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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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

© ISO/IEC 2016

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a979c4c06205/iso-iec-ts-33072-2016

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

 © ISO/IEC 2016 — All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904a06203/iso-iec-ts-33072-2016

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*".

© ISO/IEC 2016 — All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904c00205/iso-iec-ts-33072-2016

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.

© ISO/IEC 2016 — All rights reserved

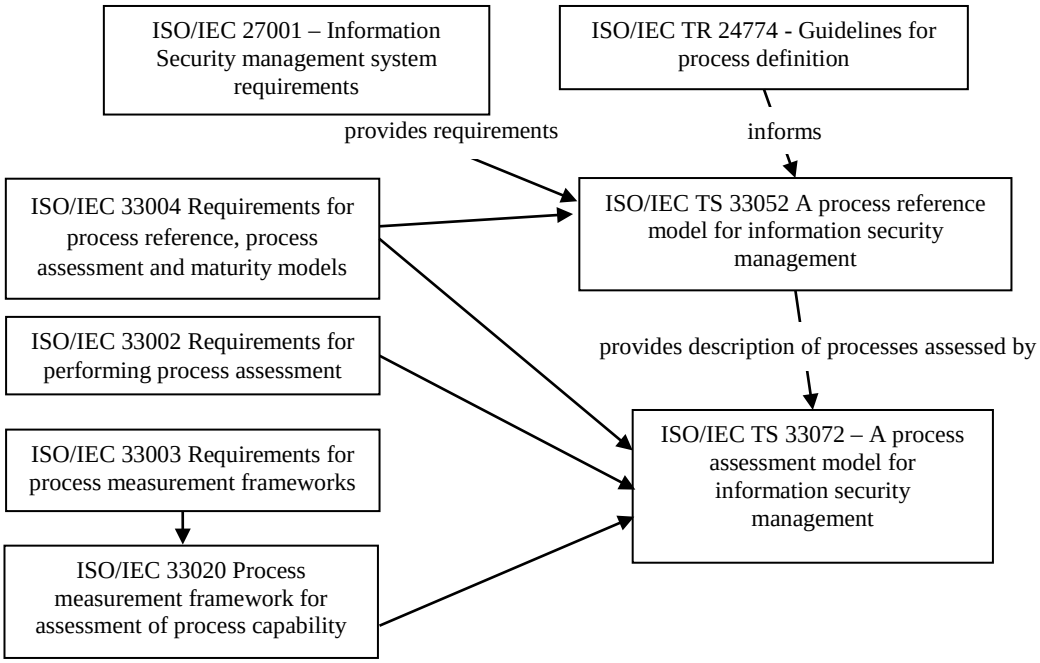


Figure 1 — Relationships between relevant standards

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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;

© ISO/IEC 2016 — All rights reserved

— 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

 © ISO/IEC 2016 — All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-e340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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.

© ISO/IEC 2016 — All rights reserved

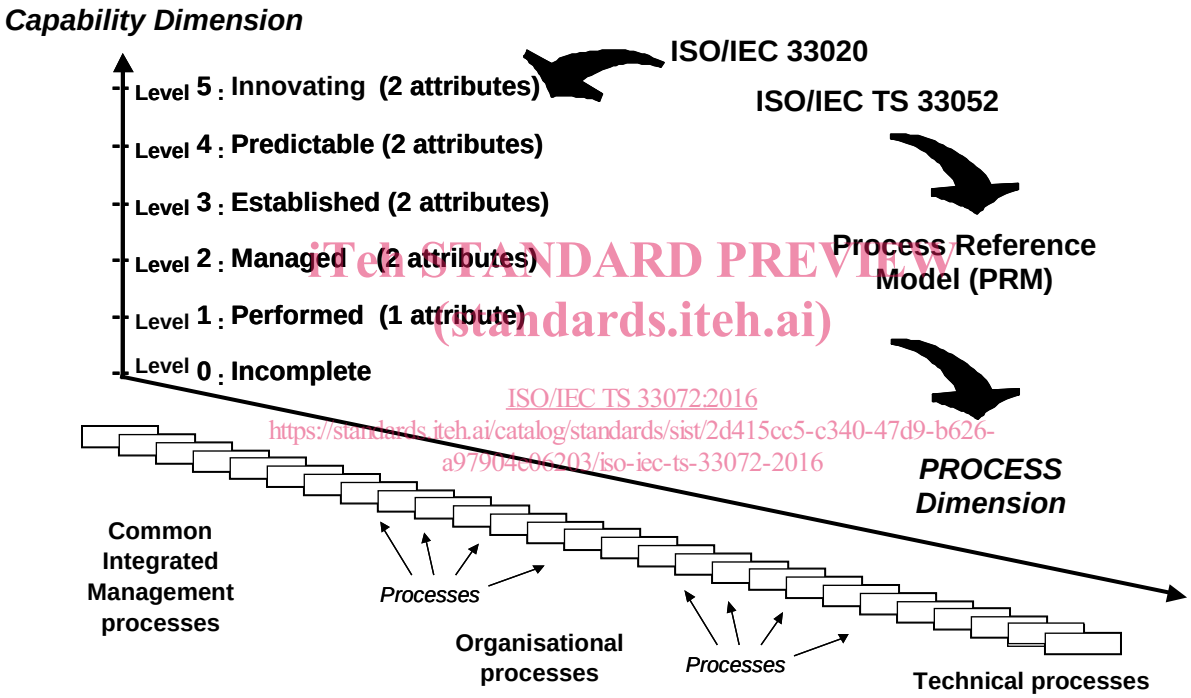
4 Overview of the Process Assessment Model

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904c06203/iso-iec-ts-33072-2016

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.

© ISO/IEC 2016 — All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

A process description shall meet the following requirements:

a) a process shall be described in terms of its purpose and process outcomes;

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/f5d1f5ce-5ce3-4749-b626-a97904e06203/iso-iec-ts-33072-2016

b) the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process;

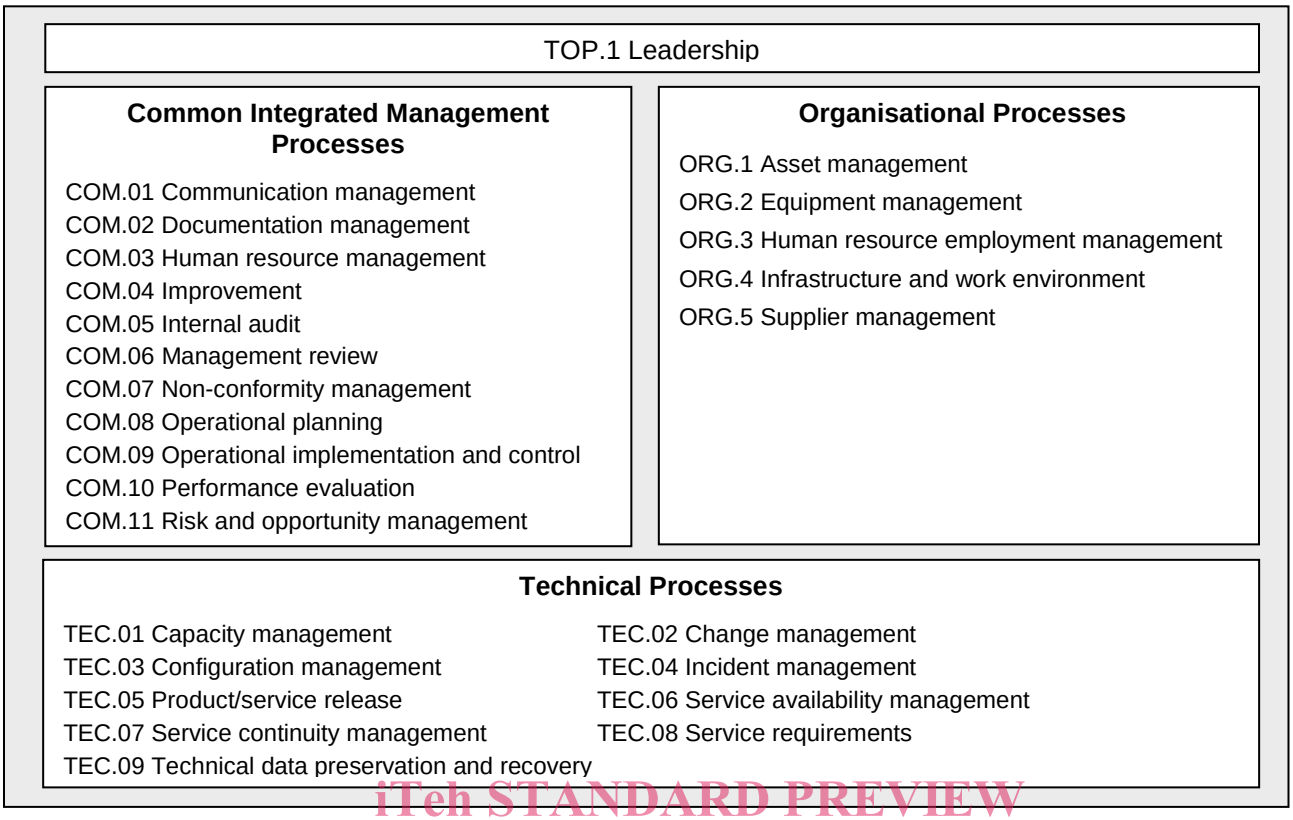
c) process descriptions shall not contain or imply aspects of the process quality characteristic beyond the basic level of any relevant process measurement framework conformant with ISO/IEC 33003."

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.

© ISO/IEC 2016 — All rights reserved



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 3 — Processes in the Process Reference Model

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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.

© ISO/IEC 2016 — All rights reserved

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

iTeh STANDARD PREVIEW

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

(standards.iteh.ai)

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.

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415ec5-e340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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

© ISO/IEC 2016 — All rights reserved

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

The process performance indicators are:

— Base Practice (BP);

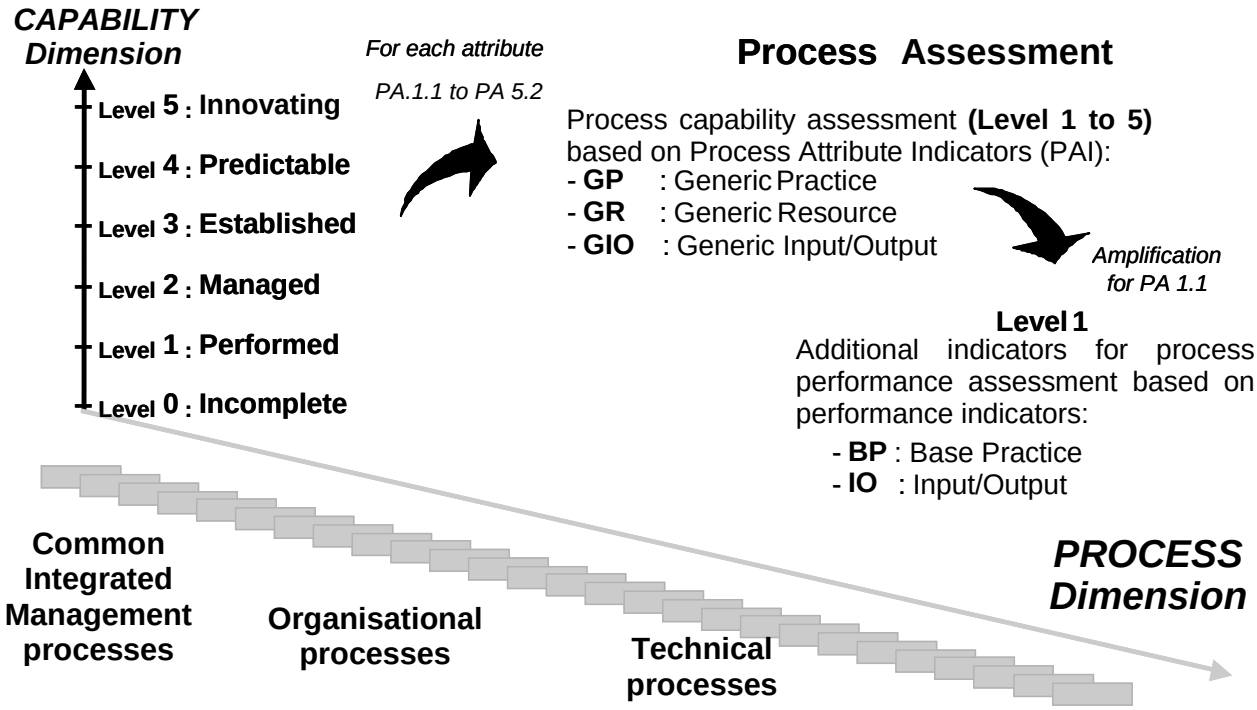
— Input/output (IO).

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.

 © ISO/IEC 2016 — All rights reserved



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 4 — Assessment indicators

4.3.1 Process Capability Indicators

ISO/IEC TS 33072:2016
https://standards.iteh.ai/catalog/standards/sist/2d415cc5-c340-47d9-b626-a97904e06203/iso-iec-ts-33072-2016

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.

© ISO/IEC 2016 — All rights reserved