



BSI Standards Publication

Information technology — Process assessment — Process capability assessment model for information security management

National foreword

This Published Document is the UK implementation of ISO/IEC TS 33072:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 93543 5

ICS 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2016.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

First edition
2016-07-15

Corrected version
2016-09-01

Information technology — Process assessment — Process capability assessment model for information security management

*Technologies de l'information — Évaluation des procédés — Modèle
d'évaluation de la capacité des procédés pour le management de la
sécurité de l'information*



Reference number
ISO/IEC TS 33072:2016(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2016

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview of the Process Assessment Model	2
4.1 Introduction to Overview	2
4.2 Structure of the Process Assessment Model	3
4.2.1 Processes	3
4.2.2 Process dimension	4
4.2.3 Capability dimension	4
4.3 Assessment Indicators	6
4.3.1 Process Capability Indicators	7
4.3.2 Process Performance Indicators	8
4.4 Measuring process capability	9
5 The process dimension and process performance indicators (Level 1)	10
5.1 General	10
5.2 ORG.1 Asset management	11
5.3 TEC.01 Capacity management	12
5.4 TEC.02 Change management	13
5.5 COM.01 Communication management	13
5.6 TEC.03 Configuration management	14
5.7 COM.02 Documentation management	15
5.8 ORG.2 Equipment management	17
5.9 ORG.3 Human resource employment management	18
5.10 COM.03 Human resource management	19
5.11 COM.04 Improvement	20
5.12 TEC.04 Incident management	21
5.13 ORG.4 Infrastructure and work environment	21
5.14 COM.05 Internal audit	22
5.15 TOP.1 Leadership	23
5.16 COM.06 Management review	24
5.17 COM.07 Non-conformity management	25
5.18 COM.09 Operational implementation and control	26
5.19 COM.08 Operational planning	27
5.20 COM.10 Performance evaluation	29
5.21 TEC.05 Product/service release	30
5.22 TEC.08 Product/Service/System requirements	31
5.23 COM.11 Risk and opportunity management	32
5.24 TEC.06 Service availability management	33
5.25 TEC.07 Service continuity management	34
5.26 ORG.5 Supplier management	34
5.27 TEC.09 Technical data preservation and recovery	35
6 Process capability indicators	36
6.1 Introduction	36
6.2 Process capability levels and process attributes	36
6.2.1 Process capability Level 0: Incomplete process	36
6.2.2 Process capability Level 1: Performed process	36
6.2.3 Process capability Level 2: Managed process	37

6.2.4	Process capability Level 3: Established process.....	42
6.2.5	Process capability Level 4: Predictable process	46
6.2.6	Process capability Level 5: Innovating process.....	51
6.3	Related processes for process attributes.....	55
Annex A	(informative) Conformity of the process assessment model.....	57
A.1	Introduction	57
A.2	Requirements for process assessment models	57
A.2.1	Introduction	57
A.2.2	Process assessment model scope	57
A.2.3	Requirements for process assessment models	58
A.2.4	Assessment indicators	58
A.2.5	Mapping process assessment models to process reference models.....	59
A.2.6	Expression of assessment results.....	61
Annex B	(informative) Input and output characteristics	62
B.1	General.....	62
B.2	Generic input and outputs	63
B.3	Specific inputs and outputs.....	67
Annex C	(informative) Association between base practices and ISO/IEC 27001 requirements	96
C.1	Associations of base practices with requirements.....	97
C.2	Associations of requirements with base practices.....	135
C.3	Base practices that have no associated requirements.....	179
	Bibliography	182

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 7, *Software and systems engineering*.

This corrected version of ISO/IEC 33072 incorporates the text that was not visible in Annex B, Table B.3, references 08-39 and 08-40, in the column entitled: "*Characteristics*".

Introduction

This Technical Specification provides an Information Security Management Process Assessment Model (PAM) for use in performing a conformant assessment of process capability in accordance with the requirements of ISO/IEC 33002. It is structured in accordance with the requirements of ISO/IEC 33004 to reflect processes that enable implementation of ISO/IEC 27001. The scale for assessing the extent of achievement of process capability is based on ISO/IEC 33020.

An integral part of conducting an assessment is to use a PAM that is constructed for that purpose. A PAM is related to a Process Reference Model (PRM) and is conformant with ISO/IEC 33004. ISO/IEC 33002 identifies the minimum requirements for performing an assessment in order to ensure consistency and repeatability of the ratings. ISO/IEC 33002 addresses the assessment of process and the application of process assessment for improvement and capability determination. Results of conformant process assessments can be compared when the scopes of the assessments are considered to be similar. The requirements for process assessment defined in ISO/IEC 33002 form a structure which:

- a) facilitates self-assessment;
- b) provides a basis for use in process improvement and capability determination;
- c) takes into account the context in which the assessed process is implemented;
- d) produces a process rating;
- e) addresses the ability of the process to achieve its purpose;
- f) is applicable across all application domains and sizes of organization;
- g) can provide an objective benchmark between organizations.

The PRM defined in ISO/IEC TS 33052 has been used as the basis for the PAM in ISO/IEC TS 33072; the process measurement framework for process capability defined in ISO/IEC 33020 is the basis for the capability measurement scale. The relationship between ISO/IEC 24774, ISO/IEC 27001, ISO/IEC 3002, ISO/IEC 33004, ISO/IEC 33020, ISO/IEC TS 33052 and ISO/IEC TS 33072 is shown in Figure 1.

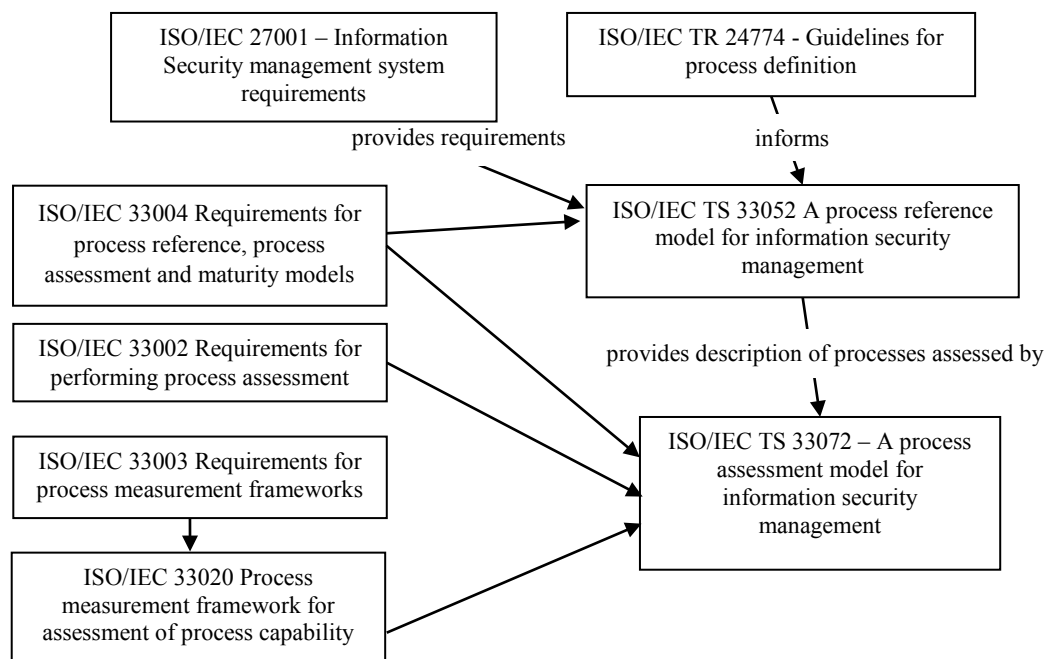


Figure 1 — Relationships between relevant standards

Any organisation can use processes with additional elements in order to suit it to the environment and circumstances. This PAM contains a set of indicators to be considered when interpreting the intent of its PRM. It provides greater detail to indicate process performance and capability. The indicators can also be used when implementing a process improvement program or to help evaluate and select an assessment model, method, methodology or tools.

This PAM embodies the core characteristics that could be expected of any PAM consistent with ISO/IEC 33004. Nevertheless any other PAMs meeting the requirements of ISO/IEC 33004 can be used in a conformant assessment.

ISO/IEC 33072 has a similar structure to ISO/IEC 15504-5 and ISO/IEC 15504-6. It can be used in conjunction with these process assessment models to support joint assessment of information security processes and system/software life cycle processes.

Within this Technical Specification:

- Clause 4 provides a detailed description of the structure and key components of a PAM, which includes two dimensions: a process dimension and a capability dimension. Assessment indicators are introduced in this clause;
- Clause 5 addresses the process dimension. It uses process definitions from ISO/IEC TS 33052 to designate the PRM. The processes of the PRM are described in the PAM in terms of purpose and outcomes. The PAM expands the PRM process definitions by including a set of process performance indicators called base practices for each process. The PAM also defines a second set of indicators of process performance by associating inputs and outputs with each process. Clause 5 is also linked directly to Annex B, which defines the inputs/outputs characteristics;
- Clause 6 addresses the capability dimension. It duplicates the definitions of the capability levels and process attributes from ISO/IEC 33020, and expands each of the nine attributes through the inclusion of a set of generic practices. These generic practices belong to a set of indicators of process capability, in association with generic resource indicators, and generic inputs/outputs indicators. Annex B is also linked directly to Clause 6 as it defines the inputs/outputs characteristics;

- Annex A provides a statement of conformance of the PAM to the requirements defined in ISO/IEC 33004;
- Annex B provides selected characteristics for typical inputs/outputs to assist the assessor in evaluating the capability level of processes;
- Annex C contains three tables. Table C.1 identifies the base practices linked to requirements; Table C.2 identifies the requirements linked to base practices; and lastly, Table C.3 identifies the base practices not linked to requirements.
- a Bibliography contains a list of informative references.

This page deliberately left blank

Information technology — Process assessment — Process capability assessment model for information security management

1 Scope

This Technical Specification:

- defines a process assessment model (PAM) that meets the requirements of ISO/IEC 33004 and that supports the performance of an assessment of process capability by providing indicators for guidance on the interpretation of the process purposes and outcomes as defined in ISO/IEC TS 33052 and the process attributes as defined in ISO/IEC 33020;
- provides guidance, by example, on the definition, selection and use of assessment indicators.

A PAM comprises a set of indicators of process performance and process capability. The indicators are used as a basis for collecting the objective evidence that enables an assessor to assign ratings. The set of indicators included in this Technical Specification is not intended to be an all-inclusive set nor is it intended to be applicable in its entirety.

The PAM in this Technical Specification is directed at assessment sponsors and competent assessors who wish to select a model, and associated documented process method, for assessment (for either capability determination or process improvement). Additionally it may be of use to developers of assessment models in the construction of their own model, by providing examples of good information security management practices. It can be used by:

- a) service providers to assess and improve an Information Security Management System (ISMS);
- b) service providers to demonstrate their capability for the design, development, transition and delivery of services that fulfil information security management requirements.

Any PAM meeting the requirements defined in ISO/IEC 33004 concerning models for process assessment can be used for assessment. Different models and methods might be needed to address differing business needs. The assessment model in this Technical Specification meets all the requirements expressed in ISO/IEC 33004.

NOTE Copyright release for the PAM: Users of this Technical Specification may reproduce subclauses 5.2 to 5.27, 6.2, B.2 and B.3 as part of any tool or other material to support the performance of process assessments so that it can be used for its intended purpose.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 33001 and ISO/IEC 27000 apply.

4 Overview of the Process Assessment Model

4.1 Introduction to Overview

ISO/IEC 33072 provides a PAM that includes examples of assessment indicators.

The PRM defined in ISO/IEC TS 33052, associated with the process attributes defined in ISO/IEC 33020, establish a PAM used as a common basis for performing assessments of information security management system process capability, allowing for the reporting of results using a common rating scale.

This PAM is a two-dimensional model of the process quality characteristic of process capability. In one dimension, the process dimension, the processes are defined. In the other dimension, the capability dimension, a set of process attributes grouped into capability levels is defined. The process attributes provide the measurable characteristics of the process quality characteristic of process capability.

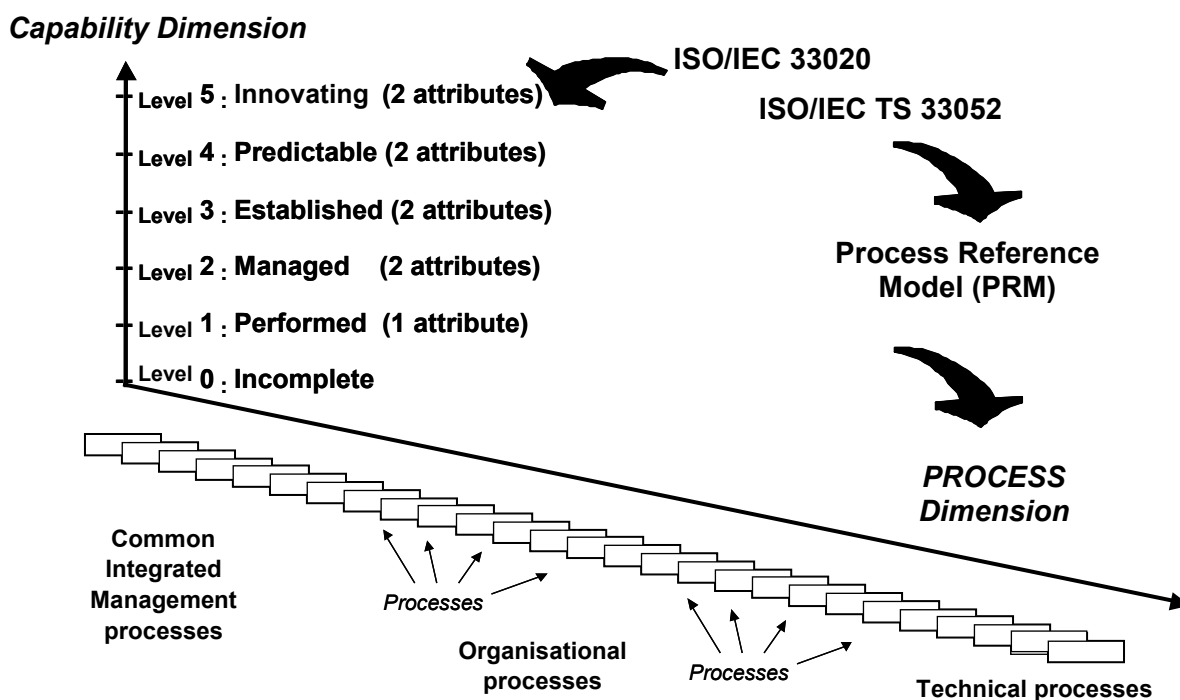


Figure 2 — Relationship between the Process Assessment Model and its inputs

Figure 2 shows the relationship between the general structure of the PAM, ISO/IEC 33020 and ISO/IEC TS 33052.

A PRM conformant with the requirements defined in ISO/IEC 33004 and a capability dimension defined in ISO/IEC 33020 cannot be used alone as the basis for conducting reliable and consistent assessments of process capability since the level of detail provided is not sufficient. The descriptions of process purpose and outcomes in a PRM, and the process attribute definitions in ISO/IEC 33020, need to be supported with a comprehensive set of indicators of process performance and process capability that are used for assessment performance.

The PAM defined in ISO/IEC 33072 is conformant with the ISO/IEC 33004 requirements for a PAM, and can be used as the basis for conducting an assessment of information security management process capability.

In order to meet the PAM requirements of ISO/IEC 33004, a documented process supporting other requirements of ISO/IEC 33002 is also required. This need may be met, for example, by the adoption of a supporting method for conducting assessments.

4.2 Structure of the Process Assessment Model

This clause describes the detailed structure of the PAM and its key components.

This PAM expands upon the PRM by including a defined set of assessment indicators. Assessment indicators comprise indicators of process performance and process capability and are defined to support an assessor's judgment of the performance and capability of an implemented process.

Clause 5, together with its associated Annex B, describes the components of the process dimension, and clause 6 describes the components of the capability dimension. Annex A provides a statement of conformance of the PAM to the requirements defined in ISO/IEC 33004.

ISO/IEC 33004 requires that processes included in a PRM satisfy the following:

"The fundamental elements of a process reference model are the descriptions of the processes within the scope of the model.

The process descriptions in the process reference model incorporate a statement of the purpose of the process which describes at a high level the overall objectives of performing the process, together with the set of outcomes which demonstrate successful achievement of the process purpose.

A process description shall meet the following requirements:

- a) a process shall be described in terms of its purpose and process outcomes;*
- b) the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process;*
- c) process descriptions shall not contain or imply aspects of the process quality characteristic beyond the basic level of any relevant process measurement framework conformant with ISO/IEC 33003."*

As processes are derived directly from ISO/IEC TS 33052, these requirements are satisfied.

4.2.1 Processes

Figure 3 shows the processes from ISO/IEC TS 33052, which are included in the process dimension of the PAM for information security management.

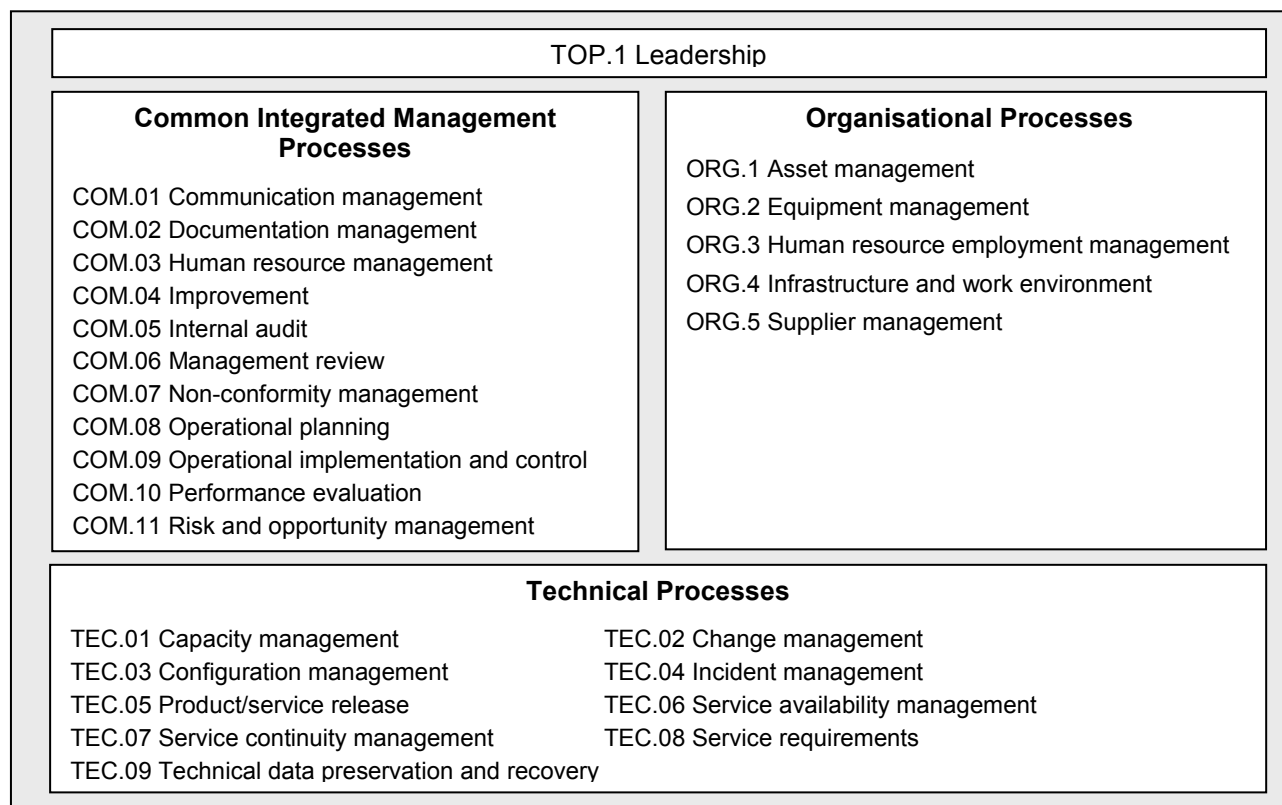


Figure 3 — Processes in the Process Reference Model

4.2.2 Process dimension

The process dimension of the PAM includes all processes from the PRM contained in ISO/IEC TS 33052 and shown in Figure 3. Each process in the PAM is described in terms of a purpose statement. These statements contain the unique functional objectives of the process when performed in a particular environment. A list of specific outcomes is associated with each of the process purpose statements, as a list of expected positive results of the performance of the processes.

Satisfying the purpose statements of a process represents the first step in building a level 1 process capability where the expected outcomes are observable. The processes are described in Clause 5.

4.2.3 Capability dimension

For the capability dimension, the process capability levels and process attributes are identical to those defined in ISO/IEC 33020.

Evolving process capability is expressed in the PAM in terms of process attributes grouped into capability levels. Process attributes are features of a process that can be evaluated on a scale of achievement, providing a measure of the capability of the process. They are applicable to all processes. Each process attribute describes a facet of the overall capability of managing and improving the effectiveness of a process in achieving its purpose and contributing to the business goals of the organization.

A capability level is a set of process attribute(s) that work together to provide a major enhancement in the capability to perform a process. The levels constitute a rational way of progressing through improvement of the capability of any process and are defined in ISO/IEC 33020.

There are six capability levels, incorporating nine process attributes.

Level 0: Incomplete process

The process is not implemented, or fails to achieve its process purpose.

At this level, there is little or no evidence of any systematic achievement of the process purpose.

Level 1: Performed process

The implemented process achieves its process purpose.

Level 2: Managed process

The previously described Performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

Level 3: Established process

The previously described Managed process is now implemented using a defined process that is capable of achieving its process outcomes.

Level 4: Predictable process

The previously described Established process now operates predictively within defined limits to achieve its process outcomes. Quantitative management needs are identified, measurement data are collected and analysed to identify assignable causes of variation. Corrective action is taken to address assignable causes of variation.

Level 5: Innovating process

The previously described Predictable process is now continually improved to respond to change aligned with organizational goals.

Within the PAM, the measure of capability is based upon the nine process attributes (PA) defined in ISO/IEC 33020. Process attributes are used to determine whether a process has reached a given capability. Each attribute measures a particular aspect of the process capability.

At each level there is no ordering between the process attributes; each attribute addresses a specific aspect of the capability level. The list of process attributes is shown in Table 1.

Table 1 — Capability levels and process attributes

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work Products management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Quantitative analysis
PA 4.2	Quantitative control
	Level 5: Innovating process
PA 5.1	Process innovation
PA 5.2	Process innovation implementation

The process attributes are evaluated on a four point ordinal scale of achievement, as defined in ISO/IEC 33020. They provide insight into the specific aspects of process capability required to support process improvement and capability determination.

4.3 Assessment Indicators

The PAM is based on the principle that the capability of a process can be assessed by demonstrating the achievement of process attributes on the basis of evidence related to assessment indicators.

There are two types of assessment indicators: process capability indicators, which apply to capability levels 1 to 5 and process performance indicators, which apply exclusively to capability level 1. These indicators are defined in Clause 4.3.2.

The process attributes in the capability dimension have a set of process capability indicators that provide an indication of the extent of achievement of the attribute in the instantiated process. These indicators concern significant activities, resources or results associated with the achievement of the attribute purpose by a process.

The process capability indicators are:

- Generic Practice (GP);
- Generic Resource (GR);
- Generic Input/Output (GIO).

As additional indicators for supporting the assessment of a process at Level 1, each process in the process dimension has a set of process performance indicators which is used to measure the degree of achievement of the process performance attribute for the process assessed.

The process performance indicators are:

- Base Practice (BP);
- Input/output (IO).

The performance of Base Practices (BPs) provides an indication of the extent of achievement of the process purpose and process outcomes. Input/Outputs (IOs) are either used or produced (or both), when performing the process.

The process performance and process capability indicators defined in the PAM represent types of objective evidence that might be found in an instantiation of a process and therefore could be used to judge achievement of capability.

Figure 4 shows how the assessment indicators are related to process performance and process capability.

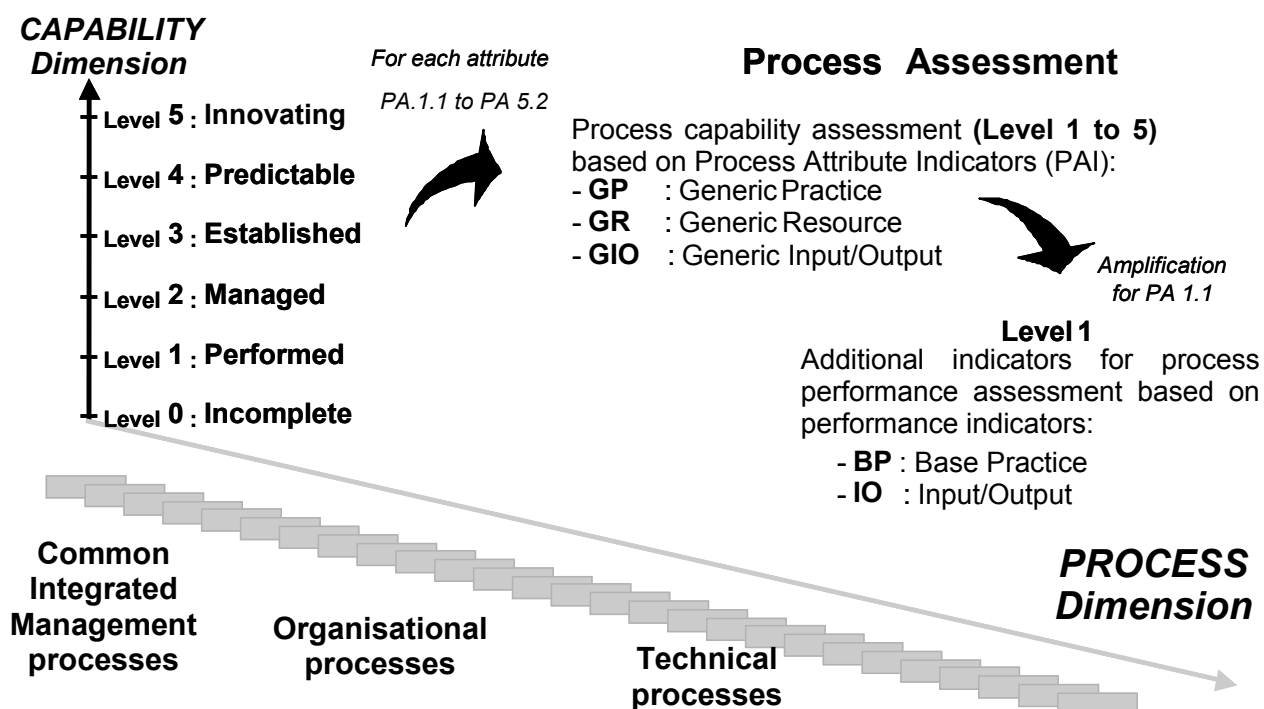


Figure 4 — Assessment indicators

4.3.1 Process Capability Indicators

The three types of process capability indicators related to levels 1 to 5 are identified in Figure 5. They are intended to be applicable to all processes.

All the process capability indicators relate to the process attributes defined in the capability dimension of the PAM. They represent the type of evidence that would support judgments of the extent to which the attributes are achieved. Evidence of their effective performance or existence supports the judgment of the degree of achievement of the attribute. The generic practices are the principal indicators of process capability.

The **Generic Practice (GP)** indicators are indicators of activities of a generic type and provide guidance on the implementation of the attribute's characteristics. They support the achievement of the process attribute and many of them concern management practices, i.e. practices that are established to support the process performance as it is characterized at level 1.

During the evaluation of process capability, the primary focus is on the performance of the generic practices. In general, performance of all generic practices is expected for full achievement of the process attribute.

The **Generic Resource (GR)** indicators are associated resources that may be used when performing the process in order to achieve the attribute. These resources may include human resources, tools, methods and infrastructure. The availability of a resource indicates the potential to fulfil the purpose of a specific attribute.

NOTE: The assessor should interpret the generic resources according to the process assessed; e.g. for PA2.1 resources (with identified objectives, responsibilities and authorities), an assessor would look for roles (with identified objectives, responsibilities and authorities) in primary and supporting processes, but for organizational processes would look for governance structures (e.g. mandated committees, positions) with identified objectives, responsibilities and authorities.

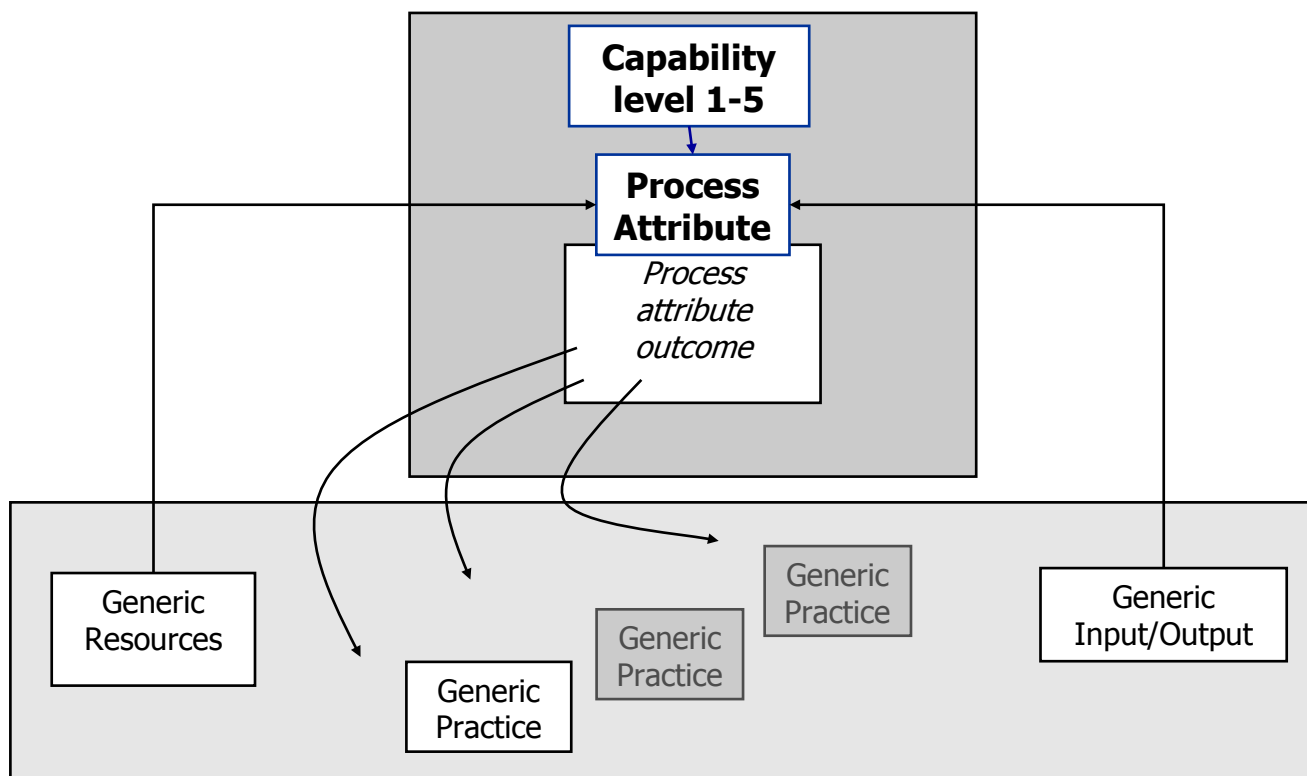


Figure 5 — Process capability indicators

The **Generic Input/Output (GIO)** indicators are sets of characteristics that would be expected to be evident in inputs/outputs of generic types as a result of achievement of an attribute. The generic inputs/outputs form the basis for the classification of the inputs/outputs defined as process performance indicators; they represent basic types of inputs/outputs from all types of processes.

These three types of indicators help to establish objective evidence of the extent of achievement of the specified process attribute.

Due to the fact that Level 1 capability of a process is only characterized by the measure of the extent to which the process purpose is achieved, the process performance attribute (PA.1.1) has a single generic practice indicator (GP.1.1.1). In order to support the assessment of PA.1.1 and to amplify the process performance achievement analysis, additional process performance indicators are defined in the PAM.

4.3.2 Process Performance Indicators

There are two types of process performance indicators: **Base Practice (BP)** indicators and **Input/Output (IO)** indicators. Process performance indicators relate to individual processes defined in the process dimension of the PAM and are chosen to explicitly address the achievement of the defined process outcomes.

Evidence of performance of the base practices, and the presence of inputs/outputs with their expected characteristics, provide objective evidence of the achievement of the process outcomes.

A base practice is an activity that addresses the purpose of a particular process. Consistently performing the base practices associated with a process will help the consistent achievement of its purpose. A coherent set of base practices is associated with each process in the process dimension. The base practices are described at an abstract level, identifying "what" should be done without specifying "how". Implementing the base practices of a process should achieve the basic outcomes that reflect the process purpose. Base practices represent only the first step in building process capability, but the base practices represent the unique, functional activities of the process, even if that performance is not systematic.

In this particular PAM the base practices have been used as a vehicle to link the outcomes of each process in the PRM with the requirements defined for that process in ISO/IEC 27001. This has been achieved using the following strategy:

- Singular requirements from ISO/IEC 27001 have been identified and assigned a unique identifier (process number plus sequential numbering within the sub-clause).
- Each process outcome has been linked to a single base practice.

This approach provides insight on how the singular requirements from ISO/IEC 27001 contribute to the achievement of the process purpose and outcomes. The performance of a process requires inputs and produces outputs that are identifiable and usable in achieving the purpose of the process. In this assessment model, each input/output has a defined set of example characteristics that may be used when reviewing the input/output to assess the effective performance of a process. Input/output characteristics may be used to identify the corresponding input/output produced/used by the assessed organization.

Clause 5 contains a complete description of the processes, including the base practices and the associated inputs and outputs.

Annex B contains a list of generic inputs/outputs together with their characteristics.

4.4 Measuring process capability

The process performance and process capability indicators in this model give examples of evidence that an assessor might obtain, or observe, in the performance of an assessment. The evidence obtained in the assessment, through observation of the implemented process, can be mapped onto the set of indicators to enable correlation between the implemented process and the processes defined in this assessment model. These indicators provide guidance for assessors in accumulating the necessary objective evidence to support judgments of capability. They are not mandatory.

An indicator is defined as an objective characteristic of a practice or input/output that supports performing a conformant assessment in accordance with the requirements of ISO/IEC 33004. The assessment indicators, and their relationship to process performance and process capability, are shown in Figure 6.

Observable (objective) evidence collected during an assessment is used to confirm the indicators (e.g., practices were performed). All such evidence comes either from the examination of inputs/outputs of the processes assessed, or from statements made by the performers and managers of the processes.

The existence of base practices, inputs/outputs, and input/output characteristics, provide evidence of the performance of the processes associated with them. Similarly, the existence of process capability indicators provides evidence of process capability.

The evidence obtained should be recorded in a form that clearly relates to an associated indicator, so that the support for the assessor's judgment can be readily confirmed or verified as required by ISO/IEC 33002.

The output from a process assessment is a set of process profiles, one for each process within the scope of the assessment. Each process profile consists of a set of the process attribute ratings for an assessed process. Each attribute rating represents a judgment by the assessor of the extent to which the attribute is achieved. To improve the reliability and repeatability of the assessment, the judgments of the assessor are based on a coherent set of recorded objective evidences.

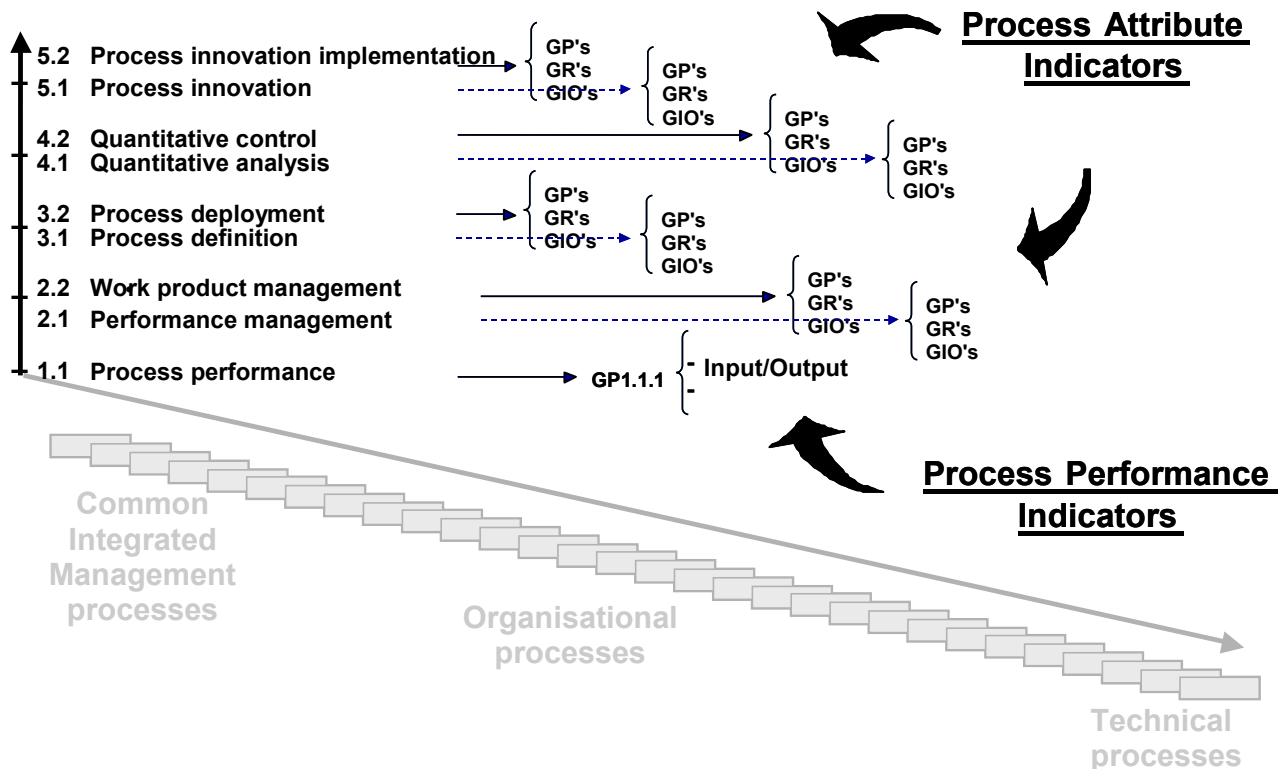


Figure 6 — Relationship between assessment indicators and process capability

5 The process dimension and process performance indicators (Level 1)

5.1 General

This clause defines the processes and the process performance indicators, also known as the process dimension, of the PAM. The processes in the process dimension can be directly mapped to the processes defined in the PRM.

The processes are classified into Process Groups which are shown in Figure 3. The process purposes, outcomes, the practices, the inputs and outputs of processes are included in this clause.

The individual processes are described in terms of process name, process purpose, and process outcomes as defined in ISO/IEC TS 33052:

- name: a short noun phrase that summarizes the scope of the process, identifying the principle concern of the process, and distinguishes it from other processes within the scope of the PRM;
- purpose: describes at a high level the overall objectives of performing the process;
- outcomes: an outcome is an observable result of the successful achievement of the process purpose. Outcomes are measurable, tangible, technical or business results that are achieved by a process. Outcomes are observable and assessable.

In addition, the process dimension of the PAM provides information in the form of:

- a set of base practices for the process needed to accomplish the process outcomes; a single base practice is explicitly associated with one or more process outcomes;

- b) a number of inputs/outputs associated with each process and their relationship to one or more of its outcomes by numbers in square brackets, (i.e. [n]);
- c) characteristics associated with each input/output.

The input/output identifiers and characteristics are contained in Annex B.

The base practices and the inputs/outputs constitute the set of indicators of process performance. The associated inputs/outputs listed in this clause may be used when reviewing potential inputs and outputs of an organization's process implementation. They provide objective guidance for potential inputs and outputs to look for, and objective evidence supporting the assessment of a particular process. A documented assessment process and assessor judgment is needed to ensure that process context (application domain, business purpose, development methodology, size of the organization, etc.) is explicitly considered when using this information. This list should not be considered as a checklist of what each organization must have but rather as an example and starting point for considering whether, given the context, the inputs/outputs are necessary and contributing to the intended purpose of the process.

NOTE Some outcomes are not linked to specific requirements of ISO/IEC 27001. These additional outcomes have been included in order to present a complete process so that the process purpose can be achieved. The complete list of affected base practices is shown in Annex C, Table C.2.

5.2 ORG.1 Asset management

Process ID	ORG.1
Name	Asset management
Purpose	The purpose of Asset Management is to establish and maintain the integrity of all identified product assets.
Outcomes	As a result of successful implementation of this process: 1. Items requiring asset management are identified. 2. Asset items are classified. 3. Assets are inventoried. 4. The status of assets is identified. 5. Changes to assets under management are controlled.
Base Practices	ORG.1.1 Identify asset items. Identify assets relevant in the lifecycle of information, and their importance. The lifecycle of information includes creation, processing, storage, transmission, deletion and destruction. The asset classification needs to be identified [Outcome 1] ORG.1.2 Classify assets. Identify asset classification. Note: Such a classification may include reference to the asset's legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. [Outcome 2] ORG.1.3 Inventory the assets. Assemble an inventory of the information security related assets. [Outcome 3] ORG.1.4 Identify asset status. The asset inventory is accurate, up to date, consistent and aligned with other inventories. [Outcome 4] ORG.1.5 Manage asset item changes. Manage changes to asset items. [Outcome 5]
Inputs	
06-01	Asset management procedure [Outcome 1,4]
02-01	Asset register [Outcome 1,4]
12-11	Information asset classification schema [Outcome 2]
03-05	Information asset control objective [Outcome 1]
03-06	Information asset management roles and responsibilities [Outcome 1]
02-05	Information asset register [Outcome 1,3,5]
06-07	Information labelling, handling and storage procedure [Outcome 1]
06-12	Removable media management procedure [Outcome 5]

Process ID	ORG.1
Name	Asset management
Outputs	
02-01	Asset register [Outcome 1]
08-33	Information asset classification record [Outcome 2]
02-05	Information asset register [Outcome 1,3,5]
08-52	Portable electronic media control log [Outcome 5]
08-55	Removable media disposition record [Outcome 5]
08-57	Return of assets confirmation record [Outcome 4]

5.3 TEC.01 Capacity management

Process ID	TEC.01
Name	Capacity management
Purpose	The purpose of Capacity Management is to ensure that the organization has capacity to meet current and future system performance requirements.
Outcomes	As a result of successful implementation of this process: 1. Current and future capacity and performance requirements are identified. 2. Capacity is provided to meet current capacity and performance requirements. 3. Capacity usage is monitored, analysed and performance is tuned. 4. Capacity is prepared to meet future capacity and performance needs.
Base Practices	TEC.01.1 Identify capacity requirements. Identify current and future capacity and performance requirements. [Outcome 1] TEC.01.2 Provide capacity. Provide capacity to meet current capacity and performance requirements. [Outcome 2] TEC.01.3 Monitor capacity usage. Monitor, analyse and performance tune capacity usage. [Outcome 3] TEC.01.4 Prepare future capacity. Prepare capacity to meet future capacity and performance needs. [Outcome 4]
Inputs	
12-01	Business continuity requirements [Outcome 1]
09-02	Capacity future needs assessment report [Outcome 4]
04-04	Capacity plan [Outcome 2,4]
12-02	Capacity requirements [Outcome 2,3,4]
09-03	Capacity usage analysis [Outcome 1,2,3,4]
02-02	Capacity usage data [Outcome 3]
12-05	Contractual requirements [Outcome 1]
12-16	New or changed services - system security requirements [Outcome 1]
12-22	Risk acceptance criteria [Outcome 1]
12-23	Service availability requirements [Outcome 1]
12-24	Statutory and regulatory requirements [Outcome 1]
Outputs	
09-02	Capacity future needs assessment report [Outcome 3]
04-04	Capacity plan [Outcome 2]
11-1	Capacity plan change request [Outcome 4]
12-02	Capacity requirements [Outcome 1]
09-03	Capacity usage analysis [Outcome 3]
02-02	Capacity usage data [Outcome 2]

5.4 TEC.02 Change management

Process ID	TEC.02
Name	Change management
Purpose	The purpose of Change Management is to provide the focus for all activities associated with changes associated with product, services, processes and systems used to produce a product or deliver a service.
Outcomes	As a result of successful implementation of this process: 1. Change requests are classified. 2. Change requests are analysed and assessed using defined criteria. 3. Changes are approved or rejected using defined criteria. 4. Changes are implemented, as appropriate.
Base Practices	TEC.02.1 Classify change requests. Classify change requests. [Outcome 1] TEC.02.2 Analyse change requests. Analyse and assess change requests using defined criteria. [Outcome 2] TEC.02.3 Approve or reject changes. Approve or reject change requests using defined criteria. [Outcome 3] TEC.02.4 Implement changes. Implement changes, as appropriate. [Outcome 4]
Inputs	
08-06	Change request approval record [Outcome 4]
09-04	Change request evaluation report [Outcome 3]
08-07	Change request record [Outcome 2]
08-69	Supplier services change request evaluation record [Outcome 3]
Outputs	
08-06	Change request approval record [Outcome 3]
09-04	Change request evaluation report [Outcome 2]
08-07	Change request record [Outcome 1]
04-05	Change schedule [Outcome 4]
02-03	Implemented changes log [Outcome 4]
08-69	Supplier services change request evaluation record [Outcome 2]

5.5 COM.01 Communication management

Process ID	COM.01
Name	Communication management
Purpose	The purpose of Communication Management is to produce timely and accurate information products to support effective communication and decision making.
Outcomes	As a result of successful implementation of this process: 1. Information content is defined in terms of identified communication needs and requirements. 2. Parties to communicate with are identified. 3. The party responsible for the communication is identified. 4. Events that require communication actions are identified. 5. The channel for the communication is selected. 6. Information products are communicated to interested parties.

Process ID	COM.01
Name	Communication management
Base Practices	COM.01.1 Define information content. Define information content in terms of identified communication needs and requirements. [Outcome 1] COM.01.2 Identify parties to communicate to. Identify parties to communicate with. [Outcome 2] COM.01.3 Identify party responsible for communication. Identify the party responsible for the communication. [Outcome 3] COM.01.4 Identify communication events. Identify the events that require communication actions. [Outcome 4] COM.01.5 Select communication channel. Select the channel for the communication. [Outcome 5] COM.01.6 Communicate information products. Communicate information products to interested parties. [Outcome 6]
Inputs	
12-03	Communication requirements [Outcome 6]
12-19	Process interface requirements [Outcome 6]
Outputs	
08-03	Audit result communication record [Outcome 6]
12-03	Communication requirements [Outcome 1,2,3,4,5]
09-10	ISMS Communication records [Outcome 6]
12-19	Process interface requirements [Outcome 2]

5.6 TEC.03 Configuration management

Process ID	TEC.03
Name	Configuration management
Purpose	The purpose of Configuration Management is to identify, control, record, track, report and verify all identified product/service components.
Outcomes	As a result of successful implementation of this process: 1. Items requiring configuration management are identified. 2. The status of configuration items and modifications is identified. 3. Changes to items under configuration management are controlled. 4. The integrity of systems, products/services and product/service components is assured. 5. The configuration of released items is controlled.
Base Practices	TEC.03.1 Identify configuration items. Identify items requiring configuration management. [Outcome 1] TEC.03.2 Identify configuration status. Record the status of configuration items and modifications. [Outcome 2] TEC.03.3 Manage changes to configuration items. Control changes to items under configuration management. [Outcome 3] TEC.03.4 Assure the integrity of configuration items. Assure the integrity of configuration item. [Outcome 4] TEC.03.5 Control the release of configuration items. Control the configuration of released items. [Outcome 5]
Inputs	
08-10	Configuration item change log [Outcome 4]
08-11	Configuration item record [Outcome 2]
09-06	Configuration item status report [Outcome 3]
03-35	Release notes [Outcome 5]
08-71	Test data change log [Outcome 4]

Process ID	TEC.03
Name	Configuration management
Outputs	
08-09	Configuration item archive [Outcome 5]
09-05	Configuration item audit report [Outcome 4]
08-10	Configuration item change log [Outcome 3]
08-11	Configuration item record [Outcome 1]
09-06	Configuration item status report [Outcome 2]
08-71	Test data change log [Outcome 3]

5.7 COM.02 Documentation management

Process ID	COM.02
Name	Documentation management
Purpose	The purpose of Document Management is to provide relevant, timely, complete, valid and, if required, confidential documented information to designated parties.
Outcomes	As a result of successful implementation of this process: 1. Documented information to be managed is identified. 2. The forms of documented information representation are defined. 3. The documented information content status is known. 4. Documented information is current, complete and valid. 5. Documented information is released according to defined criteria. 6. Documented information is available to designated parties. 7. Documented information is archived, or disposed of, as required.
Base Practices	COM.02.1 Identify documented information to be managed. Identify documented information of internal and external origin necessary for the operation of the information security management system. [Outcome 1] COM.02.2 The forms of documented information representation are defined.. Identify the forms of information to be stored in the repository. For example, this may include documents, records, audio content, video content, image content. [Outcome 2] COM.02.3 Identify documented information content status. The status of the documented information content refers to the timeliness of the information content. This includes the control of changes, for example, by using version control techniques. [Outcome 3] COM.02.4 Documented information is current, complete and valid.. The documented information contained in the repository is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). [Outcome 4] COM.02.5 The forms of documented information representation are defined.. Identify the forms of information to be stored in the repository. For example, this may include documents, records, audio content, video content, image content. [Outcome 5] COM.02.5 Release documented information according to defined criteria.. The documented information release status refers to those situations typically where authorisation is needed, such as in situations where: a) agreements are in force, b) policies and procedures are approved by management and their use in the organisation is thereby obligatory. [Outcome 5] COM.02.6 Make documented information available to designated parties.. Manage the distribution, access, retrieval and use of documented information towards interested parties. [Outcome 6] COM.02.7 Identify documented information to be managed. Identify documented information of internal and external origin necessary for the operation of the information security management system. [Outcome 7] COM.02.7 Archived, or disposed of documented information. Manage documented information, including records, through its lifecycle by addressing the following activities: - storage and preservation, including preservation of legibility; - retention and disposition. [Outcome 7] Note: Records should be protected in accordance with statutory, regulatory, contractual and business requirements.

Process ID	COM.02
Name	Documentation management
Inputs	
03-17	Management system strategy: documentation [Outcome 1,3,4,7]
Outputs	
08-01	Audit (ISMS) log [Outcome 1]
09-01	Audit result [Outcome 1]
06-02	Business continuity procedure [Outcome 1,3]
12-04	Confidentiality requirements [Outcome 1]
12-05	Contractual requirements [Outcome 1,3]
08-14	Corrective action record [Outcome 1]
08-22	Electronic transactions security violations log [Outcome 1]
06-05	Evidence collection and preservation procedure [Outcome 1]
08-32	Information archive log [Outcome 7]
03-05	Information asset control objective [Outcome 1]
08-34	Information disposition record [Outcome 7]
08-35	Information integrity verification record [Outcome 4]
12-13	Information item management requirements [Outcome 2,5]
12-14	Information management requirements [Outcome 2]
03-07	Information publication status [Outcome 6]
09-08	Information security incident report [Outcome 1]
03-08	Information security objectives [Outcome 1,3]
08-36	Information status record [Outcome 3]
05-06	Information system access policy [Outcome 1]
08-41	ISMS Measurement information results [Outcome 1]
08-42	ISMS Policy approval record [Outcome 5]
08-45	Management review record [Outcome 1]
05-08	Management system (ISMS) policy [Outcome 1,6]
03-16	Management system (ISMS) scope [Outcome 1]
03-17	Management system strategy: documentation [Outcome 1,7]
06-10	Operating Procedures [Outcome 1,6]
08-51	Personnel competency records [Outcome 1]
04-12	Product /service process lifecycle model [Outcome 1,3]
06-12	Removable media management procedure [Outcome 7]
08-56	Residual risk approval record [Outcome 5]
09-16	Risk analysis report [Outcome 1]
03-37	Risk assessment process description [Outcome 1]
08-60	Risk assessment review record [Outcome 1]
03-38	Risk identification [Outcome 1]
04-15	Risk treatment plan [Outcome 1]
03-39	Risk treatment process description [Outcome 1]
06-14	Security incident management procedure [Outcome 1]
12-24	Statutory and regulatory requirements [Outcome 1,3]
05-12	Supplier relationship information security policy [Outcome 1,5]

5.8 ORG.2 Equipment management

Process ID	ORG.2
Name	Equipment management
Purpose	The purpose of Equipment Management is to ensure integrity of the performance and behavior of equipment and associated software.
Outcomes	As a result of successful implementation of this process: 1. Equipment is sited to minimize risk of environmental or other damage. 2. Continuity in the provision of utilities and services to equipment is assured. 3. Equipment is maintained to ensure its continued availability and integrity. 4. Equipment used offsite is managed to ensure integrity of operation. 5. The integrity of information is assured when equipment is withdrawn from service. 6. Equipment relocation is controlled.
Base Practices	ORG.2.1 Site equipment. Site equipment to minimize risk of environmental or other damage. [Outcome 1] ORG.2.2 Assure continuity in service provision. Assure continuity in the provision of utilities and services to equipment. [Outcome 2] ORG.2.3 Maintain equipment. Maintain equipment to ensure its continued availability and integrity. [Outcome 3] ORG.2.4 Manage offsite equipment. Manage equipment used offsite to ensure integrity of operation. [Outcome 4] ORG.2.5 Assure information integrity. Assure the integrity of information when equipment is withdrawn from service. [Outcome 5] ORG.2.6 Control equipment relocation. Control equipment relocation. [Outcome 6]
Inputs	
12-08	Equipment environment requirements [Outcome 2,3,4,6]
Outputs	
08-08	Code validity confirmation record [Outcome 3]
08-19	Data removal verification record [Outcome 5]
12-08	Equipment environment requirements [Outcome 1,2]
12-09	Equipment maintenance requirements [Outcome 3]
06-04	Equipment offsite management procedure [Outcome 4]
08-29	Equipment removal approval record [Outcome 6]

5.9 ORG.3 Human resource employment management

Process ID	ORG.3
Name	Human resource employment management
Purpose	The purpose of Human Resource Employment Management is to prevent threats to information security by employees, before hiring, during employment and after termination of employment
Outcomes	As a result of successful implementation of this process: 1. Roles and responsibilities of employees, contractors and third party users are defined. 2. Prospective employees are screened in accordance with relevant laws, regulations and ethics, and in proportional to the business requirements and the perceived risks. 3. Prospective employees agree to the terms and conditions of their employment contract. 4. The terms and conditions of employment are applied. 5. Employees are equipped to apply relevant organizational policies and procedures, as relevant for their job function. 6. Disciplinary measures are applied to employees that have committed a breach of the agreed conditions of employment. 7. Responsibilities for performing employment termination or change of employment are defined and assigned. 8. Employees return all of the organization's assets in their possession upon termination of employment. 9. Employee access to information resources is removed upon termination of their employment.
Base Practices	ORG.3.1 Define roles and responsibilities of employees. Define roles and responsibilities of employees, contractors and third party users. [Outcome 1] ORG.3.2 Screen prospective employees. Screen prospective employees in accordance with relevant laws, regulations and ethics, and in proportional to the business requirements and the perceived risks. [Outcome 2] ORG.3.3 Confirm employee agreement. Confirm agreement of prospective employees to the terms and conditions of their employment contract. [Outcome 3] ORG.3.4 Apply employment terms and conditions. Apply the terms and conditions of employment are applied. [Outcome 4] ORG.3.5 Equip employees. Equip employees to apply relevant organizational policies and procedures, as relevant for their job function. [Outcome 5] ORG.3.6 Apply disciplinary measures. Apply disciplinary measures to employees that have committed a breach of the agreed conditions of employment. [Outcome 6] ORG.3.7 Manage employment termination. Define and assign responsibilities for performing employment termination or change of employment. [Outcome 7] ORG.3.8 Return of assets. On termination of employment, employees return all of the organization's assets in their possession. [Outcome 8] ORG.3.9 Remove employee access to information resources. Remove employee access to information resources upon termination of their employment. [Outcome 9]
Inputs	
01-2	Employee agreement [Outcome 3,4]
08-27	Employee terms and conditions approval record [Outcome 4,6,8]
08-28	Employment candidate screening review result [Outcome 3]
03-14	ISMS Roles and responsibilities [Outcome 2]
03-31	Process roles and responsibilities [Outcome 2]
08-61	Roles and responsibilities assignment record [Outcome 2]
03-41	Termination of employment roles and responsibilities [Outcome 9]

Process ID	ORG.3
Name	Human resource employment management
Outputs	
08-24	Employee access rights removal record [Outcome 9]
01-2	Employee agreement [Outcome 1]
08-25	Employee disciplinary action record [Outcome 6]
08-26	Employee security performance appraisal record [Outcome 4]
08-27	Employee terms and conditions approval record [Outcome 3]
08-28	Employment candidate screening review result [Outcome 2]
03-14	ISMS Roles and responsibilities [Outcome 1]
03-31	Process roles and responsibilities [Outcome 1]
08-57	Return of assets confirmation record [Outcome 8]
08-61	Roles and responsibilities assignment record [Outcome 1]
03-41	Termination of employment roles and responsibilities [Outcome 7]

5.10 COM.03 Human resource management

Process ID	COM.03
Name	Human resource management
Purpose	The purpose of Human Resource Management is to provide the organization with necessary competent human resources and to improve their competencies, in alignment with business needs.
Outcomes	As a result of successful implementation of this process: 1. The competencies required by the organization to produce products and services are identified. 2. Identified competency gaps are filled through training or recruitment. 3. Understanding of role and activities in achieving organisational objectives in product and service provision is demonstrated by each individual.
Base Practices	COM.03.1 Identify organisational competencies. Identify the competencies required by the organization. [Outcome 1] COM.03.2 Take action to acquire necessary competencies. Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc) [Outcome 2] COM.03.3 Evaluate competence of personnel. Evaluate the competence of the personnel [Outcome 3] COM.03.3 Take action to acquire necessary competencies. Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc) [Outcome 3] COM.03.3 Demonstrate awareness of role. Each individual demonstrates their understanding of their role and activities in achieving organisational objectives. [Outcome 3]
Inputs	
12-17	Organisational competence requirements [Outcome 2,3]
08-51	Personnel competency records [Outcome 3]
Outputs	
12-17	Organisational competence requirements [Outcome 1]
08-73	Training provision action log [Outcome 2]
08-74	Training record [Outcome 2,3]

5.11 COM.04 Improvement

Process ID	COM.04
Name	Improvement
Purpose	The purpose of Improvement is to continually improve the management system, its processes, and products.
Outcomes	As a result of successful implementation of this process: 1. Opportunities for improvement are identified. 2. Opportunities for improvement are evaluated against defined criteria. 3. Improvements are prioritised. 4. Improvements are implemented. 5. The effectiveness of implemented improvements is evaluated.
Base Practices	COM.04.1 Identify improvement opportunities. Identify opportunities for improvement. (NOTE: Opportunities for improvement could come from any kind of source such as internal audit, management review, non-conformity management.) [Outcome 1] COM.04.2 Evaluate improvement opportunities. Evaluate opportunities for improvement against defined criteria. Determine which ones have to be implemented, and how they have to be implemented [Outcome 2] COM.04.3 Prioritise improvements. Prioritise improvements, and decide when they have to be implemented. [Outcome 3] COM.04.4 Implement improvements. Perform activities that will improve the suitability, adequacy, performance, and effectiveness of the management system and its related processes and products. [Outcome 4] COM.04.5 Evaluate improvement effectiveness. Evaluate the effectiveness of implemented improvements. [Outcome 5]
Inputs	
11-3	Improvement opportunity approval request [Outcome 5]
12-10	Improvement opportunity evaluation criteria [Outcome 2,4]
08-30	Improvement opportunity evaluation result [Outcome 3,4]
08-31	Improvement opportunity record [Outcome 2,3]
05-05	Improvement policy [Outcome 2]
06-06	Improvement procedure [Outcome 2,3]
03-04	Improvement target [Outcome 4,5]
Outputs	
04-07	Improvement implementation schedule [Outcome 4]
03-03	Improvement opportunity [Outcome 1]
11-3	Improvement opportunity approval request [Outcome 3]
08-30	Improvement opportunity evaluation result [Outcome 2]
02-04	Improvement opportunity implementation log [Outcome 5]
08-31	Improvement opportunity record [Outcome 1]
03-04	Improvement target [Outcome 3]

5.12 TEC.04 Incident management

Process ID	TEC.04
Name	Incident management
Purpose	The purpose of Incident Management is to identify and resolve information security events and incidents within agreed service levels.
Outcomes	As a result of successful implementation of this process: 1. Incidents are identified. 2. Incidents are classified, prioritised and analysed. 3. Incidents are resolved and closed. 4. Incidents are reported and escalated according to agreed service levels.
Base Practices	TEC.04.1 Record incidents. Record and classify incidents. [Outcome 1] TEC.04.2 Analyse incidents. Prioritise and analyse incidents. [Outcome 2] TEC.04.3 Resolve incidents. Resolve and close incidents. [Outcome 3] TEC.04.4 Escalate incidents. Incidents are reported and escalated according to agreed service levels. [Outcome 4]
Inputs	
09-08	Information security incident report [Outcome 2]
08-62	Security incident disposition record [Outcome 4]
08-63	Security incident impact evaluation result [Outcome 3]
08-64	Security incident request record [Outcome 2]
Outputs	
09-08	Information security incident report [Outcome 1]
08-62	Security incident disposition record [Outcome 3,4]
08-63	Security incident impact evaluation result [Outcome 2]
08-64	Security incident request record [Outcome 1]

5.13 ORG.4 Infrastructure and work environment

Process ID	ORG.4
Name	Infrastructure and work environment
Purpose	The purpose of Infrastructure and Work Environment is to provide the enabling infrastructure and services to projects to support organization and project objectives throughout the life cycle.
Outcomes	As a result of successful implementation of this process: 1. The requirements for infrastructure and work environment to support processes are defined. 2. Access rights to the information resource are defined. 3. The infrastructure and work environment elements are identified and specified. 4. The infrastructure and work environment elements are acquired and commissioned. 5. The infrastructure and work environment is controlled and maintained. 6. Access to the information resource is controlled. 7. The information resource is protected from abuse.

Process ID	ORG.4
Name	Infrastructure and work environment
Base Practices	ORG.4.1 Define requirements. Define the requirements for infrastructure and work environment to support processes. [Outcome 1] ORG.4.2 Define access rights. Define access rights to the information resource. [Outcome 2] ORG.4.3 Specify elements. Identify and specify the infrastructure and work environment elements. [Outcome 3] ORG.4.4 Acquire elements. Acquire and commission the infrastructure and work environment elements. [Outcome 4] ORG.4.5 Maintain infrastructure and work environment. Control and maintain the infrastructure and work environment. [Outcome 5] ORG.4.6 Manage changes to configuration items. Control changes to items under configuration management. [Outcome 6] ORG.4.6 Control access. Control access to the information resource. [Outcome 6] ORG.4.7 Protect the information resource. Take steps, as appropriate, to protect the information resource from abuse. [Outcome 7]
Inputs	
05-02	Cryptographic controls usage policy [Outcome 7]
Outputs	
08-17	Cryptographic controls application review log [Outcome 7]
08-21	Electronic messaging scan log [Outcome 7]
08-22	Electronic transactions security violations log [Outcome 7]
12-08	Equipment environment requirements [Outcome 5]
12-12	Information infrastructure requirements [Outcome 1,2,7]
08-37	Information system access request approval record [Outcome 6]
09-09	Information system security compliance audit report [Outcome 7]
08-43	Logical access control log [Outcome 6]
09-13	Logical access system attack report [Outcome 7]
03-24	Management system strategy: privacy [Outcome 7]
08-65	Security vulnerability scan log [Outcome 7]
08-75	User access rights review record [Outcome 6]
12-26	User password system requirements [Outcome 6]
08-76	Work environment access control log [Outcome 5]
12-27	Work environment structure requirements [Outcome 1]

5.14 COM.05 Internal audit

Process ID	COM.05
Name	Internal audit
Purpose	The purpose of Internal Audit is to independently determine conformity of the management system, services, and processes to the requirements, policies, plans and agreements, as appropriate.
Outcomes	As a result of successful implementation of this process: 1. The scope and purpose of each audit is defined. 2. The objectivity and impartiality of the conduct of audits and selection of auditors are assured. 3. Conformity of selected services, products and processes with requirements, plans and agreements is determined.
Base Practices	COM.05.1 Define the criteria and scope of each audit. Define the audit criteria and the scope of each audit. [Outcome 1] COM.05.2 Select auditors . Select auditors to ensure objectivity and the impartiality of the audit process. [Outcome 2] COM.05.3 Conduct audits. Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process. [Outcome 3]

Process ID	COM.05
Name	Internal audit
Inputs	
08-02	Audit log [Outcome 3]
04-02	Audit plan [Outcome 1,2,3]
Outputs	
08-01	Audit (ISMS) log [Outcome 3]
08-02	Audit log [Outcome 2]
03-01	Audit objectives [Outcome 1]
04-02	Audit plan [Outcome 1]
08-04	Auditor list [Outcome 2]
09-07	Information security audit report [Outcome 3]
09-11	ISMS Implementation audit report [Outcome 3]
09-22	Supplier surveillance report [Outcome 3]

5.15 TOP.1 Leadership

Process ID	TOP.1
Name	Leadership
Purpose	The purpose of Leadership is to direct the organization in the achievement of its vision, mission, strategy and goals, through the definition and implementation of a management system, a management system policy, and management system objectives.
Outcomes	As a result of successful implementation of this process: 1. The context of the organization, including the expectations of its interested parties, are understood and analyzed. 2. The scope of management system activities is defined, taking the context of the organization into consideration. 3. The management system policy and objectives are defined. 4. The management system and operational process strategy is determined. 5. Commitment and leadership with respect to the management system is demonstrated.
Base Practices	TOP.1.1 Determine external and internal issues that are relevant to the organization and analyze their impacts . Determine external and internal issues that are relevant to the purpose of the assessed organization and that affect its ability to achieve the intended outcome(s) of its information security management system. (NOTE: Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009) [Outcome 1] TOP.1.1 Determine the interested parties and analyze their requirements . Determine the interested parties that are relevant to the information security management system and establish appropriate contacts with them. (NOTE: The requirements of interested parties may include legal and regulatory requirements and contractual obligations.) [Outcome 1] TOP.1.2 Determine the scope of the information security management system. Determine the boundaries and applicability of the information security management system, taking into consideration the context of the organization, the requirements of the interested parties and the interfaces and dependencies between activities performed by the organization, and those that are performed by other organization. [Outcome 2] TOP.1.3 Determine the scope of the information security management system. Determine the boundaries and applicability of the information security management system, taking into consideration the context of the organization, the requirements of the interested parties and the interfaces and dependencies between activities performed by the organization, and those that are performed by other organization. [Outcome 3] TOP.1.3 Define an information security policy . Define an information security policy that is appropriate to the purpose of the organization. [Outcome 3] TOP.1.3 Define information security objectives. Define information security objectives at relevant functions and levels, which are measurable, consistent with the information security policy, and which take into account applicable requirements and risk assessment and risk treatment results. [Outcome 3]

Process ID	TOP.1
Name	Leadership
	TOP.1.4 Determine process strategy. Determine the management system and operational process strategy. [Outcome 4] TOP.1.4 Integrate information security management system requirements into the business processes of the organization. Ensure the integration of the information security management system requirements into the business processes of the organization. [Outcome 4] TOP.1.5 Integrate information security management system requirements into the business processes of the organization. Ensure the integration of the information security management system requirements into the business processes of the organization. [Outcome 5]
Inputs	
03-16	Management system (ISMS) scope [Outcome 3]
03-19	Management system strategy: external and internal issues [Outcome 2]
03-21	Management system strategy: information security objectives [Outcome 4,5]
03-27	MS Interested parties [Outcome 2]
Outputs	
08-26	Employee security performance appraisal record [Outcome 5]
03-08	Information security objectives [Outcome 3]
05-08	Management system (ISMS) policy [Outcome 3]
03-16	Management system (ISMS) scope [Outcome 2]
03-17	Management system strategy: documentation [Outcome 4]
03-18	Management system strategy: Establish [Outcome 4]
03-19	Management system strategy: external and internal issues [Outcome 1]
03-20	Management system strategy: improvement [Outcome 4]
03-21	Management system strategy: information security objectives [Outcome 3,5]
03-22	Management system strategy: management commitment [Outcome 5]
03-23	Management system strategy: outsourcing [Outcome 4]
03-25	Management system strategy: processes [Outcome 4]
03-27	MS Interested parties [Outcome 1]
12-15	MS Interested parties MS expectations [Outcome 1]

5.16 COM.06 Management review

Process ID	COM.06
Name	Management review
Purpose	The purpose of Management Review is to assess the performance of the management system, to identify and make decisions regarding potential improvements.
Outcomes	As a result of successful implementation of this process: 1. The objectives of the review are established. 2. The status and performance of an activity or process are assessed in terms of the established objectives. 3. Risks, problems and opportunities for improvement are identified.

Process ID	COM.06
Name	Management review
Base Practices	COM.06.1 Identify the objectives for management system review. Objectives for reviewing the information security management system include:- the status of actions from previous management reviews into consideration. - consideration of changes in external and internal issues that are relevant to the information security management system- consider the information on the information security performance. - consider the feedback from interested parties. - consider the results of risk assessment and status of risk treatment plan. - consider the opportunities for continual improvement. [Outcome 1] COM.06.2 Assess status and performance of activities. Top management conduct reviews of the organization's information security management system to ensure its continuing suitability, adequacy and effectiveness. [Outcome 2] COM.06.3 Make decisions. Make decisions related to continual improvement opportunities and any need for changes to the information security management system. [Outcome 3] COM.06.3 Identify risks, problems and opportunities for improvement. Identify risks, problems, and opportunities related to improvement, and the need for changes to the information security management system. [Outcome 3]
Inputs	
03-15	Management review objectives [Outcome 2]
08-46	Management review result [Outcome 3]
Outputs	
08-44	Management review action log [Outcome 3]
03-15	Management review objectives [Outcome 1]
08-46	Management review result [Outcome 2]

5.17 COM.07 Non-conformity management

Process ID	COM.07
Name	Non-conformity management
Purpose	The purpose of the Non-conformity Management process is to resolve non-conformities and to eliminate their causes when appropriate.
Outcomes	As a result of successful implementation of this process: 1. Non-conformities are identified. 2. Non-conformities are resolved and closed. 3. The cause(s) of selected non-conformities is determined. 4. The need for action to eliminate the causes of non-conformities is evaluated. 5. A selected action proposal is implemented. 6. The effectiveness of changes to eliminate the non-conformities is confirmed.
Base Practices	COM.07.1 Identify non-conformities. Identify non-conformities. [Outcome 1] COM.07.2 Resolve and close non-conformities. Resolve and close non-conformities. [Outcome 2] COM.07.3 Determine cause of non-conformities. Determine the cause of selected non-conformities. [Outcome 3] COM.07.4 Determine the need for action. Determine the need for action to eliminate the causes of non-conformities. [Outcome 4] COM.07.5 Implement selected action proposals. Implement a selected action proposal. [Outcome 5] COM.07.6 Confirm change effectiveness. Confirm the effectiveness of changes to eliminate the non-conformities. [Outcome 6]
Inputs	
08-12	Correction action log [Outcome 3,6]
03-02	Corrective action change proposal [Outcome 5]
08-50	Non-conformity record [Outcome 2,3]

Process ID	COM.07
Name	Non-conformity management
Outputs	
08-12	Correction action log [Outcome 1,4]
03-02	Corrective action change proposal [Outcome 4]
08-13	Corrective action change proposal approval record [Outcome 5]
08-15	Corrective action request root cause analysis result [Outcome 3]
08-16	Corrective action verification record [Outcome 6]
08-49	Non-conformity disposition record [Outcome 2]
08-50	Non-conformity record [Outcome 1]

5.18 COM.09 Operational implementation and control

Process ID	COM.09
Name	Operational implementation and control
Purpose	The purpose of the Process Implementation and Control process is to deploy and control the execution and performance of operational and organisational processes.
Outcomes	As a result of successful implementation of this process: 1. The required roles, responsibilities and authorities are allocated. 2. The required resources are allocated and applied. 3. Actions required to achieve the management system objectives are implemented. 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed. 5. Deviations from planned arrangements are corrected when targets are not achieved. 6. Data is collected and analysed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the processes.
Base Practices	COM.09.1 Allocate roles, responsibilities and authorities. Allocate the required roles, responsibilities and authorities. [Outcome 1] COM.09.2 Allocate resources. Allocate and apply the required resources. [Outcome 2] COM.09.3 Archived, or disposed of documented information. Manage documented information, including records, through its lifecycle by addressing the following activities: - storage and preservation, including preservation of legibility; - retention and disposition. [Outcome 3] COM.09.3 Identify process needs and requirements. Identify process needs and requirements. [Outcome 3] COM.09.3 Perform process activities. Implement actions taken to achieve the management system objectives. [Outcome 3] COM.09.4 Review process activities. Review suitability and effectiveness of the actions required to achieve the management system objectives. [Outcome 4] COM.09.5 Correct deviations. Correct deviations from planned arrangements when targets are not achieved. [Outcome 5] COM.09.6 Collect and analyse data. Collect and analyse data as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the processes. [Outcome 6]
Inputs	

Process ID	COM.09
Name	Operational implementation and control
Outputs	
08-23	Electronic transactions security violations log review record [Outcome 4]
09-08	Information security incident report [Outcome 3]
08-39	ISMS Implementation log [Outcome 3]
08-40	ISMS Implementation review record [Outcome 4]
08-47	MS Resources provision record [Outcome 2]
08-51	Personnel competency records [Outcome 4]
11-4	Process change request [Outcome 5]
08-53	Process change request review record [Outcome 4]
08-54	Process change review record [Outcome 4]
06-12	Removable media management procedure [Outcome 3]
08-59	Risk assessment process effectiveness evaluation result [Outcome 4]
08-61	Roles and responsibilities assignment record [Outcome 1]
08-70	System activity log review record [Outcome 4]
08-72	Training effectiveness evaluation result [Outcome 4]

5.19 COM.08 Operational planning

Process ID	COM.08
Name	Operational planning
Purpose	The purpose of Operational Planning is to define the characteristics of all operational and organisational processes, and to plan their execution.
Outcomes	As a result of successful implementation of this process: 1. Process needs and requirements are identified. 2. Process input and output products are determined. 3. The set of activities that transform the inputs into outputs is determined. 4. The sequence and interaction of the process with other processes is determined. 5. The required competencies and roles for performing the process are identified. 6. The required resources for performing the process are identified. 7. Methods for monitoring the effectiveness and suitability of the process are determined. 8. Plans for the deployment of the process are developed.

Process ID	COM.08
Name	Operational planning
Base Practices	COM.08.1 Identify process needs and requirements. Identify process needs and requirements. [Outcome 1] COM.08.2 Determine process input and output products. Determine process input and output products. [Outcome 2] COM.08.3 Identify documented information to be managed. Identify documented information of internal and external origin necessary for the operation of the information security management system. [Outcome 3] COM.08.3 Identify process needs and requirements. Identify process needs and requirements. [Outcome 3] COM.08.3 Determine the set of activities that transform the inputs into outputs. Determine the set of activities that transform the inputs into outputs. [Outcome 3] COM.08.4 Determine the sequence and interaction of the process with other processes. Determine the sequence and interaction of the process with other processes. [Outcome 4] COM.08.5 Identify the required competencies and roles for performing the process. Identify the required competencies and roles for performing the process. [Outcome 5] COM.08.6 Identify the required resources for performing the process. Determine what resources will be required by the information security management system to achieve its information security objectives. Make projections of future capacity requirements to ensure the required system performance. [Outcome 6] COM.08.7 Determine the methods for monitoring the effectiveness and suitability of the process. Determine the methods for monitoring the effectiveness and suitability of the process. [Outcome 7] COM.08.8 Plan the deployment of the process. Plan the processes will be deployed in order to achieve the information security objectives. [Outcome 8]
Inputs	
05-08	Management system (ISMS) policy [Outcome 5]
03-36	Risk and opportunity identification criteria [Outcome 8]
Outputs	
06-01	Asset management procedure [Outcome 3]
04-01	Audit (ISMS) schedule [Outcome 8]
04-03	Audit programme plan [Outcome 8]
06-02	Business continuity procedure [Outcome 1]
01-1	Business information exchange agreement [Outcome 1]
06-03	Change control procedure [Outcome 1]
05-01	Clear desk policy [Outcome 1]
12-04	Confidentiality requirements [Outcome 1]
12-06	Criteria for performing risk assessments [Outcome 1]
05-02	Cryptographic controls usage policy [Outcome 1]
05-03	Cryptographic key protection and usage policy [Outcome 1]
05-04	Data backup policy [Outcome 1]
04-06	Data backup test schedule [Outcome 8]
06-05	Evidence collection and preservation procedure [Outcome 3]
12-10	Improvement opportunity evaluation criteria [Outcome 2]
05-05	Improvement policy [Outcome 1]
06-06	Improvement procedure [Outcome 3]
12-11	Information asset classification schema [Outcome 1]
03-05	Information asset control objective [Outcome 1]
03-06	Information asset management roles and responsibilities [Outcome 5]
06-07	Information labelling, handling and storage procedure [Outcome 3]
04-08	Information security control verification schedule [Outcome 8]
06-08	Information security incident response procedure [Outcome 3]
05-06	Information system access policy [Outcome 1]
04-09	Information system compliance review schedule [Outcome 8]
05-07	Information transfer policy [Outcome 1]
06-09	Information transfer procedure [Outcome 3]

Process ID	COM.08
Name	Operational planning
03-09	ISMS Measurement information analysis roles and responsibilities [Outcome 5]
03-10	ISMS Measurement information gathering events [Outcome 8]
03-11	ISMS Measurement information gathering roles and responsibilities [Outcome 5]
04-10	ISMS Policy review schedule [Outcome 8]
03-14	ISMS Roles and responsibilities [Outcome 5]
04-11	Management review schedule [Outcome 8]
03-26	Management system strategy: roles and responsibilities [Outcome 5]
05-09	Mobile device policy [Outcome 1]
06-10	Operating Procedures [Outcome 3]
12-17	Organisational competence requirements [Outcome 5]
12-18	Process criteria [Outcome 1]
03-28	Process measures [Outcome 7]
03-29	Process objectives [Outcome 1]
03-30	Process resource needs [Outcome 6]
03-31	Process roles and responsibilities [Outcome 5]
03-32	Process schedule [Outcome 8]
04-12	Product /service process lifecycle model [Outcome 1]
06-11	Protection of intellectual property rights procedure [Outcome 3]
06-12	Removable media management procedure [Outcome 3]
04-13	Resources budget [Outcome 6]
12-22	Risk acceptance criteria [Outcome 1]
03-36	Risk and opportunity identification criteria [Outcome 1]
08-58	Risk assessment action schedule [Outcome 8]
03-37	Risk assessment process description [Outcome 1]
04-14	Risk management plan [Outcome 8]
03-39	Risk treatment process description [Outcome 1]
06-13	Secure area operating procedure [Outcome 3]
05-10	Secure development policy [Outcome 1]
06-14	Security incident management procedure [Outcome 3]
04-16	Security policies compliance review schedule [Outcome 8]
05-11	Software installation by users policy [Outcome 1]
06-15	Software installation procedure [Outcome 3]
05-12	Supplier relationship information security policy [Outcome 1]
05-13	Teleworking policy [Outcome 1]
06-16	Teleworking procedure [Outcome 3]
04-19	User access rights review schedule [Outcome 8]
06-17	User authentication information control procedure [Outcome 1]

5.20 COM.10 Performance evaluation

Process ID	COM.10
Name	Performance evaluation
Purpose	The purpose of Performance Evaluation is to collect and analyze data that will be used to evaluate the performance of the management system and the business processes in terms of the defined objectives.
Outcomes	As a result of successful implementation of this process: 1. Performance monitoring and measurement needs are defined. 2. Performance measures, derived from the performance measurement needs, are identified. 3. Performance measurement methods, supportive of the performance measures, are identified. 4. Data is collected using the identified performance measurement methods. 5. The collected performance data is analyzed.

Process ID	COM.10
Name	Performance evaluation
Base Practices	COM.10.1 Determine what needs to be monitored and measured. Determine what needs to be monitored and measured, including information security processes and controls. [Outcome 1] COM.10.2 Determine appropriate performance measures. Determine appropriate performance measures that support the performance measurement needs. [Outcome 2] COM.10.3 Determine the appropriate methods for monitoring, measurement, analysis and evaluation. Determine the appropriate methods for monitoring, measurement, analysis and evaluation as well as how the results will be evaluated. [Outcome 3] COM.10.4 Monitor and measure the information security performance and the information security management system. Collect and verify data on the information security performance of the organization, as well as on the information security management system. [Outcome 4] COM.10.5 Analyse the collected data. Analyze the collected data in order to evaluate the information security performance, the effectiveness of the information security management system as well as the effectiveness of any action taken within the scope of the information security management system. [Outcome 5]
Inputs	
03-10	ISMS Measurement information gathering events [Outcome 2]
03-12	ISMS Measurement information needs [Outcome 2]
03-13	ISMS Measurement methods [Outcome 4]
02-06	ISMS Performance measurement data [Outcome 5]
Outputs	
09-08	Information security incident report [Outcome 5]
09-12	ISMS measurement information analysis report [Outcome 5]
03-12	ISMS Measurement information needs [Outcome 1]
03-13	ISMS Measurement methods [Outcome 3]
02-06	ISMS Performance measurement data [Outcome 4]
03-33	Project/service measures [Outcome 2]

5.21 TEC.05 Product/service release

Process ID	TEC.05
Name	Product/service release
Purpose	The purpose of Product/service Release is to control the availability of a product/service to the intended customer.
Outcomes	As a result of successful implementation of this process: 1. The contents of the release are determined. 2. [Release and acceptance criteria are determined.] 3. The release is assembled from the product/service/system elements. 4. Tests are defined for the release. 5. The release is tested in accordance with defined criteria. 6. Products/services/systems are released to the intended customer according to defined criteria.
Base Practices	TEC.05.1 Determine release content. Determine the contents of the release. [Outcome 1] TEC.05.3 Assemble the release. Assemble the release from the product/service/system components. [Outcome 3] TEC.05.4 Define tests. Define tests for the release. [Outcome 4] TEC.05.5 Test the release. Test the release in accordance with defined criteria. [Outcome 5] TEC.05.6 Release product/service/system. Release products/services/systems to the intended customer according to defined criteria. [Outcome 6]

Process ID	TEC.05
Name	Product/service release
Inputs	
08-38	Information system changes security impact evaluation result [Outcome 6]
12-20	Release acceptance test case [Outcome 5]
03-34	Release acceptance test criteria [Outcome 4]
09-15	Release acceptance test report [Outcome 6]
07-1	Release package [Outcome 5,6]
12-21	Release requirements [Outcome 2,3]
12-25	System acceptance criteria [Outcome 4,5]
Outputs	
08-38	Information system changes security impact evaluation result [Outcome 5]
12-20	Release acceptance test case [Outcome 4]
03-34	Release acceptance test criteria [Outcome 2]
09-15	Release acceptance test report [Outcome 5]
02-07	Release log [Outcome 6]
03-35	Release notes [Outcome 6]
07-1	Release package [Outcome 3]
12-21	Release requirements [Outcome 1]
12-25	System acceptance criteria [Outcome 2]

5.22 TEC.08 Product/Service/System requirements

Process ID	TEC.08
Name	Product/Service/System requirements
Purpose	The purpose of Product/Service/System Requirements is to establish and agree to the requirements, for products/services and systems.
Outcomes	As a result of successful implementation of this process: 1. The required characteristics and context of use of products/services/systems are identified. 2. The constraints for a product/service/system solution are defined. 3. The requirements for the product/service/system are defined. 4. The requirements for validating the product/service/system are defined.
Base Practices	TEC.08.1 Identify required service characteristics. Identify the required characteristics and context of use of new or changed services. [Outcome 1] TEC.08.2 Define service solution constraints. Define the constraints for a service solution. [Outcome 2] TEC.08.3 Define service requirements. Define the requirements for the new or changed service. [Outcome 3] TEC.08.4 Define service validation requirements. Define the requirements for validating the new or changed service. [Outcome 4]
Inputs	
08-38	Information system changes security impact evaluation result [Outcome 4]
09-14	New or changed service evaluation report [Outcome 3]
08-48	New or changed service request record [Outcome 2,3]
12-16	New or changed services - system security requirements [Outcome 4]

Process ID	TEC.08
Name	Product/Service/System requirements
Outputs	
12-05	Contractual requirements [Outcome 3]
08-38	Information system changes security impact evaluation result [Outcome 3]
09-14	New or changed service evaluation report [Outcome 2]
08-48	New or changed service request record [Outcome 1]
12-16	New or changed services - system security requirements [Outcome 3]
12-24	Statutory and regulatory requirements [Outcome 3]
12-25	System acceptance criteria [Outcome 4]

5.23 COM.11 Risk and opportunity management

Process ID	COM.11
Name	Risk and opportunity management
Purpose	The purpose of Risk and Opportunity Management is to identify, analyse, evaluate, treat and monitor risks.
Outcomes	As a result of successful implementation of this process: 1. Risks are identified. 2. Identified risks are analysed. 3. Risks are evaluated against defined criteria. 4. Risks are selected for treatment. 5. Selected risks are treated.
Base Practices	COM.11.1 Identify risks. Identify the information security risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system. Identify the risk owners for each information security risk identified [Outcome 1] COM.11.2 Assess risks. Assess risks: - the potential consequences that would result if the information security risks identified were to materialize; - the realistic likelihood of the occurrence of the information security risks identified; For each identified information security risk, determine its level of risk, allowing comparisons with results of previous risk assessments. [Outcome 2] COM.11.3 Evaluate risks. Compare the results of information security risk assessment with the criteria established, and prioritize the analyzed risks for risk treatment, according to the defined information security risk assessment process. [Outcome 3] COM.11.4 Select risks for treatment. For each identified information security risk select the appropriate information security risk treatment option, taking into account of the information security risk assessment results. [Outcome 4] COM.11.5 Treat risks. Implement and track the actions needed to address the information security risks, in accordance with the content of the information security risk treatment plan. [Outcome 5]
Inputs	
12-06	Criteria for performing risk assessments [Outcome 1]
12-22	Risk acceptance criteria [Outcome 3]
09-16	Risk analysis report [Outcome 3]
08-60	Risk assessment review record [Outcome 4]
03-38	Risk identification [Outcome 2]
04-15	Risk treatment plan [Outcome 5]
Outputs	
08-39	ISMS Implementation log [Outcome 5]
09-16	Risk analysis report [Outcome 2]
08-60	Risk assessment review record [Outcome 3]
03-38	Risk identification [Outcome 1]
04-15	Risk treatment plan [Outcome 4]

5.24 TEC.06 Service availability management

Process ID	TEC.06
Name	Service availability management
Purpose	The purpose of the Service Availability Management is to ensure that agreed service levels will be met in foreseeable circumstances.
Outcomes	As a result of successful implementation of this process: 1. Service availability requirements are identified. 2. A service availability plan is developed using the service availability requirements. 3. Service availability is tested against the service availability requirements. 4. Service availability is monitored. 5. Causes of unplanned service non-availability are identified and analysed. 6. Corrective actions are taken to address identified causes for unplanned non-availability.
Base Practices	TEC.06.1 Identify availability requirements. service availability requirements are identified. [Outcome 1] TEC.06.2 Develop availability plan. Develop a service availability plan using the service availability requirements. [Outcome 2] TEC.06.3 Test service availability. Test service availability against the service availability requirements. [Outcome 3] TEC.06.4 Monitor service availability. Monitor service availability. [Outcome 4] TEC.06.5 Identify causes of unplanned service non-availability. Identify and analyse causes of unplanned service non-availability. [Outcome 5] TEC.06.6 Take correction action. Take corrective actions to address identified causes for unplanned non-availability. [Outcome 6]
Inputs	
09-17	Service availability analysis report [Outcome 6]
02-08	Service availability log [Outcome 5]
04-17	Service availability plan [Outcome 3]
12-23	Service availability requirements [Outcome 2]
Outputs	
03-03	Improvement opportunity [Outcome 6]
09-17	Service availability analysis report [Outcome 5]
02-08	Service availability log [Outcome 4]
04-17	Service availability plan [Outcome 2]
11-5	Service availability plan change request [Outcome 6]
09-18	Service availability plan test report [Outcome 3]
08-66	Service availability plan test result review record [Outcome 3]
12-23	Service availability requirements [Outcome 1]

5.25 TEC.07 Service continuity management

Process ID	TEC.07
Name	Service continuity management
Purpose	The purpose of Service Continuity Management is to ensure that agreed service continuity commitments can be met within agreed targets and disrupted services can be resumed.
Outcomes	As a result of successful implementation of this process: 1. Service continuity requirements are identified. 2. Service continuity is planned to meet the service continuity requirements. 3. Service continuity is evaluated against the service continuity requirements. 4. Changes in service continuity requirements are monitored. 5. Service continuity is ensured by activating the continuity plan in cases of major loss of service.
Base Practices	TEC.07.1 Identify service continuity requirements. Identify service continuity requirements. [Outcome 1] TEC.07.2 Plan service continuity. Develop a service continuity plan using the service continuity requirements. [Outcome 2] TEC.07.3 Test service continuity. Test service continuity against the service continuity requirements. [Outcome 3] TEC.07.4 Monitor changes in service continuity requirements. Monitor changes in service continuity requirements. [Outcome 4] TEC.07.5 Monitor change in service continuity requirements. Ensure that service continuity planning takes account of changes to service continuity requirements. [Outcome 5]
Inputs	
08-05	Business continuity plan test result [Outcome 2]
12-01	Business continuity requirements [Outcome 4]
04-18	Service continuity plan [Outcome 3,5]
09-19	Service continuity plan test report [Outcome 4]
09-20	Service continuity plan test result finding report [Outcome 4]
Outputs	
08-05	Business continuity plan test result [Outcome 3]
12-01	Business continuity requirements [Outcome 1]
04-18	Service continuity plan [Outcome 2]
11-6	Service continuity plan change request [Outcome 4]
09-19	Service continuity plan test report [Outcome 3]
09-20	Service continuity plan test result finding report [Outcome 3]

5.26 ORG.5 Supplier management

Process ID	ORG.5
Name	Supplier management
Purpose	The purpose of Supplier Management is to ensure supplier products/services/systems are managed and integrated into the delivered products/services/systems to meet the agreed requirements.
Outcomes	As a result of successful implementation of this process: 1. Suppliers are identified. 2. Products/services to be provided are negotiated and defined with each supplier. 3. Roles and relationships between suppliers are determined. 4. The capability of subcontracted suppliers to meet obligations is confirmed. 5. Supplier obligations to meet requirements are monitored. 6. Supplier performance against agreed criteria is monitored.

Process ID	ORG.5
Name	Supplier management
Base Practices	ORG.5.1 identify suppliers to service provision. identify suppliers to product/service/system provision. [Outcome 1] ORG.5.2 Negotiate products/services/systems. Negotiate and define products/services/systems to be provided with each supplier. [Outcome 2] ORG.5.3 Determine supplier roles. Determine supplier roles and relationships. [Outcome 3] ORG.5.4 Confirm supplier capability. Confirm the capability of subcontracted suppliers to meet obligations. [Outcome 4] ORG.5.5 Monitor supplier obligations. Monitor supplier obligations to meet service requirements. [Outcome 5] ORG.5.6 Monitor supplier performance. Monitor supplier performance against agreed criteria. [Outcome 6]
Inputs	
01-1	Business information exchange agreement [Outcome 5]
03-30	Process resource needs [Outcome 1,2]
01-3	Supplier agreement [Outcome 3,4,5,6]
02-09	Supplier performance data [Outcome 6]
Outputs	
01-1	Business information exchange agreement [Outcome 2]
03-40	Sub-contracted supplier roles and responsibilities [Outcome 3]
01-3	Supplier agreement [Outcome 2]
08-67	Supplier agreement review record [Outcome 5]
08-68	Supplier capability assessment record [Outcome 4]
02-09	Supplier performance data [Outcome 5]
09-21	Supplier performance evaluation report [Outcome 6]
02-10	Supplier role assignments list [Outcome 1]
08-69	Supplier services change request evaluation record [Outcome 2]

5.27 TEC.09 Technical data preservation and recovery

Process ID	TEC.09
Name	Technical data preservation and recovery
Purpose	The purpose of Technical Data Preservation and Recovery is to backup and preserve data, and to recover data from archive media.
Outcomes	As a result of successful implementation of this process: 1. Data backup requirements are identified. 2. Data restore requirements are identified. 3. Data backups are executed. 4. Data restoration is performed. 5. Backup media are preserved under controlled conditions. 6. Restored data is verified.
Base Practices	TEC.09.1 Select data backup media. Select data backup media. [Outcome 1] TEC.09.2 Identify data restore requirements. Identify data restore requirements. [Outcome 2] TEC.09.3 Execute data backups. Execute data backups. [Outcome 3] TEC.09.4 Perform data restore. Perform data restore. [Outcome 4] TEC.09.5 Preserve backup media. Preserve backup media. [Outcome 5] TEC.09.6 Verify restored data. Verify restored data. [Outcome 6]

Process ID	TEC.09
Name	Technical data preservation and recovery
Inputs	
12-01	Business continuity requirements [Outcome 1]
12-07	Data backup requirements [Outcome 3]
11-2	Data recovery request [Outcome 4]
08-20	Data restore log [Outcome 6]
04-18	Service continuity plan [Outcome 1]
Outputs	
08-18	Data backup log [Outcome 3]
12-07	Data backup requirements [Outcome 1]
11-2	Data recovery request [Outcome 2]
08-20	Data restore log [Outcome 4]

6 Process capability indicators

6.1 Introduction

This clause presents the process capability indicators related to the process capability attributes (process attribute, PA) associated with capability levels 1 to 5 defined in the capability dimension of the process assessment model. Process capability indicators are the means of achieving the capabilities addressed by the considered process capability attributes. Evidence of process capability indicators supports the judgment of the degree of achievement of the process capability attribute. Clause 5 describes the assessment indicators for process performance which is characterized by Level 1 process capability.

6.2 Process capability levels and process attributes

The capability process quality characteristic of the process assessment model consists of capability levels as defined in International Standard ISO/IEC 33020. Process capability is defined on a six point ordinal scale that enables capability to be assessed from the bottom of the scale, **Incomplete**, through to the top end of the scale, **Innovating**. The scale represents increasing capability of the implemented process, from failing to achieve the process purpose through to continually improved and responding to strategic organizational change.

NOTE 1: In the next paragraphs, ISO/IEC 33020 process attribute definitions and attribute outcomes are identified with *italic font*.

NOTE 2: Following each generic resource and generic work product is '[PA.x.y outcome]'. This refers to process attribute x.y outcome n which is satisfied by this indicator.

6.2.1 Process capability Level 0: Incomplete process

The process is not implemented, or fails to achieve its process purpose.

At this level there is little or no evidence of any systematic achievement of the process purpose.

6.2.2 Process capability Level 1: Performed process

The implemented process achieves its process purpose. The following process attribute demonstrates the achievement of this level.

6.2.2.1 PA.1.1 Process performance process attribute

The process performance process attribute is a measure of the extent to which the process purpose is achieved. As a result of full achievement of this process attribute:

- a) *The process achieves its defined process outcomes.*

6.2.2.1.1 Generic practice for PA.1.1

PA.1.1.GP1 Achieve the process outcomes

Achieve the intent of the base practices.

Produce work products that evidence the process outcomes.

NOTE: The assessment of a performed process is based on process performance indicators, which are defined in Clause 5 of this document.

6.2.2.1.2 Generic resources for PA.1.1

- Resources are used to perform the intent of process specific base practices. [PA.1.1 outcome a]

6.2.2.1.3 Generic work products for PA.1.1

7.0 Product [PA.1.1 outcome a]

- Work products exist that provide evidence of the achievement of the process outcomes.

6.2.3 Process capability Level 2: Managed process

The previously described *Performed process* is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

The following process attributes, together with the previously defined process attribute, demonstrate the achievement of this level:

6.2.3.1 PA.2.1 Performance management process attribute

The performance management process attribute is a measure of the extent to which the performance of the process is managed. As a result of full achievement of this process attribute:

- b) *Objectives for the performance of the process are identified;*
- c) *Performance of the process is planned;*
- d) *Performance of the process is monitored;*
- e) *Performance of the process is adjusted to meet plans;*
- f) *Responsibilities and authorities for performing the process are defined, assigned and communicated;*
- g) *Personnel performing the process are prepared for executing their responsibilities;*
- h) *Resources and information necessary for performing the process are identified, made available, allocated and used;*
- i) *Interfaces between the involved parties are managed to ensure both effective communication and clear assignment of responsibility.*

6.2.3.1.1 Generic practices for PA.2.1

PA.2.1.GP1 Identify the objectives for the performance of the process.

NOTE: Performance objectives may include – (1) quality of the artefacts produced, (2) process cycle time or frequency, (3) resource usage and (4) boundaries of the process.

Performance objectives are identified based on process requirements.

The scope of the process performance is defined.

Assumptions and constraints are considered when identifying the performance objectives.

PA.2.1.GP2 Plan the performance of the process to fulfil the identified objectives.

Plan(s) for the performance of the process are developed. The process performance cycle is defined.

Key milestones for the performance of the process are established.

Estimates for process performance attributes are determined and maintained.

Process activities and tasks are defined.

Schedule is defined and aligned with the approach to performing the process.

Process work product reviews are planned.

PA.2.1.GP3 Monitor the performance of the process against the plans.

The process is performed according to the plan(s).

Process performance is monitored to ensure that planned results are achieved and to identify possible deviations.

PA.2.1.GP4 Adjust the performance of the process.

Process performance issues are identified.

Appropriate actions are taken when planned results and objectives are not achieved.

The plan(s) are adjusted, as necessary.

Rescheduling is performed as necessary.

PA.2.1.GP5 Define responsibilities and authorities for performing the process.

Responsibilities, commitments and authorities to perform the process are defined, assigned and communicated.

Responsibilities and authorities to verify process work products are defined and assigned.

The needs for process performance experience, knowledge and skills are defined.

PA.2.1.GP6 Prepare those performing the process to execute their responsibilities.

Competencies for management and execution of the process are ensured by training or work-based learning.

Required competencies are identified based on the responsibilities.

PA.2.1.GP7 Identify and make available resources to perform the process according to plan.

The human and infrastructure resources necessary for performing the process are identified, made available, allocated and used.

The information necessary to perform the process is identified and made available.

PA.2.1.GP8 Manage the interfaces between involved parties.

The individuals and groups involved in the process performance are determined.

Responsibilities of the involved parties are assigned.

Interfaces between the involved parties are managed.

Communication is assured between the involved parties.

Communication between the involved parties is effective.

6.2.3.1.2 Generic resources for PA.2.1

- Human resources with identified objectives, responsibilities and authorities; [PA.2.1 outcome a, e, f, g, h]
- Facilities and infrastructure resources; [PA.2.1 outcome a, e, g, h]
- Project planning, management and control tools, including time and cost reporting; [PA.2.1 outcome b, c, d]
- Workflow management system; [PA.2.1 outcome e, h]
- Email and/or other communication mechanisms; [PA.2.1 outcome e, h]
- Information and/or experience repository; [PA.2.1 outcome b, c, f, g]
- Problem and issue management mechanisms. [PA.2.1 outcome d]

6.2.3.1.3 Generic work products for PA.2.1

4.0 Plan [PA 2.1 outcome a, b, c, d, e, f, g, h]

- Defines objectives to perform the process.
- Describes assumptions and constraints considered in defining the objectives.
- Includes milestones and timetable to produce the work products of the process.
- Identifies tasks, resources, responsibilities and infrastructure needed to perform the process.
- Considers risks related to fulfil defined objectives.
- Identifies stakeholders and communication mechanisms to be used.
- Describes how the plan is controlled and adjusted when needed.

8.0 Record [PA.2.1 outcome c, d, e, g, h]

- Contains status information about corrections; schedule and work breakdown structure.
- Monitors identified risks.
- States results achieved or provides evidence of activities performed in a process.
- Provides evidence of communication, meetings, reviews and corrections.

9.0 Report [PA.2.1 outcome b, c, d]

- Monitors process performance against defined objectives and plans.
- Identifies deviations in process performance.
- Describes results and status of the process.
- Provides evidence of management activities.

6.2.3.2 PA.2.2 Work product management process attribute

The work product management process attribute is a measure of the extent to which the work products produced by the process are appropriately managed. As a result of full achievement of this process 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.*

NOTE 1 Requirements for documentation and control of work products may include requirements for the identification of changes and revision status, approval and re-approval of work products, distribution of work products, and for making relevant versions of applicable work products available at points of use.

NOTE 2 The work products referred to in this Clause are those that result from the achievement of the process purpose through the process outcomes.

6.2.3.2.1 Generic practices for PA.2.2

PA.2.2.GP1 Define the requirements for the work products.

The requirements for the work products to be produced are defined. Requirements may include defining contents and structure.

Quality criteria of the work products are identified.

Appropriate review and approval criteria for the work products are defined.

PA.2.2.GP2 Define the requirements for documentation and control of the work products.

Requirements for the documentation and control of the work products are defined. Such requirements may include requirements for (1) distribution, (2) identification of work products and their components (3) traceability

Dependencies between work products are identified and understood.

Requirements for the approval of work products to be controlled are defined.