TECHNICAL SPECIFICATION

ISO/IEC TS 33072

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)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword v

Introduction vi

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 97
C.1 Associations of base practices with requirements 98
C.2 Associations of requirements with base practices 136
C.3 Base practices that have no associated requirements 180

Bibliography 183

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.

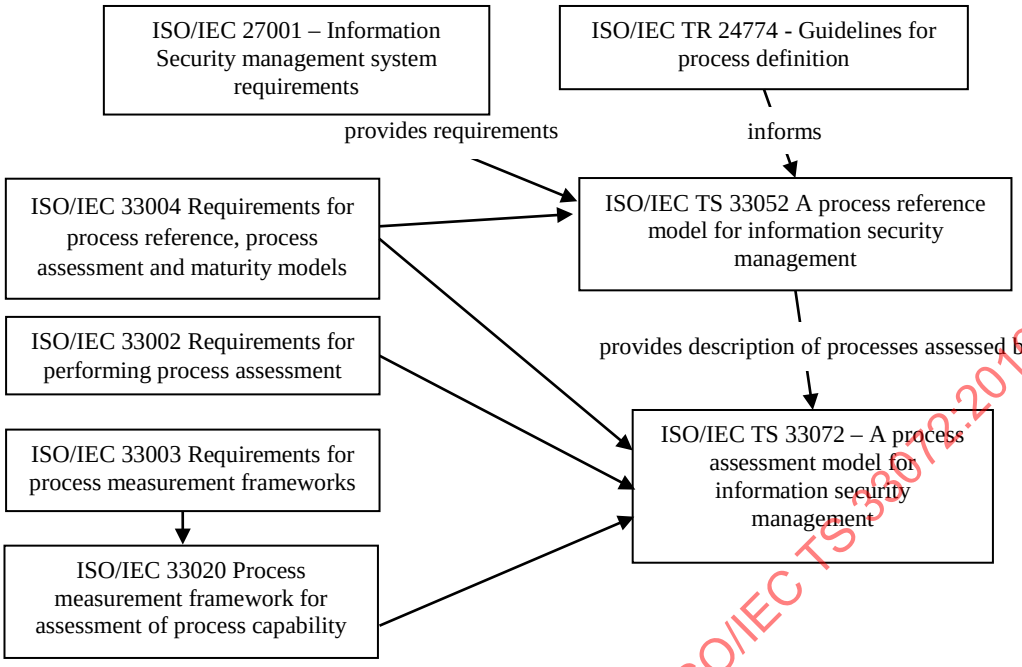

Figure 1 — Relationships between relevant standards

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.

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.

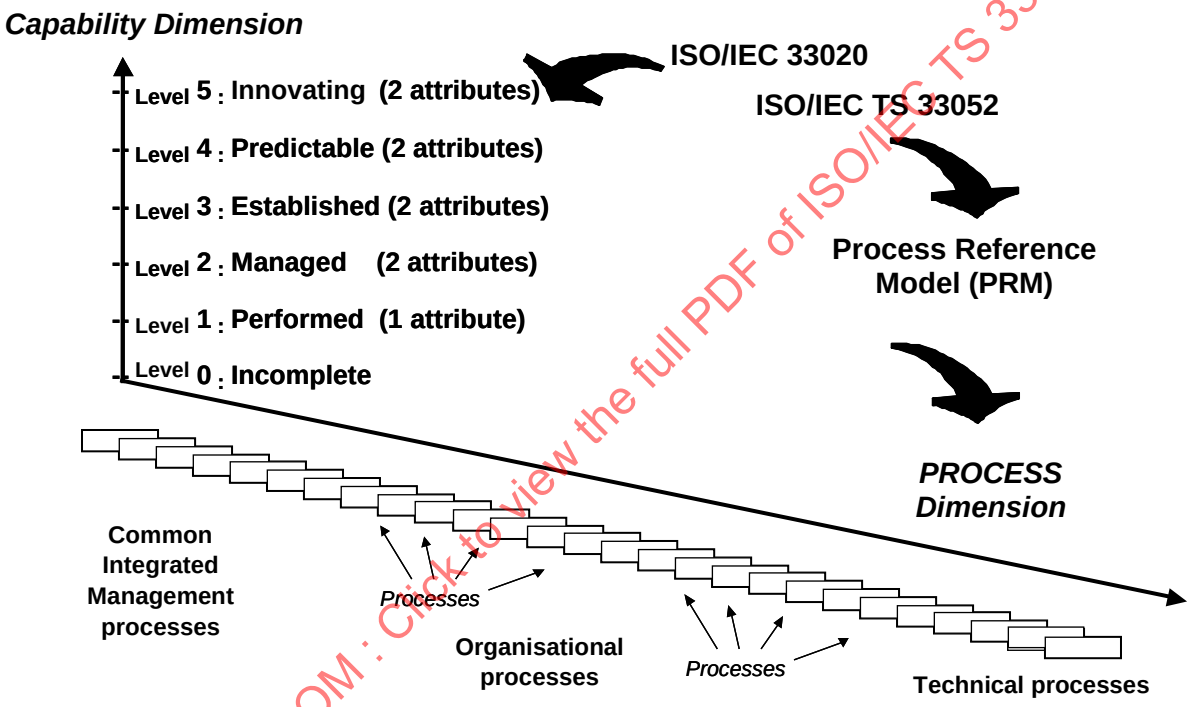

Figure 2 — Relationship between the Process Assessment Model and its inputs

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.

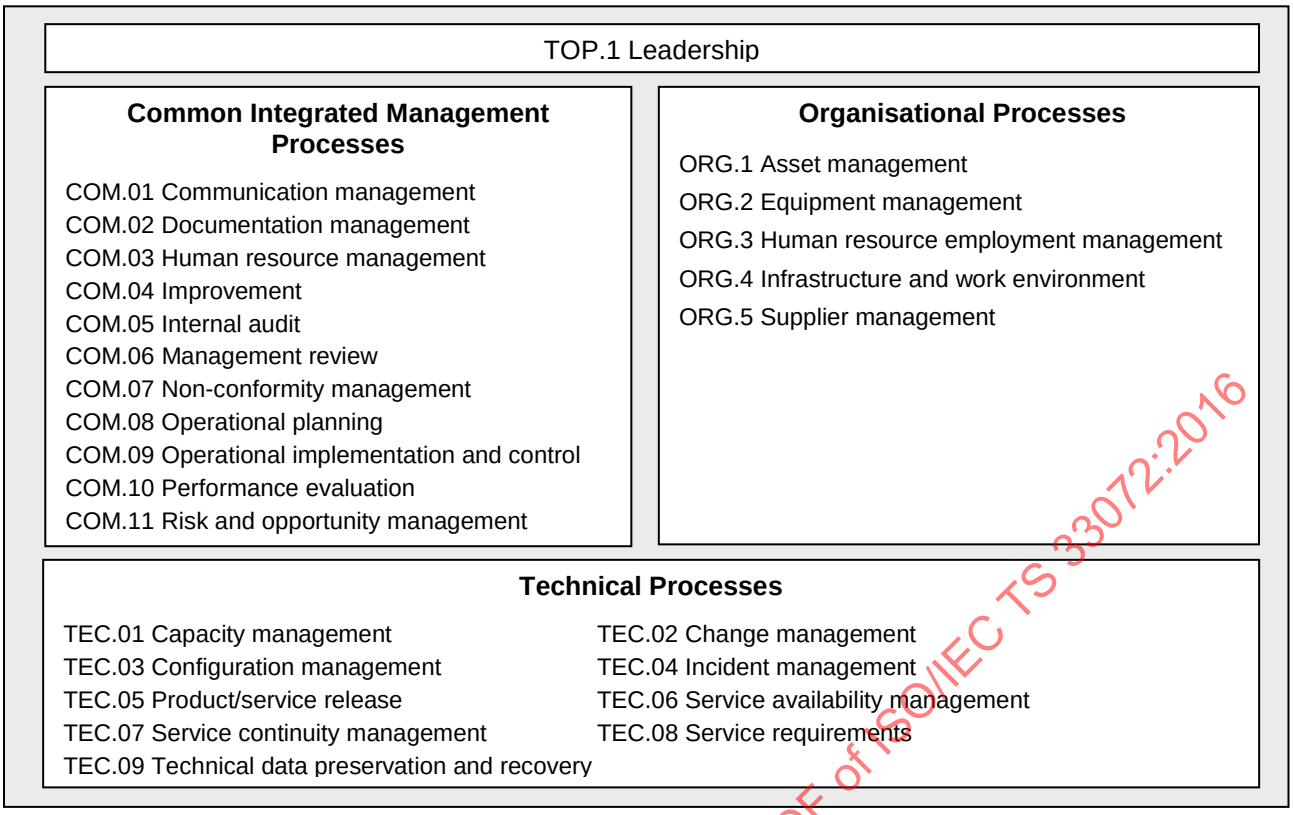

Figure 3 — Processes in the Process Reference Model

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.

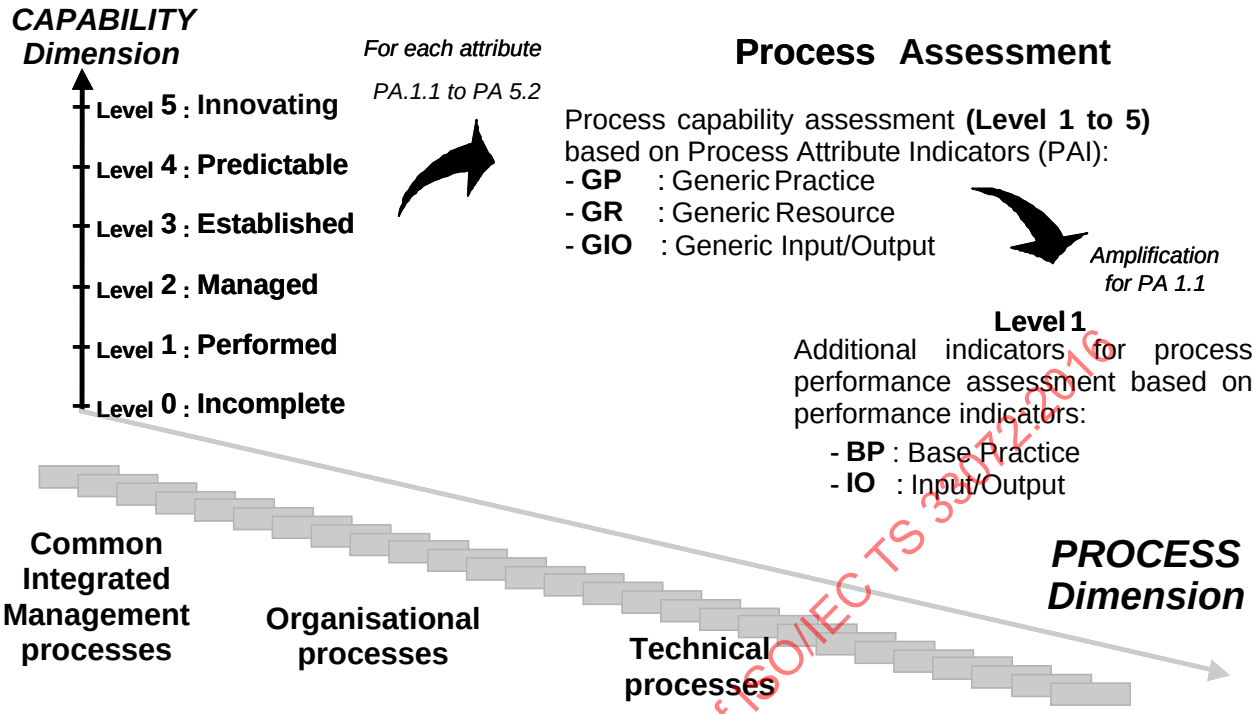

Figure 4 — Assessment indicators

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.

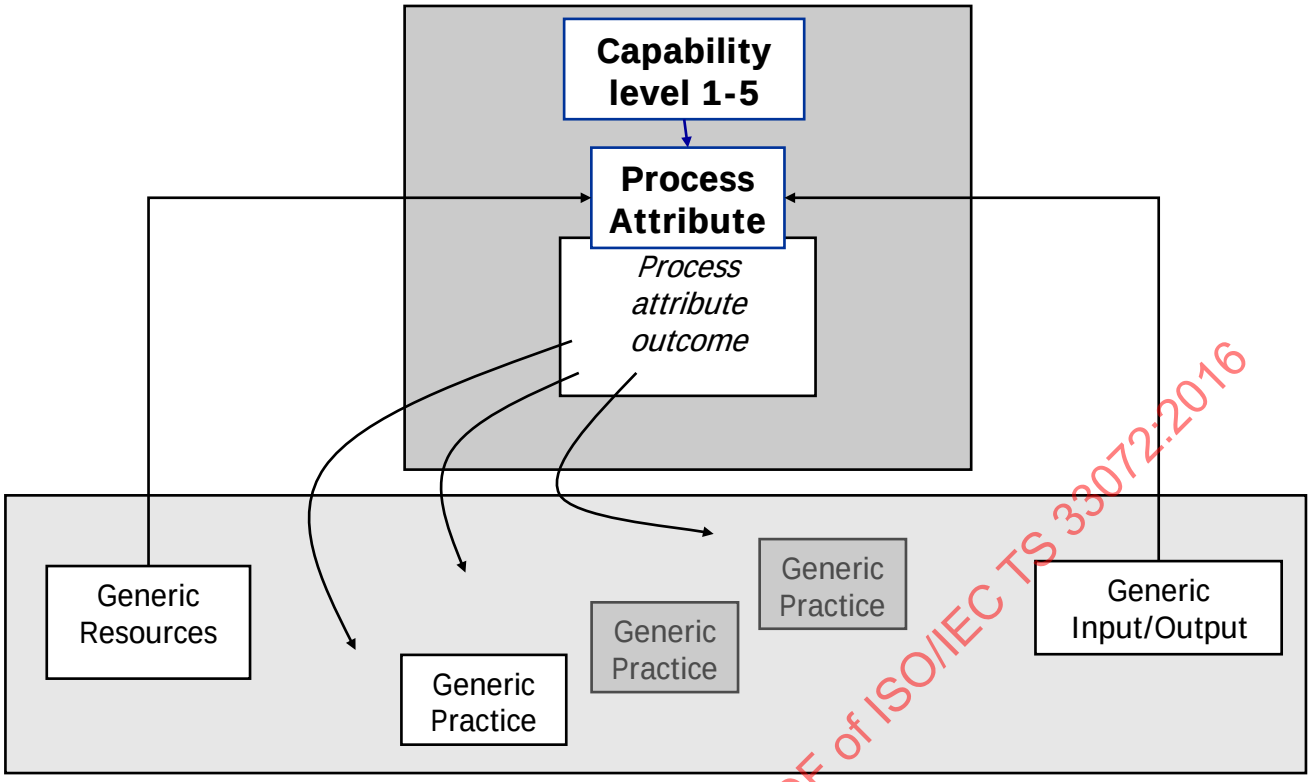

Figure 5 — Process capability indicators

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.

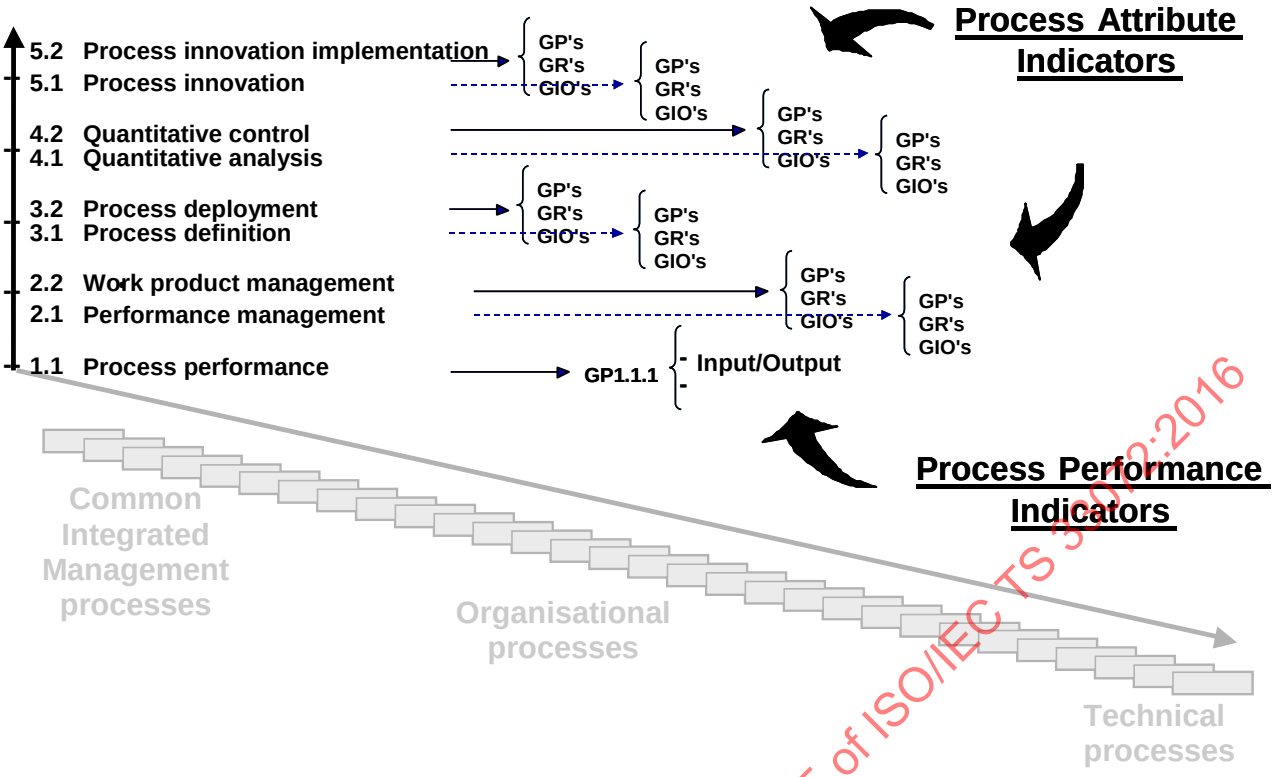

Figure 6 — Relationship between assessment indicators and process capability

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:

a) 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;

b) purpose: describes at a high level the overall objectives of performing the process;

c) 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) 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 comminication 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 repostory. 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 repostory. 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 volations 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 breech 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 breech 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 organsational 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 ncessary 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 ncessary 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 organsational 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 opportunties.** 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 volations 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 securit ypolicy, 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 securitymanagement 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 securitymanagement 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 volations 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 avalability.** Test service availability against the service availability requirements. [Outcome 3] TEC.06.4 **Monitor service availability.** Monitor service availabilit. [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.

PA.2.2.GP3 Identify, document and control the work products. The work products to be controlled are identified. Change control is established for work products. The work products are documented and controlled in accordance with requirements. Versions of work products are assigned to product configurations as applicable. The work products are made available through appropriate access mechanisms. The revision status of the work products may readily be ascertained.
PA.2.2.GP4 Review and adjust work products to meet the defined requirements. Work products are reviewed against the defined requirements in accordance with planned arrangements. Issues arising from work product reviews are resolved.

6.2.3.2.2 Generic resources for PA.2.2

- Requirement management method / toolset; [PA.2.2 outcome a, b, c]
- Configuration management system; [PA.2.2 outcome b, c]
- Documentation elaboration and support tool; [PA.2.2 outcome b, c]
- Document identification and control procedure; [PA.2.2 outcome b, c]
- Work product review methods and experiences; [PA.2.2 outcome d]
- Review management method / toolset; [PA.2.2 outcome d]
- Intranets, extranets and/or other communication mechanisms; [PA.2.2 outcome b, c]
- Problem and issue management mechanisms. [PA.2.2 outcome d]

6.2.3.2.3 Generic work products for PA.2.2

4.0 Plan [PA 2.2 outcome b]

- Expresses selected policy or strategy to manage work products.
- Describes requirements to develop, distribute, and maintain the work products.
- Defines quality control actions needed to manage the quality of the work product.

7.0 Product [PA 2.2 outcome a, b, c, d]

- Demonstrates process specific work products to be managed.

8.0 Record [PA 2.2 outcome c, d]

- Records the status of documentation or work product.
- Demonstrates work product reviews and contributes to traceability.
- Describes non-conformance detected during work product reviews.

— Provides evidence that the changes are under control.

10.0 Repository [PA 2.2 outcome c]

— Contains and makes available work products and/or configuration items.

— Supports monitoring of changes to work products.

12.0 Specification [PA 2.2 outcome a, b]

— Defines the attributes associated with a work product to be created.

— Defines the functional and non-functional requirements for work products.

— Identifies work product dependencies.

— Identifies approval criteria for documents.

6.2.4 Process capability Level 3: Established process

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

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

6.2.4.1 PA.3.1 Process definition process attribute

The process definition process attribute is a measure of the extent to which a standard process is maintained to support the deployment of the defined process. As a result of full achievement of this process attribute:

a) A standard process, including appropriate tailoring guidelines, is defined and maintained that describes the fundamental elements that must be incorporated into a defined process;

b) The sequence and interaction of the standard process with other processes is determined;

c) Required competencies and roles for performing the process are identified as part of the standard process;

d) Required infrastructure and work environment for performing the process are identified as part of the standard process;

e) Suitable methods and measures for monitoring the effectiveness and suitability of the process are determined.

6.2.4.1.1 Generic practices for PA.3.1

PA.3.1.GP1 Define the standard process that will support the deployment of the defined process.
A standard process is developed that includes the fundamental process elements.
The standard process identifies the deployment needs and deployment context.
Guidance and/or procedures are provided to support implementation of the process as needed.
Appropriate tailoring guideline(s) are available as needed.

PA.3.1.GP2 Determine the sequence and interaction between processes so that they work as an integrated system of processes. The standard process's sequence and interaction with other processes are determined. Deployment of the standard process as a defined process maintains integrity of processes.
PA.3.1.GP3 Identify the roles and competencies for performing the standard process. Process performance roles are identified Competencies for performing the process are identified.
PA.3.1.GP4 Identify the required infrastructure and work environment for performing the standard process. Process infrastructure components are identified (facilities, tools, networks, methods, etc). Work environment requirements are identified.
PA.3.1.GP5 Determine suitable methods and measures to monitor the effectiveness and suitability of the standard process. Methods and measures for monitoring the effectiveness and suitability of the process are determined. Appropriate criteria and data needed to monitor the effectiveness and suitability of the process are defined. The need to conduct internal audit and management review is established. Process changes are implemented to maintain the standard process.

6.2.4.1.2 Generic resources for PA.3.1

- Process modelling methods / tools; [PA.3.1 outcome a, b, c, d]
- Training material and courses; [PA.3.1 outcome a, b, c]
- Resource management system; [PA.3.1 outcome b, c]
- Process infrastructure; [PA.3.1 outcome a, b]
- Audit and trend analysis tools; [PA.3.1 outcome e]
- Process monitoring method. [PA.3.1 outcome e]

6.2.4.1.3 Generic work products for PA.3.1

3.0 Description [PA 3.1 outcome a, b, c, e]

- Describes the standard process, including the fundamental process elements, interactions with other processes and appropriate tailoring guidelines.
- Addresses the performance, management and deployment of the process, as described by capability levels 1 and 2 and the PA 3.2 Process deployment attribute.
- Addresses methods to monitor process effectiveness and suitability.
- Identifies data and records to be collected when performing the defined process, in order to improve the standard process.
- Identifies and communicates the personnel competencies, roles and responsibilities for the standard and defined process.
- Identifies the personnel performance criteria for the standard and defined process.

— Identifies the tailoring guidelines for the standard process.

— Identifies process measures.

4.0 Plan [PA 3.1 outcome c, d]

— Identifies approaches for defining, maintaining and supporting a standard process, including infrastructure, work environment, training, internal audit and management review.

5.0 Policy [PA 3.1 outcome a, b, c, d, e]

— Provides evidence of organizational commitment to maintain a standard process to support the deployment of the defined process.

10.0 Repository [PA 3.1 outcome d]

— Is used to support and maintain the standard process assets.

12.0 Specification [PA 3.1 outcome a]

— Provides reference for the standards used by the standard process and identification about how they are used.

6.2.4.2 PA.3.2 Process deployment process attribute

The process deployment process attribute is a measure of the extent to which the standard process is deployed as a defined process to achieve its process outcomes. As a result of full achievement of this process attribute:

a) A defined process is deployed based upon an appropriately selected and/or tailored standard process;

b) Required roles, responsibilities and authorities for performing the defined process are assigned and communicated;

c) Personnel performing the defined process are competent on the basis of appropriate education, training, and experience;

d) Required resources and information necessary for performing the defined process are made available, allocated and used;

e) Required infrastructure and work environment for performing the defined process are made available, managed and maintained;

f) Appropriate data are collected and analyzed as a basis for understanding the behaviour of the process, to demonstrate the suitability and effectiveness of the process, and to evaluate where continual improvement of the process can be made.

6.2.4.2.1 Generic practices for PA.3.2

PA.3.2.GP1 Deploy a defined process that satisfies the context specific requirements of the use of the standard process.
The defined process is appropriately selected and/or tailored from the standard process.
Conformance of defined process with standard process requirements is verified.

PA.3.2.GP2 Assign and communicate roles, responsibilities and authorities for performing the defined process. The roles for performing the defined process are assigned and communicated. The responsibilities and authorities for performing the defined process are assigned and communicated.
PA.3.2.GP3 Ensure necessary competencies for performing the defined process. Appropriate competencies for assigned personnel are identified. Suitable training is available for those deploying the defined process.
PA.3.2.GP4 Provide resources and information to support the performance of the defined process. Required human resources are made available, allocated and used. Required information to perform the process is made available, allocated and used.
PA.3.2.GP5 Provide adequate process infrastructure to support the performance of the defined process. Required infrastructure and work environment is available. Organizational support to effectively manage and maintain the infrastructure and work environment is available. Infrastructure and work environment is used and maintained.
PA.3.2.GP6 Collect and analyse data about performance of the process to demonstrate its suitability and effectiveness. Data required to understand the behaviour, suitability and effectiveness of the defined process are identified. Data are collected and analysed to understand the behaviour, suitability and effectiveness of the defined process. Results of the analysis are used to identify where continual improvement of the standard and/or defined process can be made.

6.2.4.2.2 Generic resources for PA.3.2

- Feedback mechanisms (customer, staff, other stakeholders); [PA.3.2 outcome f]
- Process repository; [PA.3.2 outcome a, b]
- Resource management system; [PA.3.2 outcome b, c, d]
- Knowledge management system; [PA.3.2 outcome d]
- Problem and change management system; [PA.3.2 outcome f]
- Working environment and infrastructure; [PA.3.2 outcome e]
- Data collection analysis system: [PA.3.2 outcome f]
- Process assessment framework; [PA.4.1 outcome f]
- Audit / review system. [PA.3.2 outcome f]

6.2.4.2.3 Generic work products for PA.3.2

2.0 Data [PA 3.2 outcome f]

— Provides evidence that the project's defined process performance data was collected.

4.0 Plan [PA 3.2 outcome a, b, f]

— Expresses the strategy for the organizational support, allocation and use of the process infrastructure.

— Describes the project's resources and the elements of the infrastructure needed to deploy the defined process.

— Expresses the strategy to satisfy the project's training needs.

— Identifies process improvement proposal(s) based on analysis of suitability and effectiveness.

3.0 Description [PA 3.2 outcome a]

— Describes the defined process for use by the project.

— Describes the verification activities needed to ensure the conformance of the project's defined process with the organization's standard process.

— Represents the interactions of the project's defined process with other processes.

8.0 Record [PA 3.2 outcome a, b, c, d, e, f]

— Captures the project's work breakdown structure needed to define the tasks and their dependencies.

— Provides evidence that the project personnel possess the required authorities, skills, experience and knowledge.

— Provides evidence that project personnel have received the required training to satisfy the needs of the project.

— Provides evidence that project infrastructure and working environment are made available and maintained for performing the defined process.

— Records the status of required corrective actions.

9.0 Report [PA 3.2 outcome f]

— Provides results of the analysis, recommended corrective action, feedback to the process owner and to the organization's standard process.

— Identifies improvement opportunities of the defined process.

— Provides evidence on the suitability and effectiveness of the defined process.

10.0 Repository [PA 3.2 outcome d]

— Provides evidence that information is made available for performing the defined process.

12.0 Specification [PA 3.2 outcome f]

— Provides a basis to analyse data associated with the performance of the defined process.

6.2.5 Process capability 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.

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

6.2.5.1 PA.4.1 Quantitative analysis process attribute

The quantitative analysis process attributes a measure of the extent to which information needs are defined, relationships between process elements are identified and data are collected. As a result of full achievement of this process attribute:

a) The process is aligned with quantitative business goals;

b) Process information needs in support of relevant defined quantitative business goals are established;

c) Process measurement objectives are derived from process information needs;

d) Measurable relationships between process elements that contribute to the process performance are identified;

e) Quantitative objectives for process performance in support of relevant business goals are established;

f) Appropriate measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance;

g) Results of measurement are collected, validated and reported in order to monitor the extent to which the quantitative objectives for process performance are met;

NOTE 1 Information needs typically reflect management, technical, project, process or product needs.

NOTE 2 Measures may be either process measures or product measures or both.

6.2.5.1.1 Generic practices for PA.4.1

PA.4.1.GP1 Align the process with quantitative business goals. Quantitative business goals relevant to the process are identified. The process supports achievement of the identified business goals.
PA.4.1.GP2 Identify process information needs, in relation to quantitative business goals. Business goals relevant to establishing quantitative process measurement objectives for the process are identified. Process stakeholders are identified and their information needs are defined. Information needs are relevant to the quantitative business goals.
PA.4.1.GP3 Derive process measurement objectives from process information needs. Process measurement objectives to satisfy defined process information needs are defined.
PA.4.1.GP4 Identify measurable relationships between process elements that contribute to the process performance. Relationships between process elements are determined. Measures of process performance are justifiable.

PA.4.1.GP5 Establish quantitative objectives for the performance of the defined process, according to the alignment of the process with the business goals. Process performance objectives are defined to explicitly reflect the quantitative business goals. Process performance objectives are verified with process stakeholders to be realistic and useful.
PA.4.1.GP6 Identify product and process measures that support the achievement of the quantitative objectives for process performance. Detailed measures are defined to support monitoring, analysis and verification needs of process and product goals. Measures to satisfy process measurement and performance objectives are defined. Frequency of data collection is defined. Algorithms and methods to create derived measurement results from base measures are defined, as appropriate. Verification mechanism for base and derived measures is defined.
PA.4.1.GP7 Collect product and process measurement results through performing the defined process. Data collection mechanism is created for all identified measures. Required data is collected in an effective and reliable manner. Measurement results are created from the collected data within defined frequency. Analysis of measurement results is performed within defined frequency. Measurement results are validated to confirm that the results fulfil the process information needs. Measurement results are reported to those responsible for monitoring the extent to which quantitative objectives are met.

6.2.5.1.2 Generic resources for PA.4.1

- Management information (cost, time, reliability, profitability, customer benefits, risks etc.); [PA.4.1 outcome a, b, c, d, e, f, g]
- Applicable measurement techniques; [PA.4.1 outcome f]
- Product and process measurement tools and results databases; [PA.4.1 outcome f, g]
- Process measurement framework; [PA.4.1 outcome d, e, f, g]
- Tools for data analysis and measurement. [PA.4.1 outcome c, d, e, f, g]

6.2.5.1.3 Generic work products for PA.4.1

2.0 Data [PA 4.1 outcome g]

- Defines data to be collected as specified in plans and measures.

3.0 Description [PA 4.1 outcome a, b, d, f]

- Defines information needs for the process.
- Specifies candidate measures.

4.0 Plan [PA 4.1 outcome a, b, c, e, f]

— Identifies the objective to be achieved.

— Describes process performance goals aligned with business goals and context-specific other relevant goals.

— Defines quantitative objectives for process performance.

— Specifies measures for the process.

— Defines tasks and schedules to collect and analyse data.

— Allocates responsibilities and resources for measurement.

9.0 Report [PA 4.1 outcome g]

— Provides results of process data analysis to identify process performance parameters.

12.0 Specification [PA 4.1 outcome b, c, f]

— Describes information needs and performance objectives.

— Provides a basis for analyzing process performance.

— Defines explicit criteria for data validation.

— Defines frequency of data collection.

6.2.5.2 PA.4.2 Quantitative control process attribute

The quantitative control process attribute is a measure of the extent to which objective data are used to manage process performance that is predictable. As a result of full achievement of this process attribute:

a) Techniques for analysing the collected data are selected;

b) Assignable causes of process variation are determined through analysis of the collected data;

c) Distributions that characterize the process performance are established;

d) Corrective actions are taken to address assignable causes of variation;

e) Separate distributions are established (as necessary) for analysing the process under the influence of assignable causes of variation;

6.2.5.2.1 Generic practices for PA.4.2

PA.4.2.GP1 Select analysis techniques, appropriate to collected data. Process control analysis methods and techniques are defined. Selected techniques are validated against process control objectives.
PA.4.2.GP2 Determine assignable causes of process variation by analysing the collected data. Variation in process performance is attributed to a specific, unpredictable cause. Assignable cause indicates a possible problem in the defined process.

PA.4.2.GP3 Establish distributions that characterize the process performance. Variation in measurement results is used to analyse process performance. Deviations are analysed to identify potential cause(s) of variation. Trends of process performance are identified.
PA.4.2.GP4 Identify and implement corrective actions to address assignable causes. Results are provided to those responsible for taking action. Corrective actions are determined to address each assignable cause. Corrective actions are implemented to address assignable causes of variation. Corrective action results are monitored. Corrective actions are evaluated to determine their effectiveness.
PA.4.2.GP5 Establish separate distributions for analysing the process under the influence of assignable causes of variation. Consequences of process variation are analysed. Distributions are used to quantitatively understand process performance.

6.2.5.2.2 Generic resources for PA.4.2

- Process control and analysis techniques; [PA.4.2 outcome a, b]
- Statistical analysis tools / applications; [PA.4.2 outcome b, c, e]
- Process control tools / applications. [PA.4.2 outcome c, d, e]

6.2.5.2.3 Generic work products for PA.4.2

2.0 Data [PA 4.2 outcome b]

- Provides measurement data to identify assignable causes of variation.

3.0 Description [PA 4.2 outcome b, c, e]

- Defines parameters for process control.
- Defines and maintains limits for variation.

4.0 Plan [PA 4.2 outcome a]

- Defines analysis methods and techniques at detailed level.

8.0 Record [PA 4.2 outcome c, d, e]

- Provides information on defects and problems.
- Records the changes.
- Documents corrective actions to be implemented.

— Monitors the status of corrective actions.

9.0 Report [PA 4.2 outcome a, c, d, e]

— Provides analyzed measurement results of process performance.

— Identifies corrective actions to address assignable causes of variation.

— Ensures that selected techniques are effective and measures are validated.

10.0 Repository [PA 4.2 outcome a, b, c, d, e]

— Collects the data and provides the basis for analysis, corrective actions and results reporting.

12.0 Specification [PA 4.2 outcome a, b, e]

— Defines the method for collecting data.

— Measures the efficiency of the process.

6.2.6 Process capability Level 5: Innovating process

The previously described *Predictable process* is now continually improved to respond to organizational change.

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

6.2.6.1 PA.5.1 Process innovation process attribute

The process innovation process attribute is a measure of the extent to which changes to the process are identified from investigations of innovative approaches to the definition and deployment of the process. As a result of full achievement of this process attribute:

a) Process innovation objectives are defined that support the relevant business goals;

b) Appropriate data are analysed to identify opportunities for best practice and innovation;

c) Innovation opportunities derived from new technologies and process concepts are identified;

d) An implementation strategy is established to achieve the process innovation objectives.

6.2.6.1.1 Generic practices for PA.5.1

PA.5.1.GP1 Define the process innovation objectives for the process that support the relevant business goals.

Directions to process innovation are set.

New business visions and goals are analyzed to give guidance for new process objectives and potential areas of process change.

Quantitative and qualitative process innovation objectives are defined and documented.

PA.5.1.GP2 Analyse data of the process to identify opportunities for best practice and innovation. Feedback on opportunities for innovation is actively sought. Innovation opportunities are identified. Industry best practices are identified and evaluated.
PA.5.1.GP3 Identify innovation opportunities of the process from new technologies and process concepts. Impact of new technologies on process performance is identified and evaluated. Impact of new process concepts is identified and evaluated. Innovation opportunities are identified. Emergent risks are considered in identifying innovation opportunities
PA.5.1.GP4 Define an implementation strategy based on long-term innovation vision and objectives. Commitment to innovation is demonstrated by organizational management and process owner(s). Proposed process changes are evaluated and piloted to determine their benefits and expected impact on defined business objectives. Changes are classified and prioritized based on their impact on defined innovation objectives. Measures that validate the results of process changes are defined to determine expected effectiveness of the process change. Implementation of the approved change(s) is planned as an integrated program or project. Implementation plan and impact on business goals are discussed and reviewed by organizational management.

6.2.6.1.2 Generic resources for PA.5.1

- Process innovation framework; [PA.5.1 outcome a, c, d]
- Process feedback and analysis system (measurement data, causal analysis results etc.); [PA.5.1 outcome b]
- Piloting and trialling mechanism. [PA.5.1 outcome b, c]

6.2.6.1.3 Generic work products for PA.5.1

2.0 Data [PA 5.1 outcome b, c]

- Provides analytical data to identify opportunities for best practice and innovation.

3.0 Description [PA 5.1 outcome c, d]

- Identifies potential areas of innovation and new technology.

4.0 Plan [PA 5.1 outcome a, d]

- Define and maintain business goals.
- Provides evidence of management commitment.
- Defines innovation objectives for the process

— Allocates resources for innovation activities.

— Schedules activities for root cause analysis.

— Defines an approach to implementing selected innovations.

— Identifies scope of pilot innovation activities.

5.0 Policy [PA 5.2 outcome a]

— Establishes expectations for conduct and evaluation of pilot innovations.

8.0 Record [PA 5.1 outcome c, d]

— Identifies potential innovation opportunities.

— Records information on new technology and techniques.

9.0 Report [PA 5.1 outcome b, c]

— Identifies potential innovations and process changes.

6.2.6.2 PA.5.2 Process innovation implementation process attribute

The process innovation implementation process attribute is a measure of the extent to which changes to the definition, management and performance of the process achieves the relevant process innovation objectives. As a result of full achievement of this process attribute:

a) Impact of all proposed changes is assessed against the objectives of the defined process and standard process;

b) Implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted upon;

c) Effectiveness of process change on the basis of actual performance is evaluated against the defined product requirements and process objectives.

6.2.6.2.1 Generic practices of PA.5.2

PA.5.2.GP1 Assess the impact of each proposed change against the objectives of the defined and standard process.
Objective priorities for process innovation are established.
Specified changes are assessed against product quality and process performance requirements and goals.
Impact of changes to other defined and standard processes is considered.

PA.5.2.GP2. **Manage the implementation of agreed changes** to selected areas of the defined and standard process according to the implementation strategy. A mechanism is established for incorporating accepted changes into the defined and standard process(es) effectively and completely. The factors that impact the effectiveness and full deployment of the process change are identified and managed, such as: • Economic factors (productivity, profit, growth, efficiency, quality, competition, resources, and capacity); • Human factors (job satisfaction, motivation, morale, conflict / cohesion, goal consensus, participation, training, span of control); • Management factors (skills, commitment, leadership, knowledge, ability, organisational culture and risks); • Technology factors (sophistication of system, technical expertise, development methodology, need of new technologies). Training is provided to users of the process. Process changes are effectively communicated to all affected parties**.** Records of the change implementation are maintained.
PA.5.2.GP3 Evaluate the effectiveness of process change on the basis of actual performance against process performance and capability objectives and business goals. Performance and capability of the changed process are measured and compared with historical data. A mechanism is available for documenting and reporting analysis results to management and owners of standard and defined process. Measures are analysed to evaluate the effectiveness of process changes. Other feedback is recorded, such as opportunities for further innovation of the standard process.

6.2.6.2.2 Generic resources for PA.5.2

— Change management system. [PA.5.2 outcome a, b, c]

— Process evaluation system (impact analysis, etc.). [PA.5.2 outcome a, c]

6.2.6.2.3 Generic work products for PA.5.2

3.0 Description [PA 5.2 outcome b]

— Documents changes as a result of process innovation actions.

4.0 Plan [PA 5.2 outcome a, b]

— Defines activities and schedule for pilot change implementation.

— Allocates resources for pilot implementation.

— Assigns responsibility for pilot implementation.

— Defines activities and schedule for organizational implementation of process change.

— Allocates resources and responsibilities for organizational implementation.

— Specifies scope of pilot implementation of proposed change.

8.0 Record [PA 5.2 outcome b]

— Contains records of all completed and in-progress pilot implementations.

— Records history of and justification for changes.

9.0 Report [PA 5.2 outcome a, b, c]

— Describes results of pilot implementation of process change.

— Evaluates effectiveness of process compared to process innovation objectives.

— Provides details on implementation of organizational changes.

— Describes proposed changes to standard and defined process.

12.0 Specification [PA 5.2 outcome c]

— Specifies measures derived from process innovation objectives.

6.3 Related processes for process attributes

Certain processes support achievement of the capabilities addressed by a process attribute. Table 11 lists those processes and indicates the relation between those processes and each process attribute (PA). This information can be used in planning process assessments and in analysis and validation of the assessment results.

Table 11 — Related processes for process attributes

	Process attributes							
Related processes	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Asset management				X				
Capacity management				X				
Change management		X						
Communication	X							
Configuration management		X						
Documentation management		X		X				
Equipment management				X				
Human resource employment management	X			X				
Human resource management	X			X				
Improvement				X				
Incident management		X						
Information environment access management	X			X				
Infrastructure and work environment				X				
Internal audit		X						
Leadership							X	X
Management review				X				
Non-conformity management				X				
Operational implementation and control				X				
Operational planning			X					
Performance evaluation				X	X	X		
Product/ service release		X						
Risk and opportunity management	X			X				

	Process attributes							
Related processes	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Service availability management				X				
Service continuity management				X				
Service requirements	X							
Supplier management	X							
Technical data preservation and recovery		X						

Annex A
(informative)

Conformity of the process assessment model

A.1 Introduction

This Technical Specification sets out a process assessment model that meets the requirements for conformance defined in ISO/IEC 33004. The process assessment model can be used in the performance of assessments that meet the requirements of ISO/IEC 33002. It may also be used as an example for a process assessment model developer.

This clause serves as the statement of conformance of the process assessment model to the requirements defined in ISO/IEC 33004. For ease of reference, the requirements from Clause 6 of ISO/IEC 33004 are embedded verbatim in the text of this clause. They should not be construed as normative elements of this International Standard.

Since this process assessment model has been explicitly constructed to be an elaboration of the process reference model defined in ISO/IEC TS 33050-4, the conformance claim is relatively simple. For other models, particularly ones with a different architecture, the demonstration of conformance may be more difficult requiring more detail in the mapping.

A.2 Requirements for process assessment models

A.2.1 Introduction

> *In order to assure that assessment results are translatable into the intended process measurement framework in a repeatable and reliable manner, process assessment models shall adhere to certain requirements. A process assessment model shall contain a definition of its purpose, scope and elements; its mapping to the process measurement framework and specified process reference model(s); and a mechanism for consistent expression of results.*
>
> *[ISO/IEC 33004, 6.1]*

The purpose of this process assessment model is to support assessment of process capability using the process measurement framework defined in ISO/IEC 33020.

A.2.2 Process assessment model scope

> *Process assessment models are related to one or more process reference models and a process measurement framework. Processes in process assessment model(s) are based on the process descriptions provided in process reference models; process attributes and process quality levels (if applicable) are derived from a process measurement framework.*
>
> *In order to assure that assessment results are translatable into a set of process profiles in a repeatable and reliable manner, process assessment models shall adhere to certain requirements.*
>
> *[ISO/IEC 33004, 6.2]*

The process scope of this process assessment model is defined in the process reference model specified in ISO/IEC TS 33050-4, which defines a process reference model satisfying the requirements of ISO/IEC 33004, Clause 5. The process capability scope of this process assessment model is defined in the process

measurement framework specified in ISO/IEC 33020, which defines a process measurement framework for process capability satisfying the requirements of ISO/IEC 33003.

A.2.3 Requirements for process assessment models

6.3.1 *A process assessment model shall relate to at least one process from the specified process reference model(s).*

6.3.2 *A process assessment model shall address, for a given process, all, or a continuous subset, of the levels (starting at process quality level 1) of the process measurement framework for process quality characteristic for each of the processes within its scope.*

NOTE: It would be permissible for a model, for example, to address solely process quality level 1, or to address process quality levels 1, 2 and 3, but it would not be permissible to address process quality levels 2 and 3 without process quality level 1.

6.3.3 *A process assessment model shall declare its scope of coverage in the terms of:*

a) the selected process reference model(s);

b) the selected processes taken from the process reference model(s);

c) the process quality level of the process characteristic selected from the process measurement framework.

[ISO/IEC 33004, 6.3]

This process assessment model is based upon the process reference model defined in ISO/IEC TS 33050-4, addressing all of the processes identified in Clause 4, Figure 3 of this Technical Specification.

In the capability dimension of this process assessment model, the model addresses all of the process attributes and capability levels defined in the process measurement framework in ISO/IEC 33020, Clause 5.

A.2.4 Assessment indicators

A process assessment model shall be based on a set of indicators that

a) explicitly addresses the purposes and process outcomes, as defined in the selected process reference model, of all the processes within the scope of the process assessment model; and

b) demonstrates the achievement of the process attributes for the process quality characteristic scope of the process assessment model.

The assessment indicators generally fall into three types:

a) Practices – institutionalised behaviours that support achievement of either the Process Purpose or a specific process attribute.

b) Information items and their characteristics that demonstrate the respective achievements.

c) Resources and infrastructure that support the respective achievements.

[ISO/IEC 33004, 6.3.4]

The process assessment model provides a two-dimensional view of process capability for the processes in the process reference model, through the inclusion of assessment indicators as shown in Figure 4. The assessment Indicators used are:

— base practices and work products; and

— generic practices, generic resources and generic work products

as shown in Clause 4, Figure 3. They support the judgment of the performance and capability of an implemented process.

A.2.5 Mapping process assessment models to process reference models

A process assessment model shall provide an explicit mapping from the relevant elements of the process assessment model to the processes of the selected process reference model(s) and to the relevant process attributes of the process measurement framework.

The mapping shall be complete, clear and unambiguous. The mapping of the assessment indicators within the process assessment model shall be to:

a) the purpose and process outcomes of the processes in the specified process reference model;

b) the process attributes (including all of the process attribute achievements listed for each process attribute) in the process measurement framework.

This enables process assessment models that are structurally different to be related to the same process reference model(s).

[ISO/IEC 33004, 6.3.5]

Each of the Processes in this process assessment model is identical in scope to the Process defined in the process reference model. Each base practice and work product is cross-referenced to the Process outcomes it addresses. All work products relate as Inputs or Outputs to the Process as a whole - see mappings in clause 5.

Each of the process attributes in this process assessment model is identical to the process attribute defined in the process measurement framework. The generic practices address the characteristics from each process attribute. The generic resources and generic work products relate to the process attribute as a whole.

Table A.1 lists the mappings of the GPs to the achievements associated with each process attribute.

Table A.1 — Mapping of generic practices

GP	Practice name	Maps to
PA.1.1: Process performance process attribute		
PA.1.1.GP1	Achieve the process outcomes.	PA.1.1 a
PA.2.1: Performance management process attribute		
PA.2.1.GP1	Identify the objectives for the performance of the process.	PA.2.1 a
PA.2.1.GP2	Plan the performance of the process to fulfil the identified objectives.	PA.2.1 b
PA.2.1.GP3	Monitor the performance of the process against the plans.	PA.2.1 c
PA.2.1.GP4	Adjust the performance of the process.	PA.2.1 d
PA.2.1.GP5	Define responsibilities and authorities for performing the process.	PA.2.1 e
PA.2.1.GP6	Prepare those performing the process to execute their responsibilities.	PA.2.1 f
PA.2.1.GP7	Identify and make available resources to perform the process according to plan.	PA.2.1 g
PA.2.1.GP8	Manage the interfaces between involved parties.	PA.2.1 h
PA.2.2: Work product management process attribute		

GP	Practice name	Maps to
PA.2.2.GP1	Define the requirements for the work products.	PA.2.2 a
PA.2.2.GP2	Define the requirements for documentation and control of the work products.	PA.2.2 b
PA.2.2.GP3	Identify, document and control the work products.	PA.2.2 c
PA.2.2.GP4	Review and adjust work products to meet the defined requirements.	PA.2.2 d
PA.3.1: Process definition process attribute		
PA.3.1.GP1	Define the standard process that will support the deployment of the defined process.	PA.3.1 a
PA.3.1.GP2	Determine the sequence and interaction between processes so that they work as an integrated system of processes.	PA.3.1 b
PA.3.1.GP3	Identify the roles and competencies for performing the standard process.	PA.3.1 c
PA.3.1.GP4	Identify the required infrastructure and work environment for performing the standard process.	PA.3.1 d
PA.3.1.GP5	Determine suitable methods and measures to monitor the effectiveness and suitability of the standard process.	PA.3.1 e
PA.3.2: Process deployment process attribute		
PA.3.2.GP1	Deploy a defined process that satisfies the context specific requirements of the use of the standard process.	PA.3.2 a
PA.3.2.GP2	Assign and communicate roles, responsibilities and authorities for performing the defined process.	PA.3.2 b
PA.3.2.GP3	Ensure necessary competencies for performing the defined process.	PA.3.2 c
PA.3.2.GP4	Provide resources and information to support the performance of the defined process.	PA.3.2 d
PA.3.2.GP5	Provide adequate process infrastructure to support the performance of the defined process.	PA.3.2 e
PA.3.2.GP6	Collect and analyse data about performance of the process to demonstrate its suitability and effectiveness.	PA.3.2f
PA.4.1 Quantitative analysis process attribute		
PA.4.1.GP1	Align the process with quantitative business goals.	PA.4.1 a
PA.4.1.GP2	Identify process information needs, in relation with quantitative business goals.	PA.4.1 b
PA.4.1.GP3	Derive process measurement objectives from process information needs.	PA.4.1 c
PA.4.1.GP4	Identify measurable relationships between process elements that contribute to the process performance.	PA.4.1 d
PA.4.1.GP5	Establish quantitative objectives for the performance of the defined process, according to the alignment of the process with the business goals.	PA.4.1 e
PA.4.1.GP6	Identify product and process measures that support the achievement of the quantitative objectives for process performance.	PA.4.1 f
PA.4.1.GP7	Collect product and process measurement results through performing the defined process.	PA.4.1 g
PA.4.2 Quantitative control process attribute		
PA.4.2.GP1	Select analysis techniques, appropriate to collected data.	PA.4.2 a

GP	Practice name	Maps to
PA.4.2.GP2	Determine assignable causes of process variation by analysing the collected data.	PA.4.2 b
PA.4.2.GP3	Establish distributions that characterize the process performance.	PA.4.2 c
PA.4.2.GP4	Identify and implement corrective actions to address assignable causes.	PA.4.2 d
PA.4.2.GP5	Establish separate distributions for analysing the process under the influence of assignable causes of variation.	PA.4.2 e
PA.5.1 Process innovation process attribute		
PA.5.1.GP1	Define the process innovation objectives for the process that support the relevant business goals.	PA.5.1 a
PA.5.1.GP2	Analyse data of the process to identify opportunities for best practice and innovation.	PA.5.1 b
PA.5.1.GP3	Identify innovation opportunities of the process from new technologies and process concepts.	PA.5.1 c
PA.5.1.GP4	Define an implementation strategy based on long-term innovation vision and objectives.	PA.5.1 d
PA.5.2 Process innovation implementation process attribute		
PA.5.2.GP1	Assess the impact of each proposed change against the objectives of the defined and standard process.	PA.5.2 a
PA.5.2.GP2	Manage the implementation of agreed changes to selected areas of the defined and standard process according to the implementation strategy.	PA.5.2 b
PA.5.2.GP3	Evaluate the effectiveness of process change on the basis of actual performance against process performance and capability objectives and business goals.	PA.5.2 c

A.2.6 Expression of assessment results

A process assessment model shall provide a formal and verifiable mechanism for representing the results of an assessment as a set of process attribute ratings for each assessed process (the process profiles) selected from the specified process reference model(s).

[ISO/IEC 33004, 6.3.6]

The processes in this process assessment model are identical to those defined in the process reference model. The process attributes and the process attribute ratings in this process assessment model are identical to those defined in the Measurement Framework. Consequently, results of assessments based upon this process assessment model are expressed directly as a set of process attribute ratings for each process within the scope of the assessment. No translation or conversion is required.

Annex B
(informative)

Input and output characteristics

B.1 General

Characteristics of inputs and outputs listed in this Annex can be used when reviewing potential inputs and outputs of process implementation. The characteristics are provided as guidance for the attributes to look for to provide objective evidence supporting the assessment of a particular process. A documented process and assessor judgment is needed to ensure that the process context (application domain, business purpose, development methodology, size of the organization, etc.) is considered when using this information. Inputs and outputs are defined using the schema in Table B.1. Inputs and outputs and their characteristics should be considered as a starting point for considering whether, given the context, they are contributing to the intended purpose of the process.

Table B.1 —Input / Output identification

Input / Output identifier #	An identifier number for the input / output which is used to reference the input / output.
Input / Output name	Provides an example of a typical name associated with the input / output characteristics. This name is provided as an identifier of the type of input / output the practice or process might produce. Organizations may call these input / outputs by different names. The name of the input / output in the organization is not significant. Similarly, organizations may have several equivalent input / outputs which contain the characteristics defined in one input / output type. The formats for the input / outputs can vary. It is up to the assessor and the organizational unit coordinator to map the actual input / outputs produced in their organization to the examples given here.
Category	A group with which an item is associated.
Input / Output characteristics	Provides examples of the potential characteristics associated with the input / output types. The assessor may look for these in the samples provided by the organizational unit.

B.2 Generic input and outputs

The Generic Work Product Indicators are sets of characteristics that would be expected to be evident in input / outputs of a generic type as a result of achievement of an attribute. The generic input / outputs support the class structure of the input / outputs defined as process performance indicators. These input / output types are basic input types to process owners of all types of processes.

Table B.2 — Generic inputs and outputs

Reference	Category	Purpose	Typical Input / Output Characteristics
1.0	Contract	A contract is the formal agreement between an acquirer and a supplier. [ISO/IEC 15289:2011]	It addresses the following: a) identification of the performing organizations b) statement of work to be performed, with tasks based on a service management process or a system or software life-cycle model, and scope of tasks c) system requirements and software requirements definition and analysis results d) negotiated price and payment schedule e) deliverables, including off-the-shelf products identified f) schedule for suppliers to deliver the product or service g) proprietary rights to systems and technical data and software intellectual property rights: usage, ownership, warranty and licensing rights h) provisions for monitoring; reporting, verification, validation, and acceptance criteria i) procedures for contract changes, exceptions, resolving disputes, and closeout, such as supplier responsibilities in the event of expected or early termination of the contract or formal agreement and the transfer of services to another party. The contract may specify best practices, to include standards and strategies for processes, activities and tasks. Informally, commitments or agreements may be specified between parts of the same organization (sometimes called a memorandum of understanding).
2.0	Data	Ordered informational content	– Result of applying a measure – Available to those who need to know within defined timeframe

Reference	Category	Purpose	Typical Input / Output Characteristics
3.0	description	Information item that represents a planned or actual concept, function, design, or object. [ISO/IEC 15289:2011]	A description includes the following elements: a) Date of issue and status b) Scope c) Issuing organization d) References e) Context f) Notation for description g) Body h) Summary i) Glossary j) Change history
4.0	plan	Information item that presents a systematic course of action for achieving a declared purpose, including when, how, and by whom specific activities are to be performed. [ISO/IEC 15289:2011]	A plan includes the following elements a) Date of issue and status b) Scope c) Issuing organization d) References (applicable policies, laws, standards, contracts, requirements, and other plans and procedures) e) Approval authority f) Approach for technical and management review and reporting g) Other plans (plans or task descriptions that expand on the details of a plan) h) Planned activities and tasks i) Identification of tools, methods, and techniques j) Schedules k) Budgets and cost estimates l) Resources and their allocation m) Responsibilities and authority, including the senior responsible owner and immediate process owner n) Interfaces among parties involved o) Risks and risk identification, assessment and mitigation activities p) Quality assurance and control measures q) Environment, infrastructure, security, and safety r) Training s) Glossary t) Change procedures and history u) Termination process
5.0	policy	clear and measurable statement of preferred direction and behavior to condition the decisions made within an organization [ISO/IEC 15289:2011]	A policy includes the following elements: a) Date of issue, effective date, and status b) Scope c) Issuing organization d) Approval authority and identification of those accountable for enforcing the policy e) Authoritative references for compliance or conformance (such as policies, laws and regulations, standards, contracts, requirements, and vision or mission statements) f) Body, including objectives g) Glossary h) Change history

Reference	Category	Purpose	Typical Input / Output Characteristics
6.0	procedure	Specified way to carry out an activity or a process. [ISO 9000:2005]	A procedure includes the following elements: a) Date of issue and status b) Scope c) Issuing organization d) Approval authority e) Relationship to plans and other procedures f) Authoritative references g) Inputs and outputs h) Ordered description of steps to be taken by each participant i) Error and problem resolution j) Glossary k) Change history
7.0	product	Result of a process [ISO 9000:2005]	There are four generic product categories, as follows: — services (e.g. transport); — software (e.g. computer program, dictionary); — hardware (e.g. engine mechanical part); — processed materials (e.g. lubricant). Service is the result of at least one activity necessarily performed at the interface between the supplier and customer and is generally intangible. Provision of a service can involve, for example, the following: — an activity performed on a customer-supplied tangible product; — an activity performed on a customer-supplied intangible product; — the delivery of an intangible product; — the creation of ambience for the customer.
8.0	record	Organize the data an organizational entity retains. NOTE: Consistent with the ISO 9000 series, the purpose of a record is to state results achieved or to provide evidence of activities performed by an organizational entity.	A record includes the following elements: a) Date of record, date recorded, and status b) Scope c) Subject or category d) Issuing organization e) References f) Body g) Unique record identifier

Reference	Category	Purpose	Typical Input / Output Characteristics
9.0	report	Information item that describes the results of activities such as investigations, observations, assessments, or tests. [ISO/IEC 15289:2011]	A report includes the following elements: a) Date of issue and status b) Scope c) Issuing organization d) Contributors e) Summary f) Introduction g) Context (assumptions) h) Body (including methods of obtaining results) i) Conclusions and recommendations j) References k) Bibliography l) Glossary m) Change history
10.0	repository	Storage facility for data	– Repository for components – Storage and retrieval capabilities – Ability to browse content – Listing of contents with description of attributes – Sharing and transfer of components between affected groups – Effective controls over access – Maintain component descriptions – Recovery of archive versions of components – Ability to report component status – Changes to components are tracked to change / user requests
11.0	request	Information item that initiates a defined course of action or change to fulfill a need. [ISO/IEC 15289:2011]	A request includes the following elements: a) Date of initiation b) Scope c) Subject d) Originator of request e) Identification of requested item, service, or response f) Detailed description of requested item, service, or response, including due date g) Justifications
12.0	specification	Information item that identifies, in a complete, precise, and verifiable manner, the requirements, design, behavior, or other expected characteristics of a system, service, or process. [ISO/IEC 15289:2011]	A specification includes the following elements: a) Date of issue and status b) Scope c) Issuing organization d) References e) Approval authority f) Body g) Assurance requirements h) Conditions, constraints, and characteristics i) Glossary j) Change history

B.3 Specific inputs and outputs

Specific outputs are typically created by process owners and applied by process deployers in order to satisfy an outcome of a particular process purpose.

NOTE 1 The reference scheme for the specific inputs and outputs associates the item to the first reference (direct or implied) to an informational element in a sub-clause of ISO/IEC 27001. The set of items in a category is ordered alphabetically.

NOTE 2 The term 'normative' that appears under the Characteristics column refers to a requirement in ISO/IEC 27001 to create an item that contains at least the defined informational characteristics. Where the term 'informative' appears, it implies that the defined characteristics are recommended good practice.

NOTE 3 In most cases the sub-clause reference refers to the second edition of ISO/IEC 27001. For example in 01-2 we have 2ED A.15.1.2. In 02-1 we have 2ED A.08.1.1 (a reference to the second edition) and A7.1.1, a reference to the first edition of ISO/IEC 27001.

NOTE 4 In some cases there are multiple elements to an information item. A single item (for example 01-2) can have more than one descriptive component to it. These elements are differentiated from each other by means for an element reference. For example, in 01-2 there are two descriptive elements, 111, and 112.

Table B.3 — Specific inputs and outputs

Reference	Name	Category	Characteristics
01-1	Business information exchange agreement	Contract	Agreements shall address the secure transfer of business information between the organization and external parties.
01-2	Employee agreement	Contract	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

Reference	Name	Category	Characteristics
01-3	Supplier agreement	Contract	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. The contract contains or include a reference to: a) scope of the services to be delivered by the supplier; b) dependencies between services, processes and the parties; c) requirements to be fulfilled by the supplier; d) service targets; e) interfaces between service management processes operated by the supplier and other parties; f) integration of the supplier's activities within the SMS; g) workload characteristics; h) exceptions; i) authorities and responsibilities of the service provider and the supplier; j) reporting and communication to be provided by the supplier; k) basis for charging; l) activities and responsibilities for the expected or early termination of the contract and the transfer of services to a different party.
02-01	Asset register	Data	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
02-02	Capacity usage data	Data	The data associated with the need for the service provider to monitor capacity usage and analyse data.
02-03	Implemented changes log	Data	A consequence of executing the schedule of change containing details of the approved changes and their proposed deployment dates.
02-04	Improvement opportunity implementation log	Data	Log of actions taken in terms of approved improvement opprtunities.
02-05	Information asset register	Data	All assets shall be clearly identified [and an inventory of all important assets drawn up and maintained.] [All assets shall be clearly identified and] an inventory of all important assets drawn up [and maintained.] [All assets shall be clearly identified and] an inventory of all important assets [drawn up and] maintained.
02-06	ISMS Performance measurement data	Data	Implied in 'The organization retains appropriate documented information as evidence of the monitoring and measurement results.'
02-07	Release log	Data	Implied in information about the success or failure of releases and future release dates is provided to the change management process, and incident and service request management process.

Reference	Name	Category	Characteristics
02-08	Service availability log	Data	Availability of services is monitored, the results recorded.
02-09	Supplier performance data	Data	Data relating to the performance by the supplier against agreed service level targets and other contractual commitments.
02-10	Supplier role assignments list	Data	The service provider ensures that roles of, and relationships between, lead and sub-contracted suppliers are defined.
03-01	Audit objectives	Description	a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;6. The organization shall [conduct internal ISMS audits to] determine whether the ISMS:a) conform to the requirements of this International Standard and relevant legislation or regulations;c) are effectively implemented and maintained; and d) perform as expected. Information systems shall be [regularly] reviewed for compliance with the organization's information security policies and standards.
03-02	Corrective action change proposal	Description	Corrective actions shall be appropriate to the effects of the nonconformities encountered.
03-03	Improvement opportunity	Description	An improvement opportunity before it is recorded an prioritised. Implied in 'The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.'
03-04	Improvement target	Description	Setting targets for improvements in quality, value, capabilities, costs, productivity, resource utilization or risk reduction as appropriate.
03-05	Information asset control objective	Description	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, [documented and implemented.] Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified,] documented and implemented.
03-06	Information asset management roles and responsibilities	Description	Assets maintained in the inventory shall be owned.
03-07	Information publication status	Description	a) it is available and suitable for use, where and when it is needed; and c) distribution, access, retrieval and use;

Reference	Name	Category	Characteristics
03-08	Information security objectives	Description	The information security objectives shall: a) be consistent with the information security policy;b) be measurable (if practicable);c) take into account applicable information security requirements, and risk assessment and risk treatment results;d) be communicated; ande) be updated as appropriate. The information security objectives shall: e) be updated as appropriate. The organization shall retain documented information on the information security objectives.
03-09	ISMS Measurement information analysis roles and responsibilities	Description	f) who shall analyse and evaluate these results.
03-10	ISMS Measurement information gathering events	Description	c) when the monitoring and measuring shall be performed; e) when the results from monitoring and measurement shall be analyzed and evaluated; and
03-11	ISMS Measurement information gathering roles and responsibilities	Description	d) who shall monitor and measure;
03-12	ISMS Measurement information needs	Description	a) what needs to be monitored and measured, including information security processes and controls; The information security objectives shall: b) be measurable (if practicable);
03-13	ISMS Measurement methods	Description	b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
03-14	ISMS Roles and responsibilities	Description	All information security responsibilities shall be defined [and allocated.] Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.
03-15	Management review objectives	Description	The management review shall include consideration of: a) the status of actions from previous management reviews;b) changes in external and internal issues that are relevant to the information security management system;c) feedback on the information security performance, including trends in:1) nonconformities and corrective actions;2) monitoring and measurement results;3) audit results; and 4) fulfilment of information security objectives;d) feedback from interested parties;e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement.

Reference	Name	Category	Characteristics
03-16	Management system (ISMS) scope	Description	The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1;b) the requirements referred to in 4.2; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.4.3.1 The ISMS documentation shall include: b) the scope of the ISMS (see 4.2.1 a);
03-17	Management system strategy: documentation	Description	The organization's information security management system shall include:a) documented information required by this International Standard; andb) documented information determined by the organization as being necessary for the effectiveness of the information security management system. Documented information required by the information security management system and by this International Standard shall be controlled. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
03-18	Management system strategy: Establish	Description	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.
03-19	Management system strategy: external and internal issues	Description	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.
03-20	Management system strategy: improvement	Description	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.
03-21	Management system strategy: information security objectives	Description	The organization shall establish information security objectives at relevant functions and levels.

Reference	Name	Category	Characteristics
03-22	Management system strategy: management commitment	Description	Top management shall demonstrate leadership and commitment with respect to the information security management system by:a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;b) ensuring the integration of the information security management system requirements into the organization's processes;c) ensuring that the resources needed for the information security management system are available;d) communicating the importance of effective information security management and of conforming to the information security management system requirements;e) ensuring that the information security management system achieves its intended outcome(s);f) directing and supporting persons to contribute to the effectiveness of the information security management system;g) promoting continual improvement; andh) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
03-23	Management system strategy: outsourcing	Description	The organization shall ensure that outsourced processes are determined and controlled.
03-24	Management system strategy: privacy	Description	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
03-25	Management system strategy: processes	Description	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.
03-26	Management system strategy: roles and responsibilities	Description	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for:a) ensuring that the information security management system conforms to the requirements of this International Standard; andb) reporting on the performance of the information security management system to top management.
03-27	MS Interested parties	Description	The organization shall determine: a) interested parties that are relevant to the information security management system;
03-28	Process measures	Description	..the organization shall determine: j) how the results will be evaluated.
03-29	Process objectives	Description	..the organization shall determine: f) what will be done;
03-30	Process resource needs	Description	..the organization shall determine: g) what resources will be required;

Reference	Name	Category	Characteristics
03-31	Process roles and responsibilities	Description	..the organization shall determine: h) who will be responsible; Management responsibilities [and procedures] shall be established to ensure a quick, effective, and orderly response to information security incidents.
03-32	Process schedule	Description	..the organization shall determine: i) when it will be completed; and
03-33	Project/service measures	Description	Implied in 'When planning how to achieve its XXX objectives, the organization shall determine: — how the results will be evaluated.'
03-34	Release acceptance test criteria	Description	Implied in the release is deployed into the live environment so that the integrity of hardware, software and other service components is maintained during deployment of the release.
03-35	Release notes	Description	Notes regarding a release. Purpose of Release Notes; Release Scope; Release Contents; Release Installation / Rollback Procedure; References.
03-36	Risk and opportunity identification criteria	Description	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:a) ensure the information security management system can achieve its intended outcome(s);b) prevent, or reduce, undesired effects; andc) achieve continual improvement.
03-37	Risk assessment process description	Description	The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; The organization shall retain documented information about the information security risk assessment process.

Reference	Name	Category	Characteristics
03-38	Risk identification	Description	When planning for the information security management system, the organization shall [consider the issues referred to in 4.1 and the requirements referred to in 4.2 and] determine the risks and opportunities that need to be addressed to:a) ensure the information security management system can achieve its intended outcome(s);b) prevent, or reduce, undesired effects; andc) achieve continual improvement. c) identifies the information security risks:1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and2) identify the risk owners; The organization shall perform information security risk assessments [at planned intervals or when significant changes are proposed or occur,] taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments
03-39	Risk treatment process description	Description	The organization shall define [and apply] an information security risk treatment process to:a) select appropriate information security risk treatment options, taking account of the risk assessment results;b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;e) formulate an information security risk treatment plan; andf) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.
03-40	Sub-contracted supplier roles and responsibilities	Description	The service provider ensures that roles of, and relationships between, lead and sub-contracted suppliers [are documented].
03-41	Termination of employment roles and responsibilities	Description	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

Reference	Name	Category	Characteristics
04-01	Audit (ISMS) schedule	Plan	[The organization shall conduct internal audits] at planned intervals [to provide information on whether the information security management system:] [The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently] at planned intervals [or when significant changes occur.] Organizations shall regularly [monitor, review and audit supplier service delivery.]
04-02	Audit plan	Plan	d) define the audit criteria and scope for each audit;
04-03	Audit programme plan	Plan	The organization shall: c) plan, establish, [implement and maintain] an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
04-04	Capacity plan	Plan	A [documented] capacity management plan should be considered for mission critical systems. The service provider creates a capacity plan taking into consideration human, technical, information and financial resources.
04-05	Change schedule	Plan	A schedule of change containing details of the approved changes and their proposed deployment dates is established. The schedule of change shall be used as the basis for planning the deployment of releases.
04-06	Data backup test schedule	Plan	[Back-up copies of information and software shall be taken and tested] regularly in accordance with the agreed backup policy.
04-07	Improvement implementation schedule	Plan	The schedule of planned, approved, improvements.
04-08	Information security control verification schedule	Plan	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
04-09	Information system compliance review schedule	Plan	Information systems shall be regularly [reviewed] for compliance with the organization's information security policies and standards.

Reference	Name	Category	Characteristics
04-10	ISMS Policy review schedule	Plan	The policies for information security [shall be reviewed] at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.A5.1.2 [The information security policy shall be reviewed] at planned intervals [or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.]
04-11	Management review schedule	Plan	Top management shall review [the organization's information security management system] at planned intervals [to ensure its continuing suitability, adequacy and effectiveness.]
04-12	Product /service process lifecycle model	Plan	Information security shall be addressed in project management, regardless of the type of the project. Principles for engineering secure systems shall be established, [documented, maintained] and applied to any information system implementation efforts. Principles for engineering secure systems shall be [established,] documented, [maintained and applied to any information system implementation efforts.] Principles for engineering secure systems shall be [established, documented,] maintained [and applied to any information system implementation efforts.] Testing of security functionality shall be carried out during development.
04-13	Resources budget	Plan	The organization shall determine [and provide] the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
04-14	Risk management plan	Plan	The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.
04-15	Risk treatment plan	Plan	e) formulate an information security risk treatment plan; The organization shall retain documented information of the results of the information security risk treatment.
04-16	Security policies compliance review schedule	Plan	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
04-17	Service availability plan	Plan	The availability plan(s) shall include at least availability requirements and targets.

Reference	Name	Category	Characteristics
04-18	Service continuity plan	Plan	The service provider creates a service continuity plan(s).
04-19	User access rights review schedule	Plan	Asset owners [shall review users' access rights] at regular intervals.
05-01	Clear desk policy	Policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities [shall be adopted.]
05-02	Cryptographic controls usage policy	Policy	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
05-03	Cryptographic key protection and usage policy	Policy	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
05-04	Data backup policy	Policy	[Back-up copies of information and software shall be taken and tested] regularly in accordance with the agreed backup policy.
05-05	Improvement policy	Policy	There is a policy on continual improvement of the MS and the products/services.
05-06	Information system access policy	Policy	An access control policy shall be established, [documented and reviewed based on business and information security requirements.] An access control policy shall be [established,] documented [and reviewed based on business and information security requirements].
05-07	Information transfer policy	Policy	Formal transfer policies, [procedures and controls] shall be in place to protect the transfer of information through the use of all types of communication facilities.
05-08	Management system (ISMS) policy	Policy	Top management shall establish an information security policy that:a) is appropriate to the purpose of the organization;b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;c) includes a commitment to satisfy applicable requirements related to information security; andd) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; The information security policy shall: g) be available to interested parties, as appropriate. A set of policies for information security shall be defined, [approved by management, published and communicated to employees and relevant external parties.] A set of policies for information security shall be [defined, approved by management], published [and communicated to employees and relevant external parties.]

Reference	Name	Category	Characteristics
05-09	Mobile device policy	Policy	A policy and supporting security measures [shall be adopted to manage the risks introduced by using mobile devices.]
05-10	Secure development policy	Policy	Rules for the development of software and systems shall be established and applied to developments within the organization.
05-11	Software installation by users policy	Policy	Rules governing the installation of software by users shall be established and implemented.
05-12	Supplier relationship information security policy	Policy	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets [shall be agreed with the supplier and documented.] Information security requirements [for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and] documented.
05-13	Teleworking policy	Policy	A policy [and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.
06-01	Asset management procedure	Procedure	Procedures for handling assets shall be developed [and implemented] in accordance with the information classification scheme adopted by the organization.
06-02	Business continuity procedure	Procedure	The organization shall establish, [document], implement [and maintain] processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. The organization shall [establish,] document, [implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.] The organization shall [establish, document, implement and] maintain [processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.]
06-03	Change control procedure	Procedure	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
06-04	Equipment offsite management procedure	Procedure	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
06-05	Evidence collection and preservation procedure	Procedure	The organization shall define [and apply] procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. [The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information], which can serve as evidence.

Reference	Name	Category	Characteristics
06-06	Improvement procedure	Procedure	There is a procedure including the authorities and responsibilities for identifying, documenting, evaluating, approving, prioritizing, managing, measuring and reporting of improvements.
06-07	Information labelling, handling and storage procedure	Procedure	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
06-08	Information security incident response procedure	Procedure	[Management responsibilities] and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
06-09	Information transfer procedure	Procedure	Formal transfer [policies], procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
06-10	Operating Procedures	Procedure	Operating procedures [shall be documented and made available to all users who need them.] [Operating procedures] shall be documented [and made available to all users who need them.] [Operating procedures shall be documented] and made available to all users who need them.
06-11	Protection of intellectual property rights procedure	Procedure	Appropriate procedures [shall be implemented] to ensure compliance (IPR) with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
06-12	Removable media management procedure	Procedure	Procedures [shall be implemented] for the management of removable media in accordance with the classification scheme adopted by the organization. Procedures shall be implemented [for the management of removable media in accordance with the classification scheme adopted by the organization.] Media [shall be disposed of securely when no longer required], using formal procedures.
06-13	Secure area operating procedure	Procedure	Procedures for working in secure areas shall be designed [and applied.]
06-14	Security incident management procedure	Procedure	Information security incidents shall be responded to in accordance with the [documented] procedures. Information security incidents [shall be responded to in accordance with the] documented [procedures.]
06-15	Software installation procedure	Procedure	Procedures shall be implemented to control the installation of software on operational systems.
06-16	Teleworking procedure	Procedure	A [policy] and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Reference	Name	Category	Characteristics
06-17	User authentication information control procedure	Procedure	A formal user registration and de-registration process shall be implemented to enable assignment of access rights. The allocation of secret authentication information [shall be controlled] through a formal management process.
07-1	Release package	Product	A product/ service/ system assembled as a release.
08-01	Audit (ISMS) log	Record	The organization shall conduct internal audits. g) retain [documented] information as evidence of the audit programme(s) and the audit results. g) retain documented [information as evidence of the audit programme(s) and the audit results.]
08-02	Audit log	Record	e) [select auditors and conduct audits that] ensure objectivity and the impartiality of the audit process.
08-03	Audit result communication record	Record	f) ensure that the results of the audits are reported to relevant management; and
08-04	Auditor list	Record	e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
08-05	Business continuity plan test result	Record	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
08-06	Change request approval record	Record	Approved changes are developed and tested.
08-07	Change request record	Record	Information content related to all aspects of information captured in relation to a change request.
08-08	Code validity confirmation record	Record	Networks shall be managed and controlled to protect information in systems and applications.
08-09	Configuration item archive	Record	A configuration baseline of the affected CIs is taken before deployment of a release into the live environment. Master copies of CIs recorded in the CMDB shall be stored in secure physical or electronic libraries referenced by the configuration records. This includes at least documentation, licence information, software and, where available, images of the hardware configuration.
08-10	Configuration item change log	Record	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

Reference	Name	Category	Characteristics
08-11	Configuration item record	Record	The information recorded for each CI ensures effective control and include at least: a) description of the CI; b) relationship(s) between the CI and other CIs; c) relationship(s) between the CI and service components; d) status; e) version; f) location; g) associated requests for change; h) associated problems and known errors. 9.1 4 CIs shall be uniquely identified [and recorded in a CMDB.]
08-12	Correction action log	Record	b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity;
08-13	Corrective action change proposal approval record	Record	c) implement any action needed;2ED e) make changes to the information security management system, if necessary.
08-14	Corrective action record	Record	The organization shall retain documented information as evidence of:f) the nature of the nonconformities and any subsequent actions taken, andg) the results of any corrective action.
08-15	Corrective action request root cause analysis result	Record	2) determining the causes of the nonconformity; and 3) determining if similarnonconformities exist, or could potentially occur;
08-16	Corrective action verification record	Record	d) review the effectiveness of any corrective action taken;
08-17	Cryptographic controls application review log	Record	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
08-18	Data backup log	Record	Back-up copies of information and software shall be taken [and tested] regularly in accordance with the agreed backup policy.
08-19	Data removal verification record	Record	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
08-20	Data restore log	Record	[Back-up copies of information and software shall be taken] and tested regularly in accordance with the agreed backup policy.
08-21	Electronic messaging scan log	Record	Information involved in electronic messaging shall be appropriately protected.
08-22	Electronic transactions security volations log	Record	Event logs recording user activities, exceptions, faults and information security events shall be produced, [kept and regularly reviewed.] Event logs recording user activities, exceptions, faults and information security events shall be [produced,] kept [and regularly reviewed]. Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Reference	Name	Category	Characteristics
08-23	Electronic transactions security volations log review record	Record	Event logs recording user activities, exceptions, faults and information security events shall be [produced, kept and] regularly reviewed.
08-24	Employee access rights removal record	Record	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
08-25	Employee disciplinary action record	Record	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
08-26	Employee security performance appraisal record	Record	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
08-27	Employee terms and conditions approval record	Record	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security. Users shall be required to follow the organization's practices in the use of secret authentication information.
08-28	Employment candidate screening review result	Record	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
08-29	Equipment removal approval record	Record	Equipment, information or software shall not be taken off-site without prior authorization.
08-30	Improvement opportunity evaluation result	Record	Recorded opportunities for improvement are evaluated against agreed criteria for approval.
08-31	Improvement opportunity record	Record	Opportunities for improvement, including corrective and preventive actions, are documented.
08-32	Information archive log	Record	d) storage and preservation, including the preservation of legibility;
08-33	Information asset classification record	Record	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
08-34	Information disposition record	Record	f) retention and disposition.
08-35	Information integrity verification record	Record	b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). A.18.1.3 Records shall be protected from loss, destruction, falsification, unauthorizedaccess and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements
08-36	Information status record	Record	e) control of changes (e.g. version control); and

Reference	Name	Category	Characteristics
08-37	Information system access request approval record	Record	Users shall only be provided with access to the network and network services that they have been specifically authorized to use. The allocation and use of privileged access rights shall be restricted and controlled. [System administrator and system operator activities shall be logged] and the logs protected [and regularly reviewed.]
08-38	Information system changes security impact evaluation result	Record	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
08-39	ISMS Implementation log	Record	The organization shall [define and] apply an information security risk treatment process to.. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall implement the information security risk treatment plan. b) is effectively implemented [and maintained]. c) [plan, establish,] implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. A [policy] and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified, documented and] implemented. An appropriate set of procedures for information labelling shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization. Procedures for handling assets shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization. Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Reference	Name	Category	Characteristics
			A formal user registration and de-registration process shall be implemented to enable assignment of access rights. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. The allocation of secret authentication information shall be controlled [through a formal management process.]. A policy on the use of cryptographic controls for protection of information shall be [developed and] implemented. A policy on the use, protection and lifetime of cryptographic keys shall be [developed and] implemented through their whole lifecycle. Procedures for working in secure areas shall be [designed and] applied. A clear desk policy [for papers and removable storage media and a clear screen policy for information processing facilities] shall be adopted. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. Procedures shall be implemented to control the installation of software on operational systems. Rules governing the installation of software by users shall be [established and] implemented. The organization shall [establish, document], implement [and maintain] processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
08-40	ISMS Implementation review record	Record	The organization shall [control planned changes] and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. b) is [effectively implemented] and maintained. The policies for information security shall be reviewed [at planned intervals] or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness An access control policy shall be [established, documented and] reviewed based on business and information security requirements.

Reference	Name	Category	Characteristics
			Audit requirements and activities involving verification of operational systems shall be [carefully planned and] agreed to minimise disruptions to business processes. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be [identified, regularly] reviewed [and documented.] When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. The organization shall supervise and monitor the activity of outsourced system development. Organizations shall regularly monitor, review [and audit] supplier service delivery. The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. [The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently] at planned intervals [or when significant changes occur.] Managers shall [regularly] review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Information systems shall be [regularly] reviewed for compliance with the organization's information security policies and standards. The XXX objectives shall: d) be monitored; The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by: — implementing control of the processes in accordance with the criteria;
08-41	ISMS Measurement information results	Record	The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.
08-42	ISMS Policy approval record	Record	A set of policies for information security shall be [defined,] approved by management, [published and communicated to employees and relevant external parties.]
08-43	Logical access control log	Record	System administrator and system operator activities shall be logged [and the logs protected and regularly reviewed.] Access to operating systems shall be controlled by a secure log-on procedure.

Reference	Name	Category	Characteristics
08-44	Management review action log	Record	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
08-45	Management review record	Record	The organization shall retain documented information as evidence of the results of management reviews.
08-46	Management review result	Record	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
08-47	MS Resources provision record	Record	The organization shall [determine and] provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
08-48	New or changed service request record	Record	A record of a requests for change.
08-49	Non-conformity disposition record	Record	a) react to the nonconformity, and as applicable:1) take action to control and correct it; and2) deal with the consequences
08-50	Non-conformity record	Record	When a nonconformity occurs,
08-51	Personnel competency records	Record	d) retain appropriate documented information as evidence of competence.
08-52	Portable electronic media control log	Record	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. c) all media should be stored in a safe, secure environment, in accordance withmanufacturers' specifications;
08-53	Process change request review record	Record	The organization shall [control planned changes and] review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.]
08-54	Process change review record	Record	The organization shall [control planned changes and] review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
08-55	Removable media disposition record	Record	Media shall be disposed of securely when no longer required, [using formal procedures.] a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;
08-56	Residual risk approval record	Record	f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

Reference	Name	Category	Characteristics
08-57	Return of assets confirmation record	Record	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
08-58	Risk assessment action schedule	Record	[The organization shall perform information security risk assessments] at planned intervals or when significant changes are proposed or occur, [taking account of the criteria established in 6.1.2 a).]
08-59	Risk assessment process effectiveness evaluation result	Record	b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
08-60	Risk assessment review record	Record	e) evaluates the information security risks:1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and2) prioritise the analysed risks for risk treatment.
08-61	Roles and responsibilities assignment record	Record	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned [and communicated.] All information security responsibilities shall be [defined and] allocated.
08-62	Security incident disposition record	Record	Information security incidents shall be responded to [in accordance with the documented procedures.]
08-63	Security incident impact evaluation result	Record	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
08-64	Security incident request record	Record	Information security events shall be reported through appropriate management channels as quickly as possible. All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
08-65	Security vulnerability scan log	Record	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
08-66	Service availability plan test result review record	Record	Unplanned non-availability is investigated.
08-67	Supplier agreement review record	Record	A record of the review conducted to determine that contractual obligations are being met and that the contract reflects current requirements.
08-68	Supplier capability assessment record	Record	Record of action taken by the service provider verify that lead suppliers are managing their sub-contracted suppliers to fulfil contractual obligations.

Reference	Name	Category	Characteristics
08-69	Supplier services change request evaluation record	Record	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
08-70	System activity log review record	Record	[System administrator and system operator activities shall be logged and the logs protected] and regularly reviewed.
08-71	Test data change log	Record	Test data shall be selected carefully, and protected and controlled.
08-72	Training effectiveness evaluation result	Record	c) where applicable, [take actions to acquire the necessary competence, and] evaluate the effectiveness of the actions taken;
08-73	Training provision action log	Record	c) where applicable, take actions to acquire the necessary competence, [and evaluate the effectiveness of the actions taken;]
08-74	Training record	Record	b) ensure that these persons are competent on the basis of appropriate education, training, or experience; All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. Persons doing work under the organization's control shall be aware of: a) the information security policy;b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; andc) the implications of not conforming with the information security management system requirements.
08-75	User access rights review record	Record	Asset owners shall review users' access rights [at regular intervals.] Access to program source code shall be restricted.
08-76	Work environment access control log	Record	Security perimeters shall be [defined and] used to protect areas that contain either sensitive or critical information and information processing facilities. Physical security for offices, rooms, and facilities shall be [designed and] applied. Physical protection against natural disasters, malicious attack or accidents shall be [designed and] applied. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Reference	Name	Category	Characteristics
09-01	Audit result	Report	[The organization shall: g) retain documented information as evidence of the audit programme(s) and] the audit results.
09-02	Capacity future needs assessment report	Report	The capacity plan refers forecast demand for services.
09-03	Capacity usage analysis	Report	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
09-04	Change request evaluation report	Report	Implied in requests for change are assessed using information from the change management process and other processes.
09-05	Configuration item audit report	Report	The service provider audits the records stored in the CMDB, [at planned intervals.]
09-06	Configuration item status report	Report	The information recorded for each CI ensures effective control and include at least: a) description of the CI; b) relationship(s) between the CI and other CIs; c) relationship(s) between the CI and service components; d) status; e) version; f) location; g) associated requests for change; h) associated problems and known errors.
09-07	Information security audit report	Report	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
09-08	Information security incident report	Report	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. [The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information], which can serve as evidence.
09-09	Information system security compliance audit report	Report	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Reference	Name	Category	Characteristics
09-10	ISMS Communication records	Report	d) communicating the importance of effective information security management and of conforming to the information security management system requirements; The information security policy shall: f) be communicated within the organization; Top management shall ensure that the responsibilities and authorities for roles relevant to information security are [assigned and] communicated. The information security objectives shall be: d) be communicated; and A set of policies for information security shall be [defined, approved by management, published and] communicated to employees and relevant external parties. There shall be a [formal and] communicated disciplinary process in place to take action against employees who have committed an information security breach. Information security responsibilities and duties that remain valid after termination or change of employment shall be [defined,] communicated to the employee or contractor and enforced.
09-11	ISMS Implementation audit report	Report	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently [at planned intervals or when significant changes occur.]
09-12	ISMS measurement information analysis report	Report	The organization shall evaluate the information security performance and the effectiveness of the information security management system.
09-13	Logical access system attack report	Report	Logging facilities and log information shall be protected against tampering and unauthorized access.
09-14	New or changed service evaluation report	Report	A report of an evaluation against the criteria in the Change Management Policy that identifies criteria to determine changes with potential to have a major impact on services or the customer.
09-15	Release acceptance test report	Report	The release is verified against the agreed acceptance criteria.
09-16	Risk analysis report	Report	d) analyses the information security risks:1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and3) determine the levels of risk;
09-17	Service availability analysis report	Report	Availability of services is monitored, the results recorded and compared with agreed targets.
09-18	Service availability plan test report	Report	The results of the tests are reported.

Reference	Name	Category	Characteristics
09-19	Service continuity plan test report	Report	The results of tests are reported.
09-20	Service continuity plan test result finding report	Report	Where deficiencies are found during the test, the service provider takes necessary actions.
09-21	Supplier performance evaluation report	Report	The result of actions taken by the service provider to monitor performance of the supplier against service targets and other contractual obligations.
09-22	Supplier surveillance report	Report	Organizations shall regularly [monitor, review and] audit supplier service delivery.
11-1	Capacity plan change request	Request	Changes to the capacity plan are controlled by the change management process.
11-2	Data recovery request	Request	A request for recovery of data.
11-3	Improvement opportunity approval request	Request	<no defined content requirements>
11-4	Process change request	Request	The organization shall control planned changes [and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.] Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
11-5	Service availability plan change request	Request	Request for change on the service availability plan(s).
11-6	Service continuity plan change request	Request	Request for change on the service continuity plan(s).
12-01	Business continuity requirements	Specification	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. The service continuity requirements include at least: a) access rights to the services; b) service response times; c) end to end availability of services.
12-02	Capacity requirements	Specification	The result of an assessment based on customer needs.

Reference	Name	Category	Characteristics
12-03	Communication requirements	Specification	(a) The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; (b) The organization shall determine the need for internal and external communications relevant to the information security management system including: b) when to communicate; (c) The organization shall determine the need for internal and external communications relevant to the information security management system including: c) with whom to communicate; (d) The organization shall determine the need for internal and external communications relevant to the information security management system including: d) who shall communicate; (e) The organization shall determine the need for internal and external communications relevant to the information security management system including: e) the processes by which communication shall be effected.
12-04	Confidentiality requirements	Specification	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, [regularly reviewed and documented.] Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be [identified, regularly reviewed and] documented.
12-05	Contractual requirements	Specification	All relevant [legislative statutory, regulatory,] contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, [documented and kept up to date for each information system and the organization.] All relevant [legislative statutory, regulatory], contractual requirements and the organization's approach to meet these requirements shall be [explicitly identified,] documented [and kept up to date for each information system and the organization.] All relevant [legislative statutory, regulatory], contractual requirements and the organization's approach to meet these requirements shall be [explicitly identified, documented and] kept up to date for each information system and the organization.
12-06	Criteria for performing risk assessments	Specification	a) 2) criteria for performing information security risk assessments;
12-07	Data backup requirements	Specification	The backup requirements are identified e.g. files, folders, and drives to be backed up.

Reference	Name	Category	Characteristics
12-08	Equipment environment requirements	Specification	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage. Users shall ensure that unattended equipment has appropriate protection.
12-09	Equipment maintenance requirements	Specification	Equipment shall be correctly maintained to ensure its continued availability and integrity.
12-10	Improvement opportunity evaluation criteria	Specification	Record of opportunities for improvement are evaluated against agreed criteria for approval.
12-11	Information asset classification schema	Specification	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
12-12	Information infrastructure requirements	Specification	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source. Groups of information services, users, and information systems shall be segregated on networks.' Access to information and application system functions shall be restricted in accordance with the access control policy. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Reference	Name	Category	Characteristics
12-13	Information item management requirements	Specification	(a) When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); (b) When creating and updating documented information the organization shall ensure appropriate: b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); (c) When creating and updating documented information the organization shall ensure appropriate: c) review [and approval] for suitability and adequacy. (c) When creating and updating documented information the organization shall ensure appropriate: c) [review and] approval for suitability and adequacy.
12-14	Information management requirements	Specification	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall beidentified as appropriate, and controlled.
12-15	MS Interested parties MS expectations	Specification	The organization shall determine: b) the requirements of these interested parties relevant to information security.
12-16	New or changed services - system security requirements	Specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
12-17	Organisational competence requirements	Specification	a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;
12-18	Process criteria	Specification	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by: — establishing criteria for the processes;
12-19	Process interface requirements	Specification	Appropriate contacts with relevant authorities shall be maintained.A6.1.6 Appropriate contacts with relevant authorities shall be maintained. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
12-20	Release acceptance test case	Specification	Implied in releases are built and tested prior to deployment.
12-21	Release requirements	Specification	Requirements for a release.
12-22	Risk acceptance criteria	Specification	a) 1) the risk acceptance criteria;

Reference	Name	Category	Characteristics
12-23	Service availability requirements	Specification	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. The agreed service continuity and availability requirements shall include at least: a) access rights to the services; b) service response times; c) end to end availability of services.
12-24	Statutory and regulatory requirements	Specification	All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be explicitly identified, [documented and kept up to date for each information system and the organization.] All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be [explicitly identified,] documented [and kept up to date for each information system and the organization.] All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be [explicitly identified, documented and] kept up to date for each information system and the organization.
12-25	System acceptance criteria	Specification	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
12-26	User password system requirements	Specification	Password management systems shall be interactive and shall ensure quality passwords.
12-27	Work environment structure requirements	Specification	Security perimeters shall be defined [and used] to protect areas that contain either sensitive or critical information and information processing facilities. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Physical security for offices, rooms, and facilities shall be designed [and applied]. Physical protection against natural disasters, malicious attack or accidents shall be designed [and applied].

Annex C
(informative)

Association between base practices and ISO/IEC 27001 requirements

This International Standard provides a Process Assessment Model for assessing the process capability of processes associated with a information security management (ISMS). ISO/IEC 27001 provides requirements for the establishment of an ISMS System. This Annex identifies a Process Capability Profile (Level 1) that is implied by the requirements associated with a Management System conformant to ISO/IEC 27001.

C.1 Associations of base practices with requirements

The following table identifies each base practice with the associated singular requirements from ISO/IEC 27001, and the implied information item.

NOTE Not all the base practices identified in Section 5 will correspond to an entry in Table C.1. Table C.3 identifies the base practices associated with outcomes that were added to the PRM in order to represent well-formed processes.

Table C.1 — Association of base practices with singular requirements of ISO/IEC 27001

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
ORG.1 Asset management				
ORG.1.BP.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	A.08.1.1.1	Assets associated with information and information processing facilities shall be identified [and an inventory of these assets shall be drawn up and maintained.]	02-01 Asset register
ORG.1.BP.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	A.08.1.1.1	Assets associated with information and information processing facilities shall be identified [and an inventory of these assets shall be drawn up and maintained.]	02-05 Information asset register
ORG.1.BP.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.	A.08.2.1.1	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	08-33 Information asset classification record
ORG.1.BP.3	**Inventory the assets** Assemble an inventory of the information security related assets.	A.08.1.1.2	[Assets associated with information and information processing facilities shall be identified] and an inventory of these assets shall be drawn up [and maintained.]	02-05 Information asset register
ORG.1.BP.5	**Manage asset item changes** Manage changes to asset items.	A.08.1.1.3	[Assets associated with information and information processing facilities shall be identified] and an inventory of these assets shall be drawn up] and maintained.	02-05 Information asset register
ORG.1.BP.5	**Manage asset item changes** Manage changes to asset items.	A.08.3.2.2	Media shall be disposed of securely when no longer required, [using formal procedures.]	08-55 Removable media disposition record
ORG.1.BP.5	**Manage asset item changes** Manage changes to asset items.	A.08.3.3.1	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	08-52 Portable electronic media control log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TEC.01 Capacity management				
TEC.01.BP.3	**Monitor capacity usage** Monitor, analyse and performance tune capacity usage.	A.12.1.3.1	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	09-03 Capacity usage analysis
TEC.02 Change management				
TEC.02.BP.2	**Analyse change requests** Analyse and assess change requests using defined criteria.	A.15.2.2.1	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	08-69 Supplier services change request evaluation record
COM.01 Communication management				
COM.01.BP.1	**Define information content** Define information content in terms of identified communication needs and requirements.	07.4.1	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate;	12-03 Communication requirements
COM.01.BP.2	**Identify parties to communicate to** Identify parties to communicate with.	07.4.3	The organization shall determine the need for internal and external communications relevant to the information security management system including: c) with whom to communicate;	12-03 Communication requirements
COM.01.BP.2	**Identify parties to communicate to** Identify parties to communicate with.	A.06.1.3.1	Appropriate contacts with relevant authorities shall be maintained.	12-19 Process interface requirements
COM.01.BP.2	**Identify parties to communicate to** Identify parties to communicate with.	A.06.1.4.1	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	12-19 Process interface requirements
COM.01.BP.3	**Identify party responsible for communication** Identify the party responsible for the communication.	07.4.4	The organization shall determine the need for internal and external communications relevant to the information security management system including: d) who shall communicate;	12-03 Communication requirements
COM.01.BP.4	**Identify communication events** Identify the events that require comminication actions.	07.4.2	The organization shall determine the need for internal and external communications relevant to the information security management system including: b) when to communicate;	12-03 Communication requirements
COM.01.BP.5	**Select communication channel** Select the channel for the communication.	07.4.5	The organization shall determine the need for internal and external communications relevant to the information security management system including: e) the processes by which communication shall be effected.	12-03 Communication requirements
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	05.1.2	Top management shall demonstrate leadership and commitment with respect to the information security management system by: d) communicating the importance of effective information security management and of conforming to the information security management system requirements;	09-10 ISMS Communication records

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	05.2.3	The information security policy shall: f) be communicated within the organization;	09-10 ISMS Communication records
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	05.3.2	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are [assigned and] communicated.	09-10 ISMS Communication records
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	06.2.4	The information security objectives shall: d) be communicated;	09-10 ISMS Communication records
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	09.2.11	The organization shall: f) ensure that the results of the audits are reported to relevant management; and	08-03 Audit result communication record
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	A.05.1.1.4	A set of policies for information security shall be [defined, approved by management, published and] communicated to employees and relevant external parties.	09-10 ISMS Communication records
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	A.07.2.3.2	There shall be a [formal and] communicated disciplinary process in place to take action against employees who have committed an information security breach.	09-10 ISMS Communication records
COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	A.07.3.1.2	Information security responsibilities and duties that remain valid after termination or change of employment shall be [defined,] communicated to the employee or contractor and enforced.	09-10 ISMS Communication records
TEC.03 Configuration management				
TEC.03.BP.3	**Manage changes to configuration items** Control changes to items under configuration management.	A.14.2.4.1	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	08-10 Configuration item change log
TEC.03.BP.3	**Manage changes to configuration items** Control changes to items under configuration management.	A.14.3.1.1	Test data shall be selected carefully, protected and controlled.	08-71 Test data change log
COM.02 Documentation management				
COM.02.BP.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.	04.3.3	The scope shall be available as documented information.	03-16 Management system (ISMS) scope
COM.02.BP.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.	05.2.2	The information security policy shall: e) be available as documented information;	05-08 Management system (ISMS) policy
COM.02.BP.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.	06.1.2.9	The organization shall retain documented information about the information security risk assessment process.	03-37 Risk assessment process description

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	06.1.3.5	The organization shall retain documented information about the information security risk treatment process	03-39 Risk treatment process description
COM.02.BP.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.	06.2.6	The organization shall retain documented information on the information security objectives.	03-08 Information security objectives
COM.02.BP.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.	07.2.5	The organization shall: d) retain appropriate documented information as evidence of competence.	08-51 Personnel competency records
COM.02.BP.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.	08.1.3	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	03-17 Management system strategy: documentation
COM.02.BP.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.	08.2.3	The organization shall retain documented information of the results of the information security risk assessments.	03-38 Risk identification
COM.02.BP.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.	08.3.2	The organization shall retain documented information of the results of the information security risk treatment.	04-15 Risk treatment plan
COM.02.BP.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.	09.1.8	The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	08-41 ISMS Measurement information results
COM.02.BP.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.	09.2.13	[The organization shall: g) retain] documented [information as evidence [of the audit programme(s) and the audit results.]	08-01 Audit (ISMS) log
COM.02.BP.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.	09.3.5	The organization shall retain documented information as evidence of the results of management reviews.	08-45 Management review record
COM.02.BP.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.	10.1.9	The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.	08-14 Corrective action record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	A.08.1.3.2	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified,] documented [and implemented.]	03-05 Information asset control objective
COM.02.BP.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.	A.09.1.1.2	An access control policy shall be [established,] documented [and reviewed based on business and information security requirements].	05-06 Information system access policy
COM.02.BP.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.	A.12.1.1.2	[Operating procedures] shall be documented [and made available to all users who need them.]	06-10 Operating Procedures
COM.02.BP.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.	A.12.4.1.2	Event logs recording user activities, exceptions, faults and information security events shall be [produced,] kept [and regularly reviewed].	08-22 Electronic transactions security volations log
COM.02.BP.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.	A.13.2.4.3	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be [identified, regularly reviewed and] documented.	12-04 Confidentiality requirements
COM.02.BP.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.	A.14.2.5.2	Principles for engineering secure systems shall be [established,] documented,[maintained and applied to any information system implementation efforts.]	04-12 Product /service process lifecycle model
COM.02.BP.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.	A.15.1.1.3	Information security requirements [for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and] documented.	05-12 Supplier relationship information security policy
COM.02.BP.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.	A.16.1.5.2	Information security incidents shall be responded to in accordance with the [documented] procedures.	06-14 Security incident management procedure
COM.02.BP.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.	A.16.1.5.3	Information security incidents [shall be responded to in accordance with the] documented [procedures.]	06-14 Security incident management procedure
COM.02.BP.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.	A.16.1.7.1	[The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information], which can serve as evidence.	06-05 Evidence collection and preservation procedure

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	A.17.1.2.3	The organization shall [establish], document, [implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.]	06-02 Business continuity procedure
COM.02.BP.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.	A.18.1.1.01.2	All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be [explicitly identified,] documented [and kept up to date for each information system and the organization.]	12-24 Statutory and regulatory requirements
COM.02.BP.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.	A.18.1.1.02.2	All relevant [legislative statutory, regulatory], contractual requirements and the organization's approach to meet these requirements shall be [explicitly identified,] documented [and kept up to date for each information system and the organization.]	12-05 Contractual requirements
COM.02.BP.2	**The forms of documented information representation are defined.** Identify the forms of information to be stored in the repostory. For example, this may include documents, records, audio content, video content, image content.	07.5.2.1	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number);	12-13 Information item management requirements
COM.02.BP.2	**The forms of documented information representation are defined.** Identify the forms of information to be stored in the repostory. For example, this may include documents, records, audio content, video content, image content.	07.5.2.2	When creating and updating documented information the organization shall ensure appropriate: b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	12-13 Information item management requirements
COM.02.BP.2	**The forms of documented information representation are defined.** Identify the forms of information to be stored in the repostory. For example, this may include documents, records, audio content, video content, image content.	07.5.2.3	When creating and updating documented information the organization shall ensure appropriate: c) review [and approval] for suitability and adequacy.	12-13 Information item management requirements
COM.02.BP.2	**The forms of documented information representation are defined.** Identify the forms of information to be stored in the repostory. For example, this may include documents, records, audio content, video content, image content.	07.5.2.4	When creating and updating documented information the organization shall ensure appropriate: c) [review and] approval for suitability and adequacy.	12-13 Information item management requirements
COM.02.BP.2	**The forms of documented information representation are defined.** Identify the forms of information to be stored in the repostory. For example, this may include documents, records, audio content, video content, image content.	07.5.3.8	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	12-14 Information management requirements

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	06.2.5	The information security objectives shall: e) be updated as appropriate.	03-08 Information security objectives
COM.02.BP.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.	07.5.3.6	e) control of changes (e.g. version control); and	08-36 Information status record
COM.02.BP.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.	A.14.2.5.3	Principles for engineering secure systems shall be [established, documented,] maintained [and applied to any information system implementation efforts.]	04-12 Product /service process lifecycle model
COM.02.BP.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.	A.17.1.2.4	The organization shall [establish, document, implement and] maintain [processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.]	06-02 Business continuity procedure
COM.02.BP.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.	A.18.1.1.01.3	All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be [explicitly identified, documented and] kept up to date for each information system and the organization.	12-24 Statutory and regulatory requirements
COM.02.BP.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.	A.18.1.1.02.3	All relevant [legislative statutory, regulatory], contractual requirements and the organization's approach to meet these requirements shall be [explicitly identified, documented and] kept up to date for each information system and the organization.	12-05 Contractual requirements
COM.02.BP.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).	07.5.3.3	b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)	08-35 Information integrity verification record
COM.02.BP.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).	A.18.1.3.1	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	08-35 Information integrity verification record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	06.1.3.4	f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	08-56 Residual risk approval record
COM.02.BP.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.	A.05.1.1.2	A set of policies for information security shall be [defined,] approved by management, [published and communicated to employees and relevant external parties.]	08-42 ISMS Policy approval record
COM.02.BP.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.	A.15.1.1.2	Information security requirements [for mitigating the risks associated with supplier's access to the organization's assets] shall be agreed with the supplier [and documented.]	05-12 Supplier relationship information security policy
COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	05.2.4	The information security policy shall: g) be available to interested parties, as appropriate.	05-08 Management system (ISMS) policy
COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	07.5.3.2	a) it is available and suitable for use, where and when it is needed; and	03-07 Information publication status
COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	07.5.3.4	c) distribution, access, retrieval and use;	03-07 Information publication status
COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	A.05.1.1.3	A set of policies for information security shall be [defined, approved by management,] published [and communicated to employees and relevant external parties.]	05-08 Management system (ISMS) policy
COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	A.12.1.1.3	[Operating procedures shall be documented] and made available to all users who need them.	06-10 Operating Procedures

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	06.1.2.4	The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	08-39 ISMS Implementation log
COM.02.BP.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.	06.1.3.2	The organization shall [define and] apply an information security risk treatment process to..	08-39 ISMS Implementation log
COM.02.BP.7	**Archived, or disposed of documented information** Note: Records should be protected in accordance with statutory, regulatory, contractual and business requirements.	07.5.3.5	d) storage and preservation, including the preservation of legibility;	08-32 Information archive log
COM.02.BP.7	**Archived, or disposed of documented information** Note: Records should be protected in accordance with statutory, regulatory, contractual and business requirements.	07.5.3.7	f) retention and disposition.	08-34 Information disposition record
COM.02.BP.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.	08.1.2	The organization shall also implement plans to achieve information security objectives determined in 6.2.	08-39 ISMS Implementation log
COM.02.BP.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.	09.2.4	b) is effectively implemented [and maintained].	08-39 ISMS Implementation log
COM.02.BP.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.	09.2.7	The organization shall: c) [plan, establish,] implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.	08-39 ISMS Implementation log
COM.02.BP.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.	A.06.2.1.2	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	08-39 ISMS Implementation log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	A.06.2.2.3	A [policy and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.	08-39 ISMS Implementation log
COM.02.BP.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.	A.08.1.3.3	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified, documented and] implemented.	08-39 ISMS Implementation log
COM.02.BP.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.	A.08.2.2.2	An appropriate set of procedures for information labelling shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	08-39 ISMS Implementation log
COM.02.BP.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.	A.08.2.3.2	Procedures for handling assets shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	08-39 ISMS Implementation log
COM.02.BP.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.	A.08.3.1.2	[Procedures shall be] implemented [for the management of removable media in accordance with the classification scheme adopted by the organization.]	08-39 ISMS Implementation log
COM.02.BP.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.	A.09.2.1.2	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	08-39 ISMS Implementation log
COM.02.BP.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.	A.09.2.2.1	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	08-39 ISMS Implementation log
COM.02.BP.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.	A.09.2.4.2	[The allocation of secret authentication information] shall be controlled [through a formal management process.]	08-39 ISMS Implementation log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	A.10.1.1.2	A policy on the use of cryptographic controls for protection of information shall be [developed and] implemented.	08-39 ISMS Implementation log
COM.02.BP.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.	A.10.1.2.2	A policy on the use, protection and lifetime of cryptographic keys shall be [developed and] implemented through their whole lifecycle.	08-39 ISMS Implementation log
COM.02.BP.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.	A.11.1.5.2	Procedures for working in secure areas shall be [designed and] applied.	08-39 ISMS Implementation log
COM.02.BP.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.	A.11.2.9.2	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	08-39 ISMS Implementation log
COM.02.BP.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.	A.12.2.1.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	08-39 ISMS Implementation log
COM.02.BP.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.	A.12.5.1.2	Procedures shall be implemented to control the installation of software on operational systems.	08-39 ISMS Implementation log
COM.02.BP.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.	A.12.6.2.1	Rules governing the installation of software by users shall be [established and] implemented.	08-39 ISMS Implementation log
COM.02.BP.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.	A.17.1.2.2	The organization shall [establish, document], implement [and maintain] processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	08-39 ISMS Implementation log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.02.BP.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.	A.17.2.1.1	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	08-39 ISMS Implementation log
COM.02.BP.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.	A.18.1.2.2	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	08-39 ISMS Implementation log
ORG.2 Equipment management				
ORG.2.BP.1	**Site equipment** Site equipment to minimize risk of environmental or other damage.	A.11.2.1.1	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	12-08 Equipment environment requirements
ORG.2.BP.1	**Site equipment** Site equipment to minimize risk of environmental or other damage.	A.11.2.3.1	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	12-08 Equipment environment requirements
ORG.2.BP.2	**Assure continuity in service provision** Assure continuity in the provision of utilities and services to equipment.	A.11.2.2.1	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	12-08 Equipment environment requirements
ORG.2.BP.3	**Maintain equipment** Maintain equipment to ensure its continued availability and integrity.	A.11.2.4.1	Equipment shall be correctly maintained to ensure its continued availability and integrity.	12-09 Equipment maintenance requirements
ORG.2.BP.3	**Maintain equipment** Maintain equipment to ensure its continued availability and integrity.	A.13.1.1.1	Networks shall be managed and controlled to protect information in systems and applications.	08-08 Code validity confirmation record
ORG.2.BP.4	**Manage offsite equipment** Manage equipment used offsite to ensure integrity of operation.	A.11.2.6.1	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	06-04 Equipment offsite management procedure
ORG.2.BP.5	**Assure information integrity** Assure the integrity of information when equipment is withdrawn from service.	A.11.2.7.1	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	08-19 Data removal verification record
ORG.2.BP.6	**Control equipment relocation** Control equipment relocation.	A.11.2.5.1	Equipment, information or software shall not be taken off-site without prior authorization.	08-29 Equipment removal approval record
ORG.3 Human resource employment management				
ORG.3.BP.1	**Define roles and responsibilities of employees** Define roles and responsibilities of employees, contractors and third party users.	A.07.1.2.1	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	01-2 Employee agreement

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
ORG.3.BP.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.	A.07.1.1.1	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	08-28 Employment candidate screening review result
ORG.3.BP.3	**Confirm employee agreement** Confirm agreement of prospective employees to the terms and conditions of their employment contract.	A.07.1.2.1	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	08-27 Employee terms and conditions approval record
ORG.3.BP.3	**Confirm employee agreement** Confirm agreement of prospective employees to the terms and conditions of their employment contract.	A.09.3.1.1	Users shall be required to follow the organization's practices in the use of secret authentication information.	08-27 Employee terms and conditions approval record
ORG.3.BP.4	**Apply employment terms and conditions** Apply the terms and conditions of employment are applied.	A.07.2.1.1	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	08-26 Employee security performance appraisal record
ORG.3.BP.6	**Apply disciplinary measures** Apply disciplinary measures to employees that have committed a breech of the agreed conditions of employment.	A.07.2.3.1	There shall be a formal [and communicated] disciplinary process in place to take action against employees who have committed an information security breach.	08-25 Employee disciplinary action record
ORG.3.BP.7	**Manage employment termination** Define and assign responsibilities for performing employment termination or change of employment.	A.07.3.1.1	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, [communicated to the employee or contractor and enforced.]	03-41 Termination of employment roles and responsibilities
ORG.3.BP.8	**Return of assets** On termination of employment, employees return all of the organization's assets in their possession.	A.08.1.4.1	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	08-57 Return of assets confirmation record
ORG.3.BP.9	**Remove employee access to information resources** Remove employee access to information resources upon termination of their employment.	A.09.2.6.1	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	08-24 Employee access rights removal record
COM.03 Human resource management				
COM.03.BP.1	**Identify organisational competencies** Identify the competencies required by the organization.	07.2.1	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;	12-17 Organisational competence requirements
COM.03.BP.2	**Evaluate competence of personnel** Evaluate the competence of the personnel	07.2.2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	08-74 Training record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.03.BP.2	**Evaluate competence of personnel** Evaluate the competence of the personnel	07.3.1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	08-74 Training record
COM.03.BP.2	**Evaluate competence of personnel** Evaluate the competence of the personnel	A.07.2.2.1	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	08-74 Training record
COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	07.2.2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	08-74 Training record
COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	07.2.3	The organization shall: c) where applicable, take actions to acquire the necessary competence, [and evaluate the effectiveness of the actions taken; and]	08-73 Training provision action log
COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	07.3.1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	08-74 Training record
COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	A.07.2.2.1	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	08-74 Training record
COM.03.BP.4	**Demonstrate awareness of role** Each individual demonstrates their understanding of their role and activities in achieving organsational objectives.	07.2.2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	08-74 Training record
COM.03.BP.4	**Demonstrate awareness of role** Each individual demonstrates their understanding of their role and activities in achieving organsational objectives.	07.3.1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	08-74 Training record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.03.BP.4	**Demonstrate awareness of role** Each individual demonstrates their understanding of their role and activities in achieving organsational objectives.	A.07.2.2.1	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	08-74 Training record
COM.04 Improvement				
TEC.04 Incident management				
TEC.04.BP.1	**Record incidents** Record and classify incidents.	A.16.1.2.1	Information security events shall be reported through appropriate management channels as quickly as possible.	08-64 Security incident request record
TEC.04.BP.1	**Record incidents** Record and classify incidents.	A.16.1.3.1	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	08-64 Security incident request record
TEC.04.BP.2	**Analyse incidents** Prioritise and analyse incidents.	A.16.1.4.1	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	08-63 Security incident impact evaluation result
TEC.04.BP.3	**Resolve incidents** Resolve and close incidents.	A.16.1.5.1	Information security incidents shall be responded to [in accordance with the documented procedures.]	08-62 Security incident disposition record
ORG.4 Infrastructure and work environment				
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.11.1.1.1	Security perimeters shall be defined [and used] to protect areas that contain either sensitive or critical information and information processing facilities.	12-27 Work environment structure requirements
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.11.1.2.1	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	12-27 Work environment structure requirements
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.11.1.3.1	Physical security for offices, rooms and facilities shall be designed [and applied].	12-27 Work environment structure requirements
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.11.1.4.1	Physical protection against natural disasters, malicious attack or accidents shall be designed [and applied].	12-27 Work environment structure requirements
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.12.4.4.1	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	12-12 Information infrastructure requirements
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.13.1.2.1	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	12-12 Information infrastructure requirements

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
ORG.4.BP.1	**Define requirements** Define the requirements for infrastructure and work environment to support processes.	A.14.2.6.1	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	12-12 Information infrastructure requirements
ORG.4.BP.2	**Define access rights** Define access rights to the information resource.	A.09.4.1.1	Access to information and application system functions shall be restricted in accordance with the access control policy.	12-12 Information infrastructure requirements
ORG.4.BP.2	**Define access rights** Define access rights to the information resource.	A.12.1.4.1	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	12-12 Information infrastructure requirements
ORG.4.BP.2	**Define access rights** Define access rights to the information resource.	A.13.1.3.1	Groups of information services, users and information systems shall be segregated on networks.	12-12 Information infrastructure requirements
ORG.4.BP.5	**Maintain infrastructure and work environment** Control and maintain the infrastructure and work environment.	A.11.1.1.2	Security perimeters shall be [defined and] used to protect areas that contain either sensitive or critical information and information processing facilities.	08-76 Work environment access control log
ORG.4.BP.5	**Maintain infrastructure and work environment** Control and maintain the infrastructure and work environment.	A.11.1.3.2	Physical security for offices, rooms and facilities shall be [designed and] applied.	08-76 Work environment access control log
ORG.4.BP.5	**Maintain infrastructure and work environment** Control and maintain the infrastructure and work environment.	A.11.1.4.2	Physical protection against natural disasters, malicious attack or accidents shall be [designed and] applied.	08-76 Work environment access control log
ORG.4.BP.5	**Maintain infrastructure and work environment** Control and maintain the infrastructure and work environment.	A.11.1.6.1	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	08-76 Work environment access control log
ORG.4.BP.5	**Maintain infrastructure and work environment** Control and maintain the infrastructure and work environment.	A.11.2.8.1	Users shall ensure that unattended equipment has appropriate protection.	12-08 Equipment environment requirements
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.1.2.1	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	08-37 Information system access request approval record
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.2.3.1	The allocation and use of privileged access rights shall be restricted and controlled.	08-37 Information system access request approval record
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.2.5.1	Asset owners shall review users' access rights [at regular intervals.]	08-75 User access rights review record
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.4.2.1	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	08-43 Logical access control log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.4.3.1	Password management systems shall be interactive and shall ensure quality passwords.	12-26 User password system requirements
ORG.4.BP.6	**Control access** Control access to the information resource.	A.09.4.5.1	Access to program source code shall be restricted.	08-75 User access rights review record
ORG.4.BP.6	**Control access** Control access to the information resource.	A.12.4.3.1	System administrator and system operator activities shall be logged [and the logs protected and regularly reviewed.]	08-43 Logical access control log
ORG.4.BP.6	**Control access** Control access to the information resource.	A.12.4.3.2	[System administrator and system operator activities shall be logged] and the logs protected [and regularly reviewed.]	08-37 Information system access request approval record
ORG.4.BP.6	**Control access** Control access to the information resource.	A.12.4.3.3	[System administrator and system operator activities shall be logged and the logs protected] and regularly reviewed.	08-43 Logical access control log
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.09.4.4.1	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	12-12 Information infrastructure requirements
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.12.4.1.1	Event logs recording user activities, exceptions, faults and information security events shall be produced, [kept and regularly reviewed.]	08-22 Electronic transactions security volations log
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.12.4.2.1	Logging facilities and log information shall be protected against tampering and unauthorized access.	09-13 Logical access system attack report
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.12.6.1.1	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	08-65 Security vulnerability scan log
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.13.2.3.1	Information involved in electronic messaging shall be appropriately protected.	08-21 Electronic messaging scan log
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.14.1.3.1	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	08-22 Electronic transactions security volations log
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.18.1.4.1	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	03-24 Management system strategy: privacy
ORG.4.BP.7	**Protect the information resource** Take steps, as appropriate, to protect the information resource from abuse.	A.18.1.5.1	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	08-17 Cryptographic controls application review log
COM.05 Internal audit				

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.05.BP.1	**Define the criteria and scope of each audit** Define the audit criteria and the scope of each audit.	09.2.3	a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;	03-01 Audit objectives
COM.05.BP.1	**Define the criteria and scope of each audit** Define the audit criteria and the scope of each audit.	09.2.9	The organization shall: d) define the audit criteria and scope for each audit;	04-02 Audit plan
COM.05.BP.1	**Define the criteria and scope of each audit** Define the audit criteria and the scope of each audit.	A.18.2.3.1	Information systems shall be [regularly] reviewed for compliance with the organization's information security policies and standards.	03-01 Audit objectives
COM.05.BP.2	**Select auditors** Select auditors to ensure objectivity and the impartiality of the audit process.	09.2.10	The organization shall: e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	08-04 Auditor list
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	09.2.1	The organization shall conduct internal audits [at planned intervals] to provide information on whether the information security management system:	08-01 Audit (ISMS) log
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	09.2.12	The organization shall: g) retain [documented] information as evidence [of the audit programme(s) and the audit results.	08-01 Audit (ISMS) log
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	A.15.2.1.2	Organizations shall regularly [monitor, review] and audit supplier service delivery.	09-22 Supplier surveillance report
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	A.18.2.1.1	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently [at planned intervals or when significant changes occur.]	09-11 ISMS Implementation audit report
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	A.18.2.1.1	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently [at planned intervals or when significant changes occur.]	09-01 Audit result
COM.05.BP.3	**Conduct audits** Conduct audits according to the defined criteria ensuring objectivity and the impartiality of the audit process.	A.18.2.2.1	Managers shall [regularly] review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	09-07 Information security audit report
TOP.1 Leadership				

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TOP.1.BP.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)	04.1.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	03-19 Management system strategy: external and internal issues
TOP.1.BP.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)	04.2.2	The organization shall determine: b) the requirements of these interested parties relevant to information security.	12-15 MS Interested parties MS expectations
TOP.1.BP.2	**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.)	04.2.1	The organization shall determine: a) interested parties that are relevant to the information security management system;	03-27 MS Interested parties
TOP.1.BP.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.	04.3.1	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	03-16 Management system (ISMS) scope

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TOP.1.BP.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.	04.3.2	When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1; b) the requirements referred to in 4.2; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	03-16 Management system (ISMS) scope
TOP.1.BP.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.	05.2.1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	05-08 Management system (ISMS) policy
TOP.1.BP.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.	06.2.1	The organization shall establish information security objectives at relevant functions and levels.	03-21 Management system strategy: information security objectives
TOP.1.BP.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.	A.05.1.1.1	A set of policies for information security shall be defined, [approved by management, published and communicated to employees and relevant external parties.]	05-08 Management system (ISMS) policy
TOP.1.BP.4	**Define an information security policy** Define an information security policy that is appropriate to the purpose of the organization.	05.2.1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	05-08 Management system (ISMS) policy
TOP.1.BP.4	**Define an information security policy** Define an information security policy that is appropriate to the purpose of the organization.	A.05.1.1.1	A set of policies for information security shall be defined, [approved by management, published and communicated to employees and relevant external parties.]	05-08 Management system (ISMS) policy

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TOP.1.BP.5	**Define information security objectives** Define information security objectives at relevant functions and levels, which are measurable, consistent with the information securit ypolicy, and which take into account applicable requirements and risk assessment and risk treatment results.	05.2.1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	05-08 Management system (ISMS) policy
TOP.1.BP.5	**Define information security objectives** Define information security objectives at relevant functions and levels, which are measurable, consistent with the information securit ypolicy, and which take into account applicable requirements and risk assessment and risk treatment results.	06.2.2	The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.	03-08 Information security objectives
TOP.1.BP.5	**Define information security objectives** Define information security objectives at relevant functions and levels, which are measurable, consistent with the information securit ypolicy, and which take into account applicable requirements and risk assessment and risk treatment results.	A.05.1.1.1	A set of policies for information security shall be defined, [approved by management, published and communicated to employees and relevant external parties.]	05-08 Management system (ISMS) policy
TOP.1.BP.6	**Determine process strategy** Determine the management system and operational process strategy.	07.5.1.1	The organization's information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.	03-17 Management system strategy: documentation
TOP.1.BP.6	**Determine process strategy** Determine the management system and operational process strategy.	07.5.3.1	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition.	03-17 Management system strategy: documentation
TOP.1.BP.6	**Determine process strategy** Determine the management system and operational process strategy.	08.1.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.	03-25 Management system strategy: processes
TOP.1.BP.6	**Determine process strategy** Determine the management system and operational process strategy.	10.2.1	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	03-20 Management system strategy: improvement

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	04.4.1	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	03-18 Management system strategy: Establish
TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	05.1.1	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	03-22 Management system strategy: management commitment
TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	07.5.1.1	The organization's information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.	03-17 Management system strategy: documentation
TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	07.5.3.1	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition.	03-17 Management system strategy: documentation

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	08.1.6	The organization shall ensure that outsourced processes are determined and controlled.	03-23 Management system strategy: outsourcing
COM.06 Management review				
COM.06.BP.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.	09.3.3	The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives; d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement.	03-15 Management review objectives
COM.06.BP.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.	09.3.1	Top management shall review the organization's information security management system [at planned intervals] to ensure its continuing suitability, adequacy and effectiveness.	08-46 Management review result
COM.06.BP.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.	09.3.4	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.	08-44 Management review action log
COM.06.BP.4	**Make decisions** Make decisions related to continual improvement opportunities and any need for changes to the information security management system.	09.3.4	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.	08-44 Management review action log
COM.07 Non-conformity management				
COM.07.BP.1	**Identify non-conformities** Identify non-conformities.	10.1.1	When a nonconformity occurs ..	08-50 Non-conformity record
COM.07.BP.2	**Resolve and close non-conformities** Resolve and close non-conformities.	10.1.2	[When a nonconformity occurs], the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and	08-49 Non-conformity disposition record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.07.BP.3	**Determine cause of non-conformities** Determine the cause of selected non-conformities.	10.1.4	[When a nonconformity occurs, the organization shall: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity;] 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;	08-15 Corrective action request root cause analysis result
COM.07.BP.4	**Determine the need for action** Determine the need for action to eliminate the causes of non-conformities.	10.1.3	[When a nonconformity occurs], the organization shall: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, [by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;]	08-12 Correction action log
COM.07.BP.4	**Determine the need for action** Determine the need for action to eliminate the causes of non-conformities.	10.1.8	Corrective actions shall be appropriate to the effects of the nonconformities encountered.	03-02 Corrective action change proposal
COM.07.BP.5	**Implement selected action proposals** Implement a selected action proposal.	10.1.5	[When a nonconformity occurs], the organization shall: c) implement any action needed;	08-13 Corrective action change proposal approval record
COM.07.BP.5	**Implement selected action proposals** Implement a selected action proposal.	10.1.7	[When a nonconformity occurs], the organization shall: e) make changes to the information security management system, if necessary.	08-13 Corrective action change proposal approval record
COM.07.BP.6	**Confirm change effectiveness** Confirm the effectiveness of changes to eliminate the non-conformities.	10.1.6	[When a nonconformity occurs], the organization shall: d) review the effectiveness of any corrective action taken; and	08-16 Corrective action verification record
COM.09 Operational implementation and control				
COM.09.BP.1	**Allocate roles, responsibilities and authorities** Allocate the required roles, responsibilities and authorities.	05.3.1	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned [and communicated.]	08-61 Roles and responsibilities assignment record
COM.09.BP.1	**Allocate roles, responsibilities and authorities** Allocate the required roles, responsibilities and authorities.	A.06.1.1.2	All information security responsibilities shall be [defined and] allocated.	08-61 Roles and responsibilities assignment record
COM.09.BP.2	**Allocate resources** Allocate and apply the required resources.	07.1.2	The organization shall [determine and] provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	08-47 MS Resources provision record
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	06.1.2.4	The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	08-39 ISMS Implementation log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	06.1.3.2	The organization shall [define and] apply an information security risk treatment process to..	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	08.1.2	The organization shall also implement plans to achieve information security objectives determined in 6.2.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	09.2.4	b) is effectively implemented [and maintained].	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	09.2.7	The organization shall: c) [plan, establish,] implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.06.2.1.2	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.06.2.2.3	A [policy and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.08.1.3.3	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified, documented and] implemented.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.08.2.2.2	An appropriate set of procedures for information labelling shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.08.2.3.2	Procedures for handling assets shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.08.3.1.2	[Procedures shall be] implemented [for the management of removable media in accordance with the classification scheme adopted by the organization.]	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.09.2.1.2	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.09.2.2.1	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.09.2.4.2	[The allocation of secret authentication information] shall be controlled [through a formal management process.]	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.10.1.1.2	A policy on the use of cryptographic controls for protection of information shall be [developed and] implemented.	08-39 ISMS Implementation log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.10.1.2.2	A policy on the use, protection and lifetime of cryptographic keys shall be [developed and] implemented through their whole lifecycle.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.11.1.5.2	Procedures for working in secure areas shall be [designed and] applied.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.11.2.9.2	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.12.2.1.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.12.5.1.2	Procedures shall be implemented to control the installation of software on operational systems.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.12.6.2.1	Rules governing the installation of software by users shall be [established and] implemented.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.16.1.7.3	The organization shall [define and] apply procedures for the identification, collection, acquisition and preservation of information, [which can serve as evidence.]	09-08 Information security incident report
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.17.1.2.2	The organization shall [establish, document], implement [and maintain] processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.17.2.1.1	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	08-39 ISMS Implementation log
COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	A.18.1.2.2	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	08-39 ISMS Implementation log
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	06.1.2.5	b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;	08-59 Risk assessment process effectiveness evaluation result
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	07.2.4	The organization shall: c) [where applicable, take actions to acquire the necessary competence, and] evaluate the effectiveness of the actions taken; and	08-72 Training effectiveness evaluation result
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	08.1.4	The organization shall [control planned changes] and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	08-40 ISMS Implementation review record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	08.1.4	The organization shall [control planned changes] and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	08-53 Process change request review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	08.1.5	The organization shall control planned changes [and review] the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	08-54 Process change review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	09.2.5	b) is [effectively implemented] and maintained.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.05.1.2.1	The policies for information security shall be reviewed [at planned intervals] or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.09.1.1.3	An access control policy shall be [established, documented and] reviewed based on business and information security requirements.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.12.1.2.1	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	08-54 Process change review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.12.4.1.3	Event logs recording user activities, exceptions, faults and information security events shall be [produced, kept and] regularly reviewed.	08-23 Electronic transactions security volations log review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.12.4.3.3	[System administrator and system operator activities shall be logged and the logs protected] and regularly reviewed.	08-70 System activity log review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.12.7.1.2	Audit requirements and activities involving verification of operational systems shall be [carefully planned and] agreed to minimise disruptions to business processes.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.13.2.4.2	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be [identified, regularly] reviewed [and documented.]	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.14.2.3.1	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.14.2.7.1	The organization shall supervise and monitor the activity of outsourced system development.	08-40 ISMS Implementation review record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.15.2.1.1	Organizations shall regularly monitor, review [and audit] supplier service delivery.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.17.1.3.1	The organization shall verify the established and implemented information security continuity controls [at regular intervals] in order to ensure that they are valid and effective during adverse situations.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.18.2.1.1	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently [at planned intervals or when significant changes occur.]	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.18.2.2.1	Managers shall [regularly] review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	08-40 ISMS Implementation review record
COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	A.18.2.3.1	Information systems shall be [regularly] reviewed for compliance with the organization's information security policies and standards.	08-40 ISMS Implementation review record
COM.09.BP.5	**Correct deviations** Correct deviations from planned arrangements when targets are not achieved.	08.1.5	The organization shall control planned changes [and review] the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	11-4 Process change request
COM.09.BP.5	**Correct deviations** Correct deviations from planned arrangements when targets are not achieved.	A.12.1.2.1	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	11-4 Process change request
COM.08 Operational planning				
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.1.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 [and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.]	03-36 Risk and opportunity identification criteria
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.1.2.1	The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	03-37 Risk assessment process description

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.1.2.2	[The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:] 1) the risk acceptance criteria; [and 2) criteria for performing information security risk assessments;]	12-22 Risk acceptance criteria
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.1.2.3	[The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and] 2) criteria for performing information security risk assessments;	12-06 Criteria for performing risk assessments
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.1.3.1	The organization shall define [and apply] an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A; e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	03-39 Risk treatment process description
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	06.2.7	When planning how to achieve its information security objectives, the organization shall determine: f) what will be done;	03-29 Process objectives
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.06.1.5.1	Information security shall be addressed in project management, regardless of the type of the project.	04-12 Product /service process lifecycle model
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.06.2.1.1	A policy and supporting security measures [shall be adopted] to manage the risks introduced by using mobile devices.	05-09 Mobile device policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.06.2.2.1	A policy [and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.	05-13 Teleworking policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.08.1.3.1	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, [documented and implemented.]	03-05 Information asset control objective
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.08.2.2.1	An appropriate set of procedures for information labelling shall be developed [and implemented] in accordance with the information classification scheme adopted by the organization.	06-07 Information labelling, handling and storage procedure

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.08.2.3.1	Procedures for handling assets shall be developed and [implemented] in accordance with the information classification scheme adopted by the organization.	06-01 Asset management procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.09.1.1.1	An access control policy shall be established, [documented and reviewed based on business and information security requirements.]	05-06 Information system access policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.09.2.1.1	A formal user registration and de-registration process shall be [implemented] to enable assignment of access rights.	06-17 User authentication information control procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.09.2.4.1	The allocation of secret authentication information [shall be controlled through] a formal management process.	06-17 User authentication information control procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.10.1.1.1	A policy on the use of cryptographic controls for protection of information shall be developed [and implemented.]	05-02 Cryptographic controls usage policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.10.1.2.1	A policy on the use, protection and lifetime of cryptographic keys shall be developed [and implemented] through their whole lifecycle.	05-03 Cryptographic key protection and usage policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.11.2.9.1	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities [shall be adopted.]	05-01 Clear desk policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.12.3.1.4	[Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed] backup policy.	05-04 Data backup policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.12.5.1.1	Procedures shall be [implemented] to control the installation of software on operational systems.	06-15 Software installation procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.12.6.2.2	Rules governing the installation of software by users shall be established [and implemented].	05-11 Software installation by users policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.13.2.1.1	Formal transfer policies, [procedures and controls] shall be in place to protect the transfer of information through the use of all types of communication facilities.	05-07 Information transfer policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.13.2.4.1	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified[, regularly reviewed and documented.]	12-04 Confidentiality requirements
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.14.2.1.1	Rules for the development of software and systems shall be established and applied to developments within the organization.	05-10 Secure development policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.14.2.2.1	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	06-03 Change control procedure

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.14.2.5.1	Principles for engineering secure systems shall be established,[documented, maintained] and applied to any information system implementation efforts.	04-12 Product /service process lifecycle model
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.14.2.8.1	Testing of security functionality shall be carried out during development.	04-12 Product /service process lifecycle model
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.15.1.1.1	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets [shall be agreed with the supplier and documented.]	05-12 Supplier relationship information security policy
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.16.1.5.2	Information security incidents shall be responded to in accordance with the [documented] procedures.	06-14 Security incident management procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.17.1.2.1	The organization shall establish, [document], implement [and maintain] processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	06-02 Business continuity procedure
COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	A.18.1.2.1	Appropriate procedures [shall be implemented] to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	06-11 Protection of intellectual property rights procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.06.2.2.2	A [policy and] supporting security measures [shall be implemented to protect information accessed, processed or stored at teleworking sites.]	06-16 Teleworking procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.08.3.1.1	Procedures shall be [implemented] for the management of removable media in accordance with the classification scheme adopted by the organization.	06-12 Removable media management procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.08.3.2.1	Media [shall be disposed of securely when no longer required,] using formal procedures.	06-12 Removable media management procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.11.1.5.1	Procedures for working in secure areas shall be designed [and applied.]	06-13 Secure area operating procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.12.1.1.1	Operating procedures [shall be documented and made available to all users who need them.]	06-10 Operating Procedures
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.13.2.1.2	Formal transfer [policies], procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	06-09 Information transfer procedure

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.16.1.1.2	[Management responsibilities and] procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	06-08 Information security incident response procedure
COM.08.BP.3	**Determine the set of activities that transform the inputs into outputs** Determine the set of activities that transform the inputs into outputs.	A.16.1.7.2	The organization shall define and [apply procedures] for the identification, collection, acquisition and preservation of information, [which can serve as evidence.]	06-05 Evidence collection and preservation procedure
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	05.3.3	Top management [shall assign] the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management.	03-26 Management system strategy: roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	06.2.9	When planning how to achieve its information security objectives, the organization shall determine: h) who will be responsible;	03-31 Process roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	09.1.5	d) who shall monitor and measure;	03-11 ISMS Measurement information gathering roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	09.1.7	f) who shall analyse and evaluate these results.	03-09 ISMS Measurement information analysis roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	A.06.1.1.1	All information security responsibilities shall be defined [and allocated].	03-14 ISMS Roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	A.06.1.2.1	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	03-14 ISMS Roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	A.08.1.2.1	Assets maintained in the inventory shall be owned.	03-06 Information asset management roles and responsibilities
COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	A.16.1.1.1	Management responsibilities [and procedures] shall be established to ensure a quick, effective and orderly response to information security incidents.	03-31 Process roles and responsibilities
COM.08.BP.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.	06.2.8	When planning how to achieve its information security objectives, the organization shall determine: g) what resources will be required;	03-30 Process resource needs

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.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.	07.1.1	The organization shall determine [and provide] the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	04-13 Resources budget
COM.08.BP.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.	06.2.11	When planning how to achieve its information security objectives, the organization shall determine: j) how the results will be evaluated.	03-28 Process measures
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	06.1.1.3	The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	04-14 Risk management plan
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	06.2.10	When planning how to achieve its information security objectives, the organization shall determine: i) when it will be completed; and	03-32 Process schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	08.2.2	[The organization shall perform information security risk assessments] at planned intervals or when significant changes are proposed or occur, [taking account of the criteria established in 6.1.2 a).]	08-58 Risk assessment action schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.1.4	c) when the monitoring and measuring shall be performed;	03-10 ISMS Measurement information gathering events
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.1.6	e) when the results from monitoring and measurement shall be analyzed and evaluated; and	03-10 ISMS Measurement information gathering events
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.2.2	[The organization shall conduct internal audits] at planned intervals [to provide information on whether the information security management system:]	04-01 Audit (ISMS) schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.2.6	The organization shall: c) plan, establish, [implement and maintain] an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.	04-03 Audit programme plan
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.2.8	The organization shall: The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;	04-03 Audit programme plan
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	09.3.2	[Top management shall review the organization's information security management system] at planned intervals [to ensure its continuing suitability, adequacy and effectiveness.]	04-11 Management review schedule

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.05.1.2.2	The policies for information security [shall be reviewed] at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	04-10 ISMS Policy review schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.09.2.5.2	Asset owners [shall review users' access rights] at regular intervals.	04-19 User access rights review schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.12.3.1.3	[Backup copies of information, software and system images shall be taken and tested] regularly [in accordance with an agreed backup policy].	04-06 Data backup test schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.12.7.1.1	Audit requirements and activities involving verification of operational systems shall be carefully planned [and agreed] to minimise disruptions to business processes.	04-03 Audit programme plan
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.15.2.1.3	Organizations shall regularly [monitor, review and audit supplier service delivery.]	04-01 Audit (ISMS) schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.17.1.3.2	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	04-08 Information security control verification schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.18.2.1.2	[The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently] at planned intervals [or when significant changes occur.]	04-01 Audit (ISMS) schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.18.2.2.2	Managers shall regularly [review] the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	04-16 Security policies compliance review schedule
COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	A.18.2.3.2	Information systems shall be regularly [reviewed for compliance with the organization's information security policies and standards.]	04-09 Information system compliance review schedule
COM.10 Performance evaluation				
COM.10.BP.1	**Determine what needs to be monitored and measured** Determine what needs to be monitored and measured, including information security processes and controls.	06.2.3	The information security objectives shall: b) be measurable (if practicable);	03-12 ISMS Measurement information needs

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.10.BP.1	**Determine what needs to be monitored and measured** Determine what needs to be monitored and measured, including information security processes and controls.	09.1.2	The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls;	03-12 ISMS Measurement information needs
COM.10.BP.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.	09.1.3	b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	03-13 ISMS Measurement methods
COM.10.BP.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.	09.1.1	The organization shall evaluate the information security performance and the effectiveness of the information security management system.	09-12 ISMS measurement information analysis report
COM.10.BP.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.	A.16.1.6.1	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	09-08 Information security incident report
TEC.05 Product/service release				
TEC.05.BP.5	**Test the release** Test the release in accordance with defined criteria.	A.14.2.3.1	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	08-38 Information system changes security impact evaluation result
TEC.08 Product/Service/System requirements				
TEC.08.BP.3	**Define service requirements** Define the requirements for the new or changed service.	A.14.1.1.1	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	12-16 New or changed services - system security requirements
TEC.08.BP.3	**Define service requirements** Define the requirements for the new or changed service.	A.14.1.2.1	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	12-16 New or changed services - system security requirements
TEC.08.BP.3	**Define service requirements** Define the requirements for the new or changed service.	A.18.1.1.01.1	All relevant legislative statutory, regulatory, [contractual] requirements and the organization's approach to meet these requirements shall be explicitly identified, [documented and kept up to date for each information system and the organization.]	12-24 Statutory and regulatory requirements

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TEC.08.BP.3	**Define service requirements** Define the requirements for the new or changed service.	A.18.1.1.02.1	All relevant [legislative statutory, regulatory,] contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, [documented and kept up to date for each information system and the organization.]	12-05 Contractual requirements
TEC.08.BP.4	**Define service validation requirements** Define the requirements for validating the new or changed service.	A.14.2.9.1	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	12-25 System acceptance criteria
COM.11 Risk and opportunity management				
COM.11.BP.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	06.1.1.2	[When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and] determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.	03-38 Risk identification
COM.11.BP.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	06.1.2.6	c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	03-38 Risk identification
COM.11.BP.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	08.2.1	The organization shall perform information security risk assessments [at planned intervals or when significant changes are proposed or occur], taking account of the criteria established in 6.1.2 a).	03-38 Risk identification
COM.11.BP.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.	06.1.2.7	d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	09-16 Risk analysis report
COM.11.BP.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.	06.1.2.8	e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment.	08-60 Risk assessment review record

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
COM.11.BP.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.	06.1.3.3	e) formulate an information security risk treatment plan; and	04-15 Risk treatment plan
COM.11.BP.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.	08.3.1	The organization shall implement the information security risk treatment plan.	08-39 ISMS Implementation log
TEC.06 Service availability management				
TEC.06.BP.1	**Identify availability requirements** service availability requirements are identified.	A.17.2.1.1	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	12-23 Service availability requirements
TEC.07 Service continuity management				
TEC.07.BP.1	**Identify service continuity requirements** Identify service continuity requirements.	A.17.1.1.1	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	12-01 Business continuity requirements
TEC.07.BP.3	**Test service continuity** Test service continuity against the service continuity requirements.	A.17.1.3.1	The organization shall verify the established and implemented information security continuity controls [at regular intervals] in order to ensure that they are valid and effective during adverse situations.	08-05 Business continuity plan test result
ORG.5 Supplier management				
ORG.5.BP.2	**Negotiate products/services/systems** Negotiate and define products/services/systems to be provided with each supplier.	A.13.2.2.1	Agreements shall address the secure transfer of business information between the organization and external parties.	01-1 Business information exchange agreement
ORG.5.BP.2	**Negotiate products/services/systems** Negotiate and define products/services/systems to be provided with each supplier.	A.15.1.2.1	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	01-3 Supplier agreement
ORG.5.BP.2	**Negotiate products/services/systems** Negotiate and define products/services/systems to be provided with each supplier.	A.15.1.3.1	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	01-3 Supplier agreement
TEC.09 Technical data preservation and recovery				
TEC.09.BP.3	**Execute data backups** Execute data backups.	A.12.3.1.1	Backup copies of information, software and system images shall be taken [and tested regularly in accordance with an agreed backup policy.]	08-18 Data backup log

Base practice reference	Base practice description	ISO/IEC 27001 Requirement reference	Associated singular requirement	Information item
TEC.09.BP.4	**Perform data restore** Perform data restore.	A.12.3.1.2	Backup copies of information, software and system images shall be [taken and] tested [regularly in accordance with an agreed backup policy.]	08-20 Data restore log

C.2 Associations of requirements with base practices

The following table identifies sub-clauses and singular requirements, associated base practices and implied information items.

Table C.2 — Association of ISO/IEC 27001 requirements and base practices

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
04.1 Understanding the organization and its context				
1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	TOP.1.BP.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)	03-19 Management system strategy: external and internal issues
04.2 Understanding the needs and expectations of interested parties				
1	The organization shall determine: a) interested parties that are relevant to the information security management system;	TOP.1.BP.2	**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.)	03-27 MS Interested parties
2	The organization shall determine: b) the requirements of these interested parties relevant to information security.	TOP.1.BP.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)	12-15 MS Interested parties MS expectations
04.3 Determining the scope of the information security management system				
1	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	TOP.1.BP.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.	03-16 Management system (ISMS) scope

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
2	When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1; b) the requirements referred to in 4.2; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	TOP.1.BP.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.	03-16 Management system (ISMS) scope
3	The scope shall be available as documented information.	COM.02.BP.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.	03-16 Management system (ISMS) scope
04.4 Information security management system				
1	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	03-18 Management system strategy: Establish
05.1 Leadership and commitment				
1	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	TOP.1.BP.7	**Integrate information security management system requirements into the business processes of the organization** Ensure the integration of the information securitymanagement system requirements into the business processes of the organization.	03-22 Management system strategy: management commitment

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
2	Top management shall demonstrate leadership and commitment with respect to the information security management system by: d) communicating the importance of effective information security management and of conforming to the information security management system requirements;	COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	09-10 ISMS Communication records
05.2 Policy				
1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	TOP.1.BP.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.	05-08 Management system (ISMS) policy
1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	TOP.1.BP.4	**Define an information security policy** Define an information security policy that is appropriate to the purpose of the organization.	05-08 Management system (ISMS) policy
1	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	TOP.1.BP.5	**Define information security objectives** Define information security objectives at relevant functions and levels, which are measurable, consistent with the information securit ypolicy, and which take into account applicable requirements and risk assessment and risk treatment results.	05-08 Management system (ISMS) policy
2	The information security policy shall: e) be available as documented information;	COM.02.BP.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.	05-08 Management system (ISMS) policy
3	The information security policy shall: f) be communicated within the organization;	COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	09-10 ISMS Communication records

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
4	The information security policy shall: g) be available to interested parties, as appropriate.	COM.02.BP.6	**Make documented information available to designated parties.** Manage the distribution, access, retrieval and use of documented information towards interested parties.	05-08 Management system (ISMS) policy
05.3 Organizational roles, responsibilities and authorities				
1	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned [and communicated.]	COM.09.BP.1	**Allocate roles, responsibilities and authorities** Allocate the required roles, responsibilities and authorities.	08-61 Roles and responsibilities assignment record
2	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are [assigned and] communicated.	COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	09-10 ISMS Communication records
3	Top management [shall assign] the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management.	COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	03-26 Management system strategy: roles and responsibilities
06.1.1 General				
1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 [and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.]	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	03-36 Risk and opportunity identification criteria
2	[When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and] determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.	COM.11.BP.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	03-38 Risk identification

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
3	The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	04-14 Risk management plan
06.1.2 Information security risk assessment				
1	The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	03-37 Risk assessment process description
2	[The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:] 1) the risk acceptance criteria; [and 2) criteria for performing information security risk assessments;]	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	12-22 Risk acceptance criteria
3	[The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and] 2) criteria for performing information security risk assessments;	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	12-06 Criteria for performing risk assessments
4	The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	COM.02.BP.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.	08-39 ISMS Implementation log
4	The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	08-39 ISMS Implementation log

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
5	b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;	COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	08-59 Risk assessment process effectiveness evaluation result
6	c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	COM.11.BP.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	03-38 Risk identification
7	d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	COM.11.BP.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.	09-16 Risk analysis report
8	e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment.	COM.11.BP.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.	08-60 Risk assessment review record
9	The organization shall retain documented information about the information security risk assessment process.	COM.02.BP.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.	03-37 Risk assessment process description

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
06.1.3 Information security risk treatment				
1	The organization shall define [and apply] an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A; e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	03-39 Risk treatment process description
2	The organization shall [define and] apply an information security risk treatment process to..	COM.02.BP.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.	08-39 ISMS Implementation log
2	The organization shall [define and] apply an information security risk treatment process to..	COM.09.BP.3	**Perform process activities** Implement actions taken to achieve the management system objectives.	08-39 ISMS Implementation log
3	e) formulate an information security risk treatment plan; and	COM.11.BP.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.	04-15 Risk treatment plan
4	f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	COM.02.BP.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.	08-56 Residual risk approval record
5	The organization shall retain documented information about the information security risk treatment process	COM.02.BP.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.	03-39 Risk treatment process description

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
06.2 Information security objectives and plans to achieve them				
1	The organization shall establish information security objectives at relevant functions and levels.	TOP.1.BP.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.	03-21 Management system strategy: information security objectives
2	The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.	TOP.1.BP.5	**Define information security objectives** Define information security objectives at relevant functions and levels, which are measurable, consistent with the information securit ypolicy, and which take into account applicable requirements and risk assessment and risk treatment results.	03-08 Information security objectives
3	The information security objectives shall: b) be measurable (if practicable);	COM.10.BP.1	**Determine what needs to be monitored and measured** Determine what needs to be monitored and measured, including information security processes and controls.	03-12 ISMS Measurement information needs
4	The information security objectives shall: d) be communicated;	COM.01.BP.6	**Communicate information products** Communicate information products to interested parties.	09-10 ISMS Communication records
5	The information security objectives shall: e) be updated as appropriate.	COM.02.BP.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.	03-08 Information security objectives
6	The organization shall retain documented information on the information security objectives.	COM.02.BP.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.	03-08 Information security objectives
7	When planning how to achieve its information security objectives, the organization shall determine: f) what will be done;	COM.08.BP.1	**Identify process needs and requirements** Identify process needs and requirements.	03-29 Process objectives
8	When planning how to achieve its information security objectives, the organization shall determine: g) what resources will be required;	COM.08.BP.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.	03-30 Process resource needs
9	When planning how to achieve its information security objectives, the organization shall determine: h) who will be responsible;	COM.08.BP.5	**Identify the required competencies and roles for performing the process** Identify the required competencies and roles for performing the process.	03-31 Process roles and responsibilities
10	When planning how to achieve its information security objectives, the organization shall determine: i) when it will be completed; and	COM.08.BP.8	**Plan the deployment of the process** Plan the processes will be deployed in order to achieve the information security objectives.	03-32 Process schedule

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
11	When planning how to achieve its information security objectives, the organization shall determine: j) how the results will be evaluated.	COM.08.BP.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.	03-28 Process measures
07.1 Resources				
1	The organization shall determine [and provide] the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	COM.08.BP.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.	04-13 Resources budget
2	The organization shall [determine and] provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	COM.09.BP.2	**Allocate resources** Allocate and apply the required resources.	08-47 MS Resources provision record
07.2 Competence				
1	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;	COM.03.BP.1	**Identify organisational competencies** Identify the competencies required by the organization.	12-17 Organisational competence requirements
2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	COM.03.BP.2	**Evaluate competence of personnel** Evaluate the competence of the personnel	08-74 Training record
2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	08-74 Training record
2	The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	COM.03.BP.4	**Demonstrate awareness of role** Each individual demonstrates their understanding of their role and activities in achieving organsational objectives.	08-74 Training record
3	The organization shall: c) where applicable, take actions to acquire the necessary competence, [and evaluate the effectiveness of the actions taken; and]	COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	08-73 Training provision action log
4	The organization shall: c) [where applicable, take actions to acquire the necessary competence, and] evaluate the effectiveness of the actions taken; and	COM.09.BP.4	**Review process activities** Review suitability and effectiveness of the actions required to achieve the management system objectives.	08-72 Training effectiveness evaluation result
5	The organization shall: d) retain appropriate documented information as evidence of competence.	COM.02.BP.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.	08-51 Personnel competency records

Reference Number	Singular requirement	BP Reference	Base practice	Information item implied
07.3 Awareness				
1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	COM.03.BP.2	**Evaluate competence of personnel** Evaluate the competence of the personnel	08-74 Training record
1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	COM.03.BP.3	**Take action to acquire ncessary competencies** Where applicable, take actions to acquire the necessary competence (hiring, human resources mobility, sub-contracting, training, coaching etc)	08-74 Training record
1	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	COM.03.BP.4	**Demonstrate awareness of role** Each individual demonstrates their understanding of their role and activities in achieving organsational objectives.	08-74 Training record
07.4 Communication				
1	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate;	COM.01.BP.1	**Define information content** Define information content in terms of identified communication needs and requirements.	12-03 Communication requirements
2	The organization shall determine the need for internal and external communications relevant to the information security management system including: b) when to communicate;	COM.01.BP.4	**Identify communication events** Identify the events that require comminication actions.	12-03 Communication requirements
3	The organization shall determine the need for internal and external communications relevant to the information security management system including: c) with whom to communicate;	COM.01.BP.2	**Identify parties to communicate to** Identify parties to communicate with.	12-03 Communication requirements