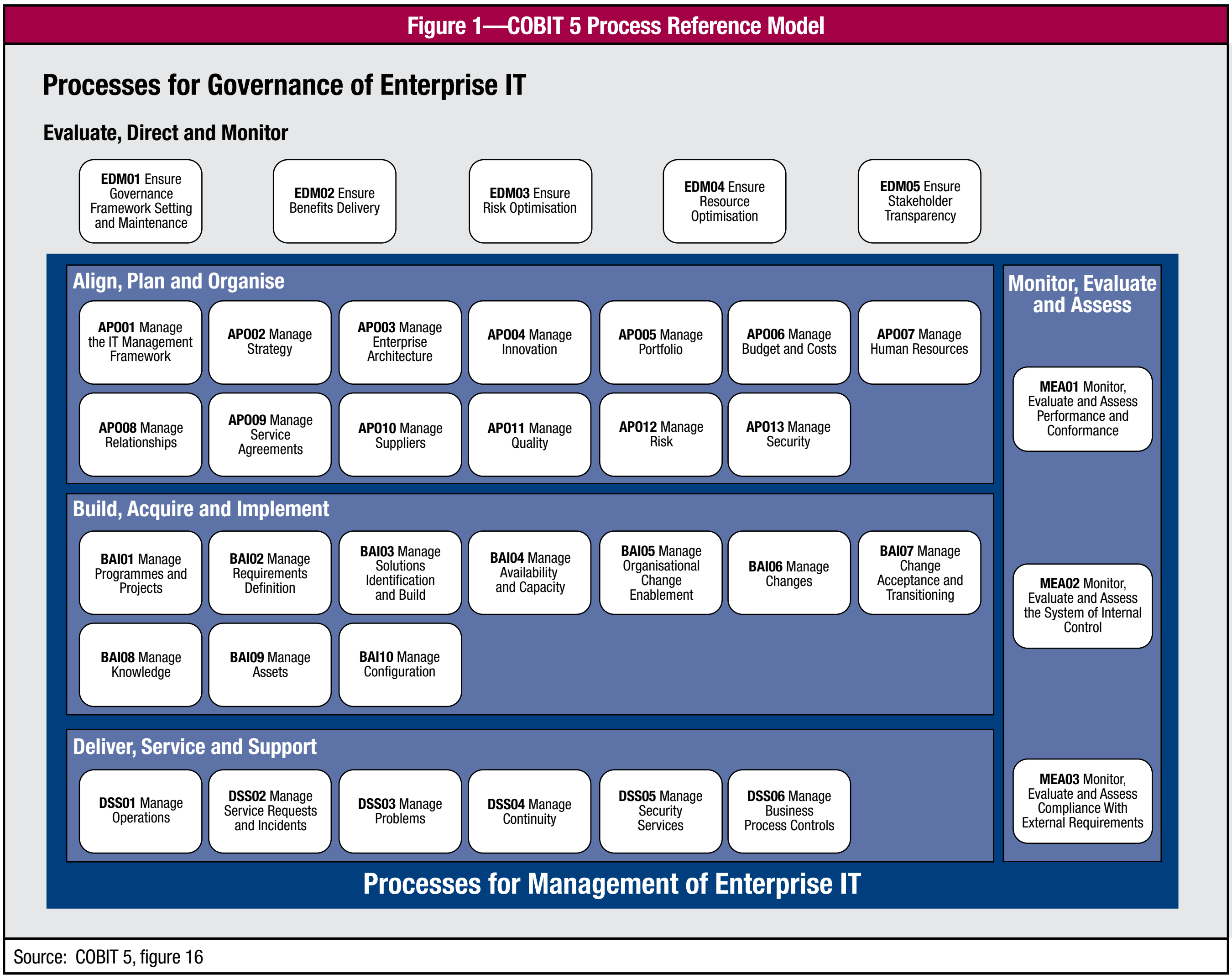
2.0 The COBIT Assessment Programme—Overview

The process reference model (PRM) for the COBIT assessment programme is COBIT 5. This means that COBIT 5 provides definitions of processes in a life cycle together with an architecture describing the relationships amongst the processes. The process purpose and outcomes are derived from COBIT 5 process enabler guidance.

2.1 COBIT 5 Architecture

The COBIT 5 PRM is a life cycle for governance and management of enterprise IT, comprised of 37 processes, as shown in **figure 1**.

Figure 1—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 Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
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 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
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
Processes for Management of Enterprise IT

Source: COBIT 5, figure 16

COBIT 5 can be obtained as a complimentary PDF at *www.isaca.org/cobit*. The COBIT 5 process details can be found in *COBIT® 5: Enabling Processes*, which is available from the ISACA Bookstore (and as a complimentary PDF for ISACA members at *www.isaca.org/cobit*).

Note that all aspects of COBIT (goals cascade, principles, the other six enablers) affect COBIT processes to some degree, depending on context. As such, COBIT guidance overall should be kept in mind when performing COBIT process assessments.

Note that it is not expected that an enterprise's processes will align exactly with the COBIT processes. Also, COBIT encourages enterprises to modify their terminology to fit with what the enterprise uses. The framework must work successfully with the enterprise culture. An early phase in the assessment may involve mapping enterprise processes and terminology to the COBIT processes to be used as the basis for the assessment.

2.2 The Measurement Framework

The assessment process involves establishing a capability rating for each process. It involves:

- Defined capability levels (from ISO/IEC 15504)
- Process attributes used to rate each process (from ISO/IEC 15504)
- Indicators on which to base the assessment achievement of each process attribute (based on and aligned with ISO/IEC 15504)
- A standard rating scale (from ISO/IEC 15504)

2.2.1 Process Capability Levels

The capability of each assessed process is expressed as a capability level from 0 to 5, as shown in **figure 2**. Each process capability level is aligned with a process situation.

Figure 2—Process Capability Levels

Process Level	Capability
0 (Incomplete)	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.
1 (Performed)	The implemented process achieves its process purpose.
2 (Managed)	The performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3 (Established)	The managed process is now implemented using a defined process that is capable of achieving its process outcomes.
4 (Predictable)	The established process now operates within defined limits to achieve its process outcomes.
5 (Optimizing)	The predictable process is continuously improved to meet relevant current and projected business goals.

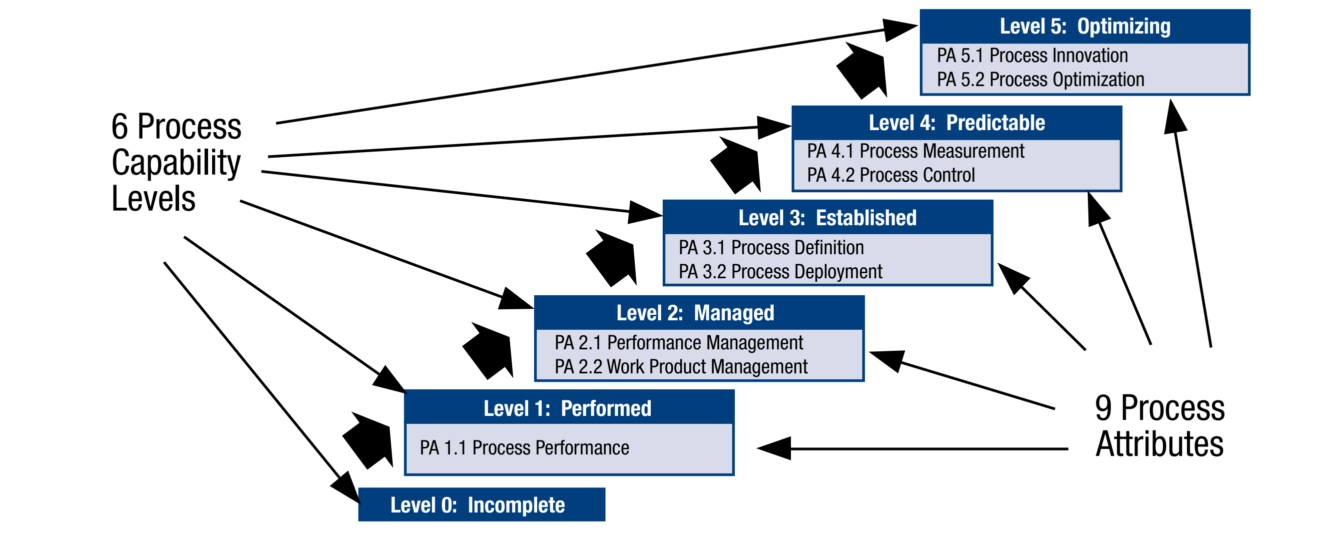
Process capability level 0 does not have an attribute. Level 0 reflects a non-implemented process or a process that fails to at least partially achieve its outcomes.

As part of the scoping, the enterprise should choose which level of capability it requires, depending on business objectives. Scoping can also restrict an assessment to reduce the complexity, effort and cost of the assessment.

2.2.2 Process Attributes

Within the COBIT PAM, the measure of capability is based on the nine process attributes (prefixed by PA) defined in ISO/IEC 15504-2, as shown in **figure 3**. Each attribute applies to a specific process capability. Process attributes are used to determine whether a process has reached a given capability.

Figure 3—Process Attributes


Level 5: Optimizing
PA 5.1 Process Innovation
PA 5.2 Process Optimization
Level 4: Predictable
PA 4.1 Process Measurement
PA 4.2 Process Control
Level 3: Established
PA 3.1 Process Definition
PA 3.2 Process Deployment
Level 2: Managed
PA 2.1 Performance Management
PA 2.2 Work Product Management
Level 1: Performed
PA 1.1 Process Performance
Level 0: Incomplete
6 Process Capability Levels
9 Process Attributes

2.2.3 Assessment Indicators

Assessment indicators in the COBIT PAM provide the basis for determining whether process attributes have been achieved:

- **Capability Level 1**—Indicators are specific for each process and assess whether the following attribute has been achieved: *The implemented process achieves its process purpose.*
- **Capability Levels 2 to 5**—Assessment of capability is based on generic process indicators of performance. These are called generic because they apply across all processes, but they are different from one capability level to another.

Note: Level 1 deals specifically with the 'detailed content' of each of the 37 COBIT 5 processes. Levels 2 through 5 are discussed with the 'generic attributes' for all processes.

It is generally understood that the higher the process capability level reached, the lower the risk of the process failing to meet its intended purpose. It is also generally understood that the higher the capability, the more costly the process is to operate.

2.2.4 Rating Scale

Each attribute is rated using a standard rating scale defined in the ISO/IEC 15504 standard. These ratings consist of:

- **N**—Not achieved. There is little or no evidence of achievement of the defined attribute in the assessed process.
- **P**—Partially achieved. There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable.
- **L**—Largely achieved. There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weaknesses related to this attribute may exist in the assessed process.
- **F**—Fully achieved. There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process.

There is a need to ensure a consistent degree of interpretation when deciding which rating to assign. The table in **figure 4** describes the rating in terms of both the original rating scale (defined previously) and those ratings translated into a percentage scale showing the extent of achievement.

Figure 4—Rating Levels

N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
F	Fully achieved	>85% to 100% achievement

Source: This figure is reproduced from ISO/IEC 15504-2:2003, with the permission of ISO/IEC at *www.iso.org*. Copyright remains with ISO/IEC.

The assessors use these scales during their assessment to guide their judgement of the current level of achievement.

2.2.5 Determining the Capability Level

The capability level of a process is determined by whether the process attributes at that level have been largely or fully achieved and whether the process attributes for the lower levels have been fully achieved. The table in **figure 5** outlines each level and the necessary ratings that must be achieved.

Figure 5—Levels and Necessary Ratings

Scale	Process Attributes	Rating
Level 1	Process Performance	Largely or fully
Level 2	Process Performance Performance Management Work Product Management	Fully Largely or fully Largely or fully
Level 3	Process Performance Performance Management Work Product Management Process Definition Process Deployment	Fully Fully Fully Largely or fully Largely or fully
Level 4	Process Performance Performance Management Work Product Management Process Definition Process Deployment Process Measurement Process Control	Fully Fully Fully Fully Fully Largely or fully Largely or fully

Figure 5—Levels and Necessary Ratings *(cont.)*

Scale	Process Attributes	Rating
Level 5	Process Performance Performance Management Work Product Management Process Definition Process Deployment Process Measurement Process Control Process Innovation Process Optimization	Fully Fully Fully Fully Fully Fully Fully Largely or fully Largely or fully

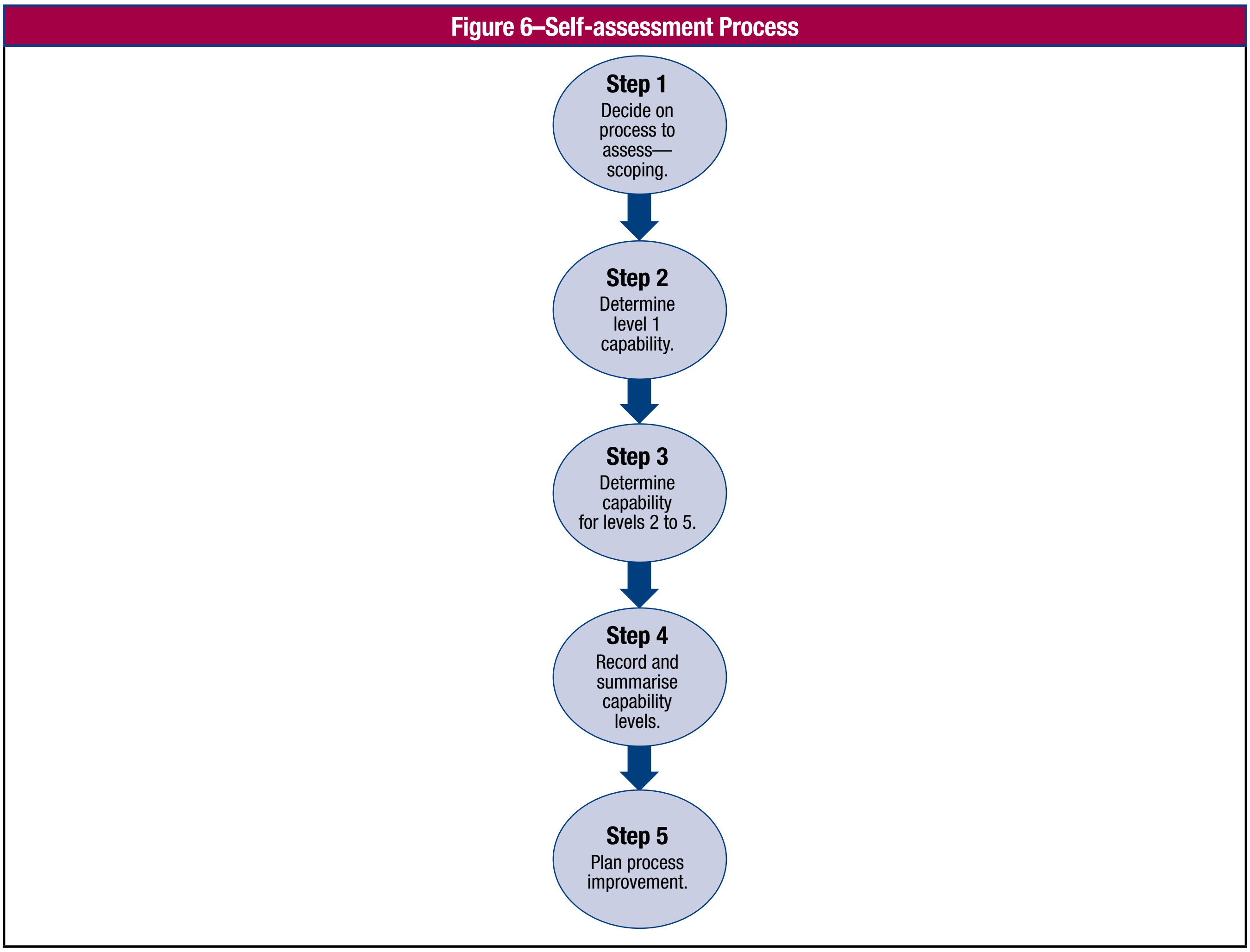
Source: This table is reproduced from ISO/IEC 15504-2, with the permission of ISO/IEC at *www.iso.org*. Copyright remains with ISO/IEC.

Note: A process can be rated at one level with an attribute 'largely' or 'fully' achieved. However, the attribute will need to be fully achieved to be rated at the next level.

3.0 The COBIT Self-assessment Process

The COBIT self-assessment process, shown in **figure 6**, is a simplified approach to performing an assessment that is not evidence-based, does not require an independent or certified assessor and can be done by enterprise management as a precursor to a more formal assessment. A self-assessment can identify process gaps that require improvements in advance of a formal assessment; it can be done for a relatively small investment and assists enterprise management in setting target capability levels.

Figure 6—Self-assessment Process


Step 1
Decide on process to assess—scoping.
Step 2
Determine level 1 capability.
Step 3
Determine capability for levels 2 to 5.
Step 4
Record and summarise capability levels.
Step 5
Plan process improvement.

The self-assessment is supported by the:

- Assessment summary table in appendix A
- Detailed assessment schedule (An example of EDM01 is provided in appendix B. There is a more detailed template that includes all 37 COBIT 5 processes provided in the supplementary tool kit. In section 1 the results are summarised and the capability level determined, and section 2 records an assessment against criteria for each level of capability.)

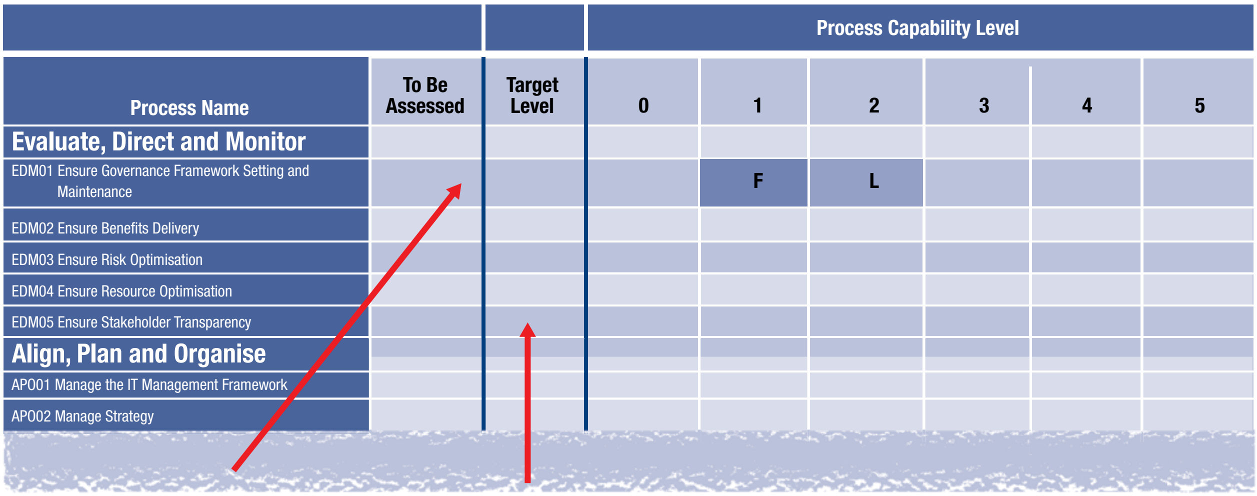
3.1 Step 1—Decide on Processes to Assess—Scoping

The first step in the self-assessment is to decide what processes are to be assessed. Use the scoping template in the COBIT assessment programme tool kit to help select the processes to be assessed. Those processes selected should be recorded in the table in appendix A, as shown in **figure 7**.

A self-assessment can address all the COBIT processes or focus on a number of processes of concern to enterprise management or on those relating to specific business goals for IT.

The assessment scoping tool in the tool kit provides mappings related to business goals and IT goals. The tool kit is provided 'in hierarchical format' with the *COBIT Assessor Guide: Using COBIT 5* and the *COBIT Self-assessment Guide: Using COBIT 5*.

Figure 7—Assessment Summary Table



Process Name	To Be Assessed	Target Level	Process Capability Level 0	1	2	3	4	5
Evaluate, Direct and Monitor								
EDM01 Ensure Governance Framework Setting and Maintenance				F	L			
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								

Step 1—Decide and record which processes are to be assessed.

Record the target process capability level.

At this stage, the target process capability level can be recorded. This will establish the level of capability required of the process. In setting the target capability levels, consideration should be given to the impact on the business objectives of the enterprise if a specified level of capability is not achieved. The first consideration is the impact on the enterprise if the process is non-existent or not working effectively or efficiently. The second consideration concerns the additional consequences of the effective and efficient operation of the processes at the various capability levels, as shown in **figure 8** from ISO/IEC 15504-4.

Figure 8—Additional Consequences of the Effective and Efficient Operation of the Processes

Capability Level	Process Attribute Where Gap Occurs	Potential Consequence
1	PA 1.1 Process Performance	Missing work products; process outcomes not achieved
2	PA 2.1 Performance Management	• Cost or time overruns; inefficient use of resources; unclear responsibilities • Uncontrolled decisions; uncertainty over whether time and cost objectives will be met
	PA 2.2 Work Product Management	• Unpredictable product quality and integrity; uncontrolled versions; increased support costs; integration problems; increased rework costs
3	PA 3.1 Process Definition	• Identified best practice and lessons learned from previous projects not defined, published and available within organization • No foundation for organizationwide process improvement
	PA 3.2 Process Deployment	• Implemented process not incorporating identified best practice and lessons leaned from previous projects; inconsistent process performance across organization • Lost opportunities to understand process and identify improvements
4	PA 4.1 Process Management	• No quantitative understanding of how well process performance objectives and defined business goals are being achieved. • No quantitative ability to detect performance problems early
	PA 4.2 Process Control	• Process not capable and/or stable (predictable) within defined limits • Quantitative performance objectives and defined business goals not met
5	PA 5.1 Process Innovation	• Process improvement objectives not clearly defined • Opportunities for improvement not clearly identified
	PA 5.2 Process Optimization	• Inability to change process effectively to achieve relevant process improvement objectives • Inability to evaluate effectiveness of process changes

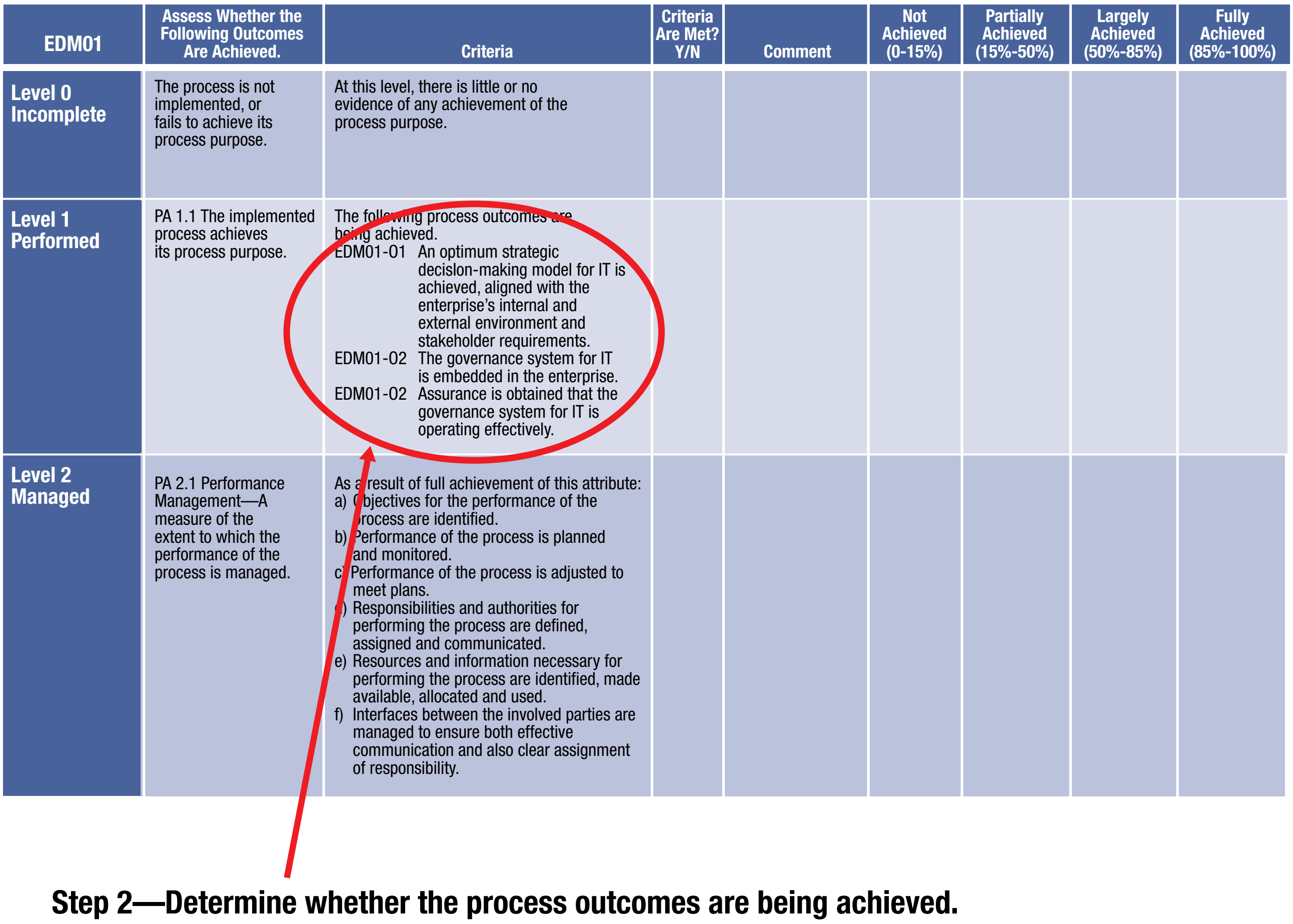
Source: This figure is reproduced from ISO/IEC 15504-4, with the permission of ISO/IEC at *www.iso.org*. Copyright remains with ISO/IEC.

3.2 Step 2—Determine Whether the Selected Process Is a Level 1 Capability

The first step in the assessment of each process is to determine whether a process is actually being performed and is achieving its outcomes. In the self-assessment worksheet (appendix B) there is a table for each process. The indicators at capability level 1 are specific for each process and assess whether the following attribute has been achieved: *The implemented process achieves its purpose.*

As shown in **figure 9**, under the column titled 'criteria' there is a list of process outcomes. These are from COBIT 5 and are different for each process.

Figure 9—Assessment Template Example



EDM01	Assess Whether the Following Outcomes Are Achieved.	Criteria	Criteria Are Met? Y/N	Comment	Not Achieved (0-15%)	Partially Achieved (15%-50%)	Largely Achieved (50%-85%)	Fully Achieved (85%-100%)
Level 0 Incomplete	The process is not implemented, or fails to achieve its process purpose.	At this level, there is little or no evidence of any achievement of the process purpose.						
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	The following process outcomes are being achieved. EDM01-01 An optimum strategic decision-making model for IT is achieved, aligned with the enterprise's internal and external environment and stakeholder requirements. EDM01-02 The governance system for IT is embedded in the enterprise. EDM01-02 Assurance is obtained that the governance system for IT is operating effectively.						
Level 2 Managed	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 both effective communication and also clear assignment of responsibility.						

Step 2—Determine whether the process outcomes are being achieved.

In undertaking an assessment for capability level 1 for any process, the extent to which the outcomes for the process are being achieved needs to be decided, as shown in **figure 10**.

Figure 10—Rating Levels

N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
F	Fully achieved	>85% to 100% achievement

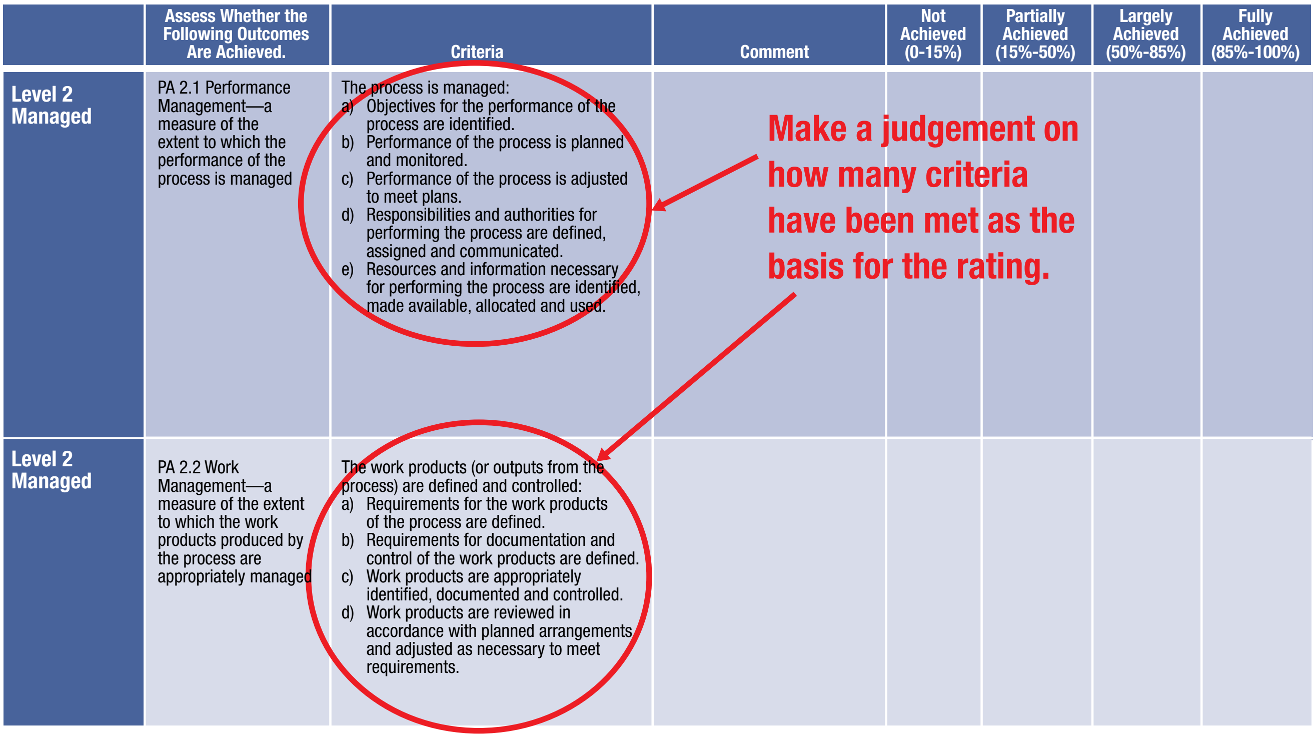
Source: This figure is reproduced from ISO/IEC 15504-2:2003, with the permission of ISO/IEC at *www.iso.org*. Copyright remains with ISO/IEC.

In the case of EDM01 in **figure 11**, if all three outcomes are being achieved, it can be rated **F** for 'fully achieved'; if only two outcomes are achieved, it can be rated **L** for 'largely achieved'; if only one outcome is achieved, it can be rated **P** for 'partially achieved', and if none are achieved, it can be rated **N** for 'not achieved'. In some cases, some of the outcomes are being achieved, in which case it will be rated **L** (largely) or **P** (partially) achieved; judgement is required.

3.3 Step 3—Determine Whether Capability Levels 2 to 5 for the Selected Processes Are Being Achieved

Above level 2, the assessment criteria are generic, i.e., the criteria are the same for each and every process.

Figure 11—Detailed Assessment Schedule Part 2: Level 2 (Managed)



	Assess Whether the Following Outcomes Are Achieved.	Criteria	Comment	Not Achieved (0-15%)	Partially Achieved (15%-50%)	Largely Achieved (50%-85%)	Fully Achieved (85%-100%)
Level 2 Managed	PA 2.1 Performance Management—a measure of the extent to which the performance of the process is managed	The process is managed: 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.					
Level 2 Managed	PA 2.2 Work Management—a measure of the extent to which the work products produced by the process are appropriately managed	The work products (or outputs from the process) are defined and controlled: 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.					

Make a judgement on how many criteria have been met as the basis for the rating.

Again, in each case, a judgement must be made as to whether the criteria have been met, and that decision must be translated into a rating (**figure 10**) and recorded in the template for the process.

This should be repeated for each capability until a capability level is rated as 'largely' or 'fully achieved'.

3.4 Step 4—Record and Summarise the Capability Levels

The summary of assessment results should be recorded in section 1. The capability level is determined at the level where both capability indicators are either 'largely' or 'fully achieved'.

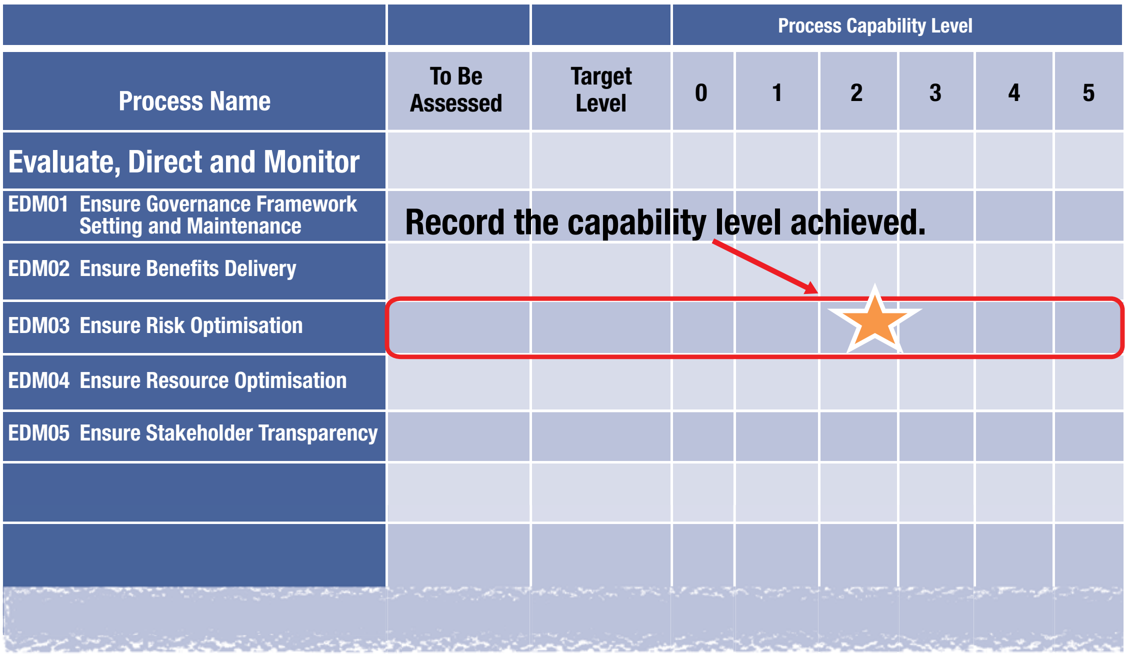
In **figure 12**, the capability level of the process is level 2. This should be recorded in the process assessment results table, as shown in **figure 13**.

Figure 12—Detailed Assessment Schedule Section 1

Process Name	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
EDM01		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria		**F**	**F**	**L**	**P**	**N**				
Capability Level Achieved				**2**						

Legend:
N (Not Achieved, 0–15%) **P** (Partially Achieved, >15%–50%) **L** (Largely Achieved, >50%–85%) **F** (Fully Achieved, >85–100%)

Figure 13—Assessment Summary Table



			Process Capability Level					
Process Name	To Be Assessed	Target Level	0	1	2	3	4	5
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								

Record the capability level achieved.

3.5 Step 5—Develop an Improvement Plan of Action

Based on the self-assessment, consideration should be given to the development of a plan of action for process improvement.

One option could be to commence an initial improvement plan based on the self-assessment. This could address the areas of highest importance to the enterprise's business goals and focus on areas with gaps between the 'current' and 'target' process capability levels.

A second option would be to undertake a more formal independent assessment, based on the COBIT PAM and the assessor guide. This will provide a more reliable assessment and more guidance to the areas of required improvements.

For further guidance on process improvement and process capability determination, see appendix C. The recommended reference is: ISO, ISO/IEC 15504-4 2004, *Guidance on use for process improvement and process capability determination*, Switzerland, 2004.

Page intentionally left blank

Appendix A. Process Assessment Results

Figure 14—Process Assessment Results

Process Name	To Be Assessed	Process Capability Level					
		0	1	2	3	4	5
Evaluate, Direct and Monitor (EDM)							
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 (APO)							
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 Suppliers							
APO11 Manage Quality							
APO12 Manage Risk							
APO13 Manage Security							
Build, Acquire and Implement (BAI)							
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 Configuration							
Deliver, Service and Support (DSS)							
DSS01 Manage Operations							
DSS02 Manage Service Requests and Incidents							
DSS03 Manage Problems							
DSS04 Manage Continuity							
DSS05 Manage Security Services							
DSS06 Manage Business Process Controls							
Monitor, Evaluate and Assess (MEA)							
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							

Page intentionally left blank

Appendix B. Self-assessment Template

Example EDM01 Ensure Governance Framework Setting and Maintenance

Figure 15 shows the summary template for the assessment results for the EDM01 example.

Figure 15—Summary of the Assessment Result

Process Name	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria										
Capability Level Achieved										
Legend: **N** (Not Achieved, 0–15%) **P** (Partially Achieved, 15%–50%) **L** (Largely Achieved, 50%–85%) **F** (Fully Achieved, 85–100%)										

Figure 16 shows the detailed assessments for the EDM01 example, using the data collection spreadsheet tool from the supporting tool kit.

Figure 16—Example Detailed Assessments for EDM01

EDM01	**Ensure Governance Framework Setting and Maintenance**							
Purpose	Satisfy the business requirement of sustaining or extending the business strategy and governance requirements while being transparent about benefits, cost and risk.							
EDM01	**Assess Whether the Following Outcomes Are Achieved.**	**Criteria**	**Criteria Are Met? Y/N**	**Comment**	**Not Achieved (0–15%)**	**Partially Achieved (>15%–50%)**	**Largely Achieved (>50%–85%)**	**Fully Achieved (>85%–100%)**
Level 0 Incomplete	**The process is not implemented or fails to achieve its process purpose.**	At this level, there is little or no evidence of any achievement of the process purpose.						
Level 1 Performed	**PA 1.1 Process Performance—The implemented process achieves its process purpose.**	The following process outcomes are being achieved: • EDM01-01 An optimum strategic decision-making model for IT is achieved, aligned with the enterprise's internal and external environment and stakeholder requirements. • EDM01-02 The governance system for IT is embedded in the enterprise. • EDM01-02 Assurance is obtained that the governance system for IT is operating effectively.						
Level 2 Managed	**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 both effective communication and clear assignment of responsibility.						

Figure 16—Example Detailed Assessments for EDM01 *(cont.)*

EDM01	Ensure Governance Framework Setting and Maintenance								
Purpose	Satisfy the business requirement of sustaining or extending the business strategy and governance requirements while being transparent about benefits, cost and risk.								
EDM01	**Assess Whether the Following Outcomes Are Achieved.**	**Criteria**	**Criteria Are Met? Y/N**	**Comment**	**Not Achieved (0–15%)**	**Partially Achieved (>15%–50%)**	**Largely Achieved (>50%–85%)**	**Fully Achieved (>85%–100%)**
Level 2 Managed *(cont.)*	**PA 2.2 Work Product Management—A measure of the extent to which the work products produced by the process are appropriately managed. The work products (or outputs from the process) are defined and controlled.**	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.						
Level 3 Established	**PA 3.1 Process Definition—A measure of the extent to which a standard process is maintained to support the deployment of the defined process.**	As a result of full achievement of this attribute: a. A standard process, including appropriate tailoring guidelines, is defined that describes the fundamental elements that must be incorporated into a defined process. b. The sequence and interaction of the standard process with other processes are determined. c. Required competencies and roles for performing a process are identified as part of the standard process. d. Required infrastructure and work environment for performing a process are identified as part of the standard process. e. Suitable methods for monitoring the effectiveness and suitability of the process are determined.						
	PA 3.2 Process Deployment—A measure of the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes.	As a result of full achievement of this attribute: a. A defined process is deployed based on an appropriately selected and/or tailored standard process. b. Required roles, responsibilities and authorities for performing the defined process are assigned and communicated. c. Personnel performing the defined process are competent on the basis of appropriate education, training and experience. d. Required resources and information necessary for performing the defined process are made available, allocated and used. e. Required infrastructure and work environment for performing the defined process are made available, managed and maintained. f. Appropriate data are collected and analysed as a basis for understanding the behaviour, and to demonstrate the suitability and effectiveness of the process, and to evaluate where continuous improvement of the process can be made.						

Figure 16—Example Detailed Assessments for EDM01 *(cont.)*

EDM01	**Ensure Governance Framework Setting and Maintenance**							
Purpose	Satisfy the business requirement of sustaining or extending the business strategy and governance requirements while being transparent about benefits, cost and risk.							
EDM01	**Assess Whether the Following Outcomes Are Achieved.**	**Criteria**	**Criteria Are Met? Y/N**	**Comment**	**Not Achieved (0–15%)**	**Partially Achieved (>15%–50%)**	**Largely Achieved (>50%–85%)**	**Fully Achieved (>85%–100%)**
Level 4 Predictable	**PA 4.1 Process Measurement—A measure of the extent to which measurement results are used to ensure that performance of the process supports the achievement of relevant process performance objectives in support of defined business goals.**	As a result of full achievement of this attribute: a. Process information needs in support of relevant defined business goals are established. b. Process measurement objectives are derived from process information needs. c. Quantitative objectives for process performance in support of relevant business goals are established. d. Measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance. e. Results of measurement are collected, analysed and reported to monitor the extent to which the quantitative objectives for process performance are met. f. Measurement results are used to characterise process performance.						
	PA 4.2 Process Control—A measure of the extent to which the process is quantitatively managed to produce a process that is stable, capable and predictable within defined limits.	As a result of full achievement of this attribute: a. Analysis and control techniques are determined and applied where applicable. b. Control limits of variation are established for normal process performance. c. Measurement data are analysed for special causes of variation. d. Corrective actions are taken to address special causes of variation. e. Control limits are re-established (as necessary) following corrective action.						
Level 5 Optimizing	**PA 5.1 Process Innovation—A measure of the extent to which changes to the process are identified from analysis of common causes of variation in performance, and from investigations of innovative approaches to the definition and deployment of the process.**	As a result of full achievement of this attribute: a. Process improvement objectives for the process are defined that support the relevant business goals. b. Appropriate data are analysed to identify common causes of variations in process performance. c. Appropriate data are analysed to identify opportunities for best practice and innovation. d. Improvement opportunities derived from new technologies and process concepts are identified. e. An implementation strategy is established to achieve the process improvement objectives.						
	PA 5.2 Process Optimization—A measure of the extent to which changes to the definition, management and performance of the process result in effective impact that achieves the relevant process improvement objectives.	As a result of full achievement of this attribute: a. Impact of all proposed changes is assessed against the objectives of the defined process and standard process. b. Implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted on. c. Effectiveness of process change on the basis of actual performance is evaluated against the defined product requirements and process objectives to determine whether results are due to common or special causes.						

Appendix C. Further Reading

- ISACA, COBIT® 5, USA, 2012
- ISACA, *COBIT® 5 Implementation*, USA, 2012
- ISACA, *COBIT® 5: Enabling Processes*, USA, 2012
- ISACA, *COBIT® Process Assessment Guide (PAM): Using COBIT® 5*, USA, 2012
- ISACA, *COBIT® Assessor Guide: Using COBIT® 5*, USA, 2012
- ISO, ISO/IEC 15504-1 *2004 Information technology—Process assessment—Part 1: Concepts and vocabulary*, Switzerland, 2004
- ISO, ISO/IEC 15504-2 2003 *Performing an assessment*, Switzerland, 2003
- ISO, ISO/IEC 15504-3 2004 *Guidance on performing an assessment*, Switzerland, 2004
- ISO, ISO/IEC 15504-4 2004 *Guidance on use for process improvement and process capability determination*, Switzerland, 2004
- ISO, ISO/IEC 15504-5 2006 *Information technology—Process assessment—Part 5: An exemplar Process Assessment Model*, Switzerland, 2006
- ISO, ISO/IEC 15504-7 2008 *Assessment of organizational maturity*, Switzerland, 2008