TECHNICAL SPECIFICATION

ISO/IEC TS 33072

First edition
2016-06-01

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

PROOF/ÉPREUVE

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

COPYRIGHT PROTECTED DOCUMENT

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

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*.

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.

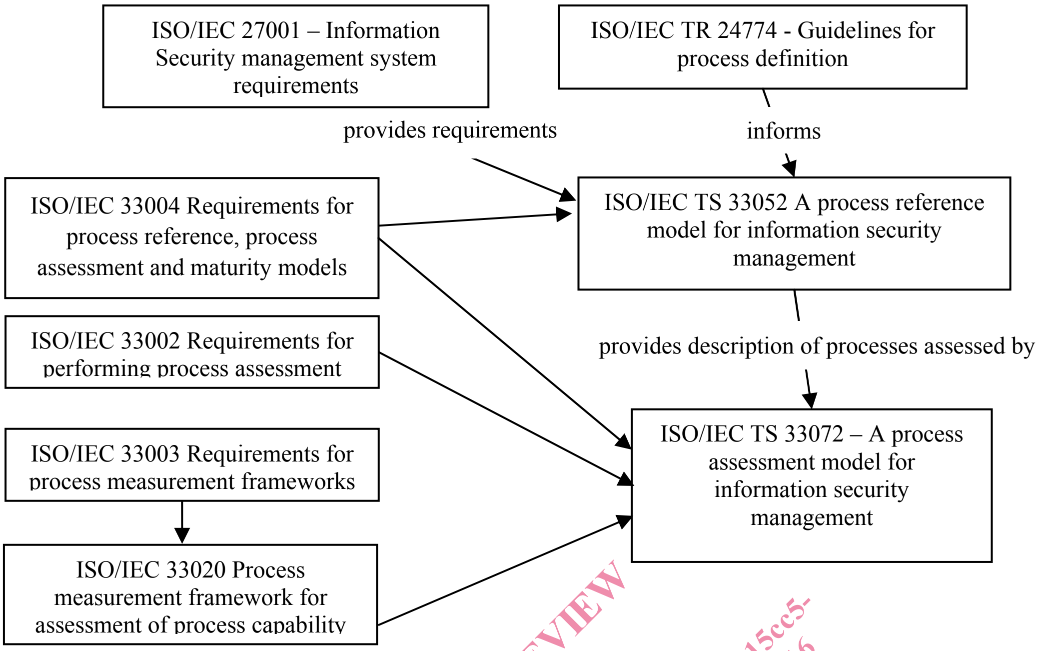

Figure 1 — Relationships between relevant standards

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 cab 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.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 33001, *Information technology — Process assessment — Concepts and terminology*

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.

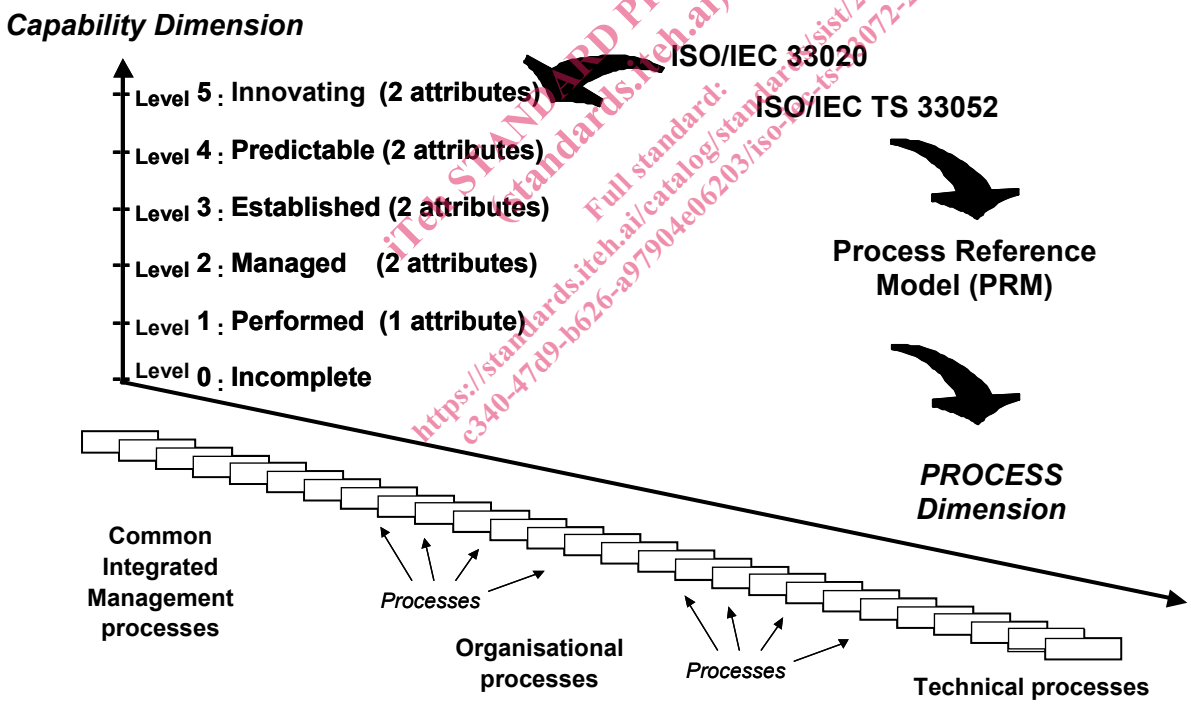

Figure 2 — Relationship between the Process Assessment Model and its inputs

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.

TOP.1 Leadership

Common Integrated Management Processes

COM.01 Communication management
COM.02 Documentation management
COM.03 Human resource management
COM.04 Improvement
COM.05 Internal audit
COM.06 Management review
COM.07 Non-conformity management
COM.08 Operational planning
COM.09 Operational implementation and control
COM.10 Performance evaluation
COM.11 Risk and opportunity management

Organisational Processes

ORG.1 Asset management
ORG.2 Equipment management
ORG.3 Human resource employment management
ORG.4 Infrastructure and work environment
ORG.5 Supplier management

Technical Processes

TEC.01 Capacity management
TEC.02 Change management
TEC.03 Configuration management
TEC.04 Incident management
TEC.05 Product/service release
TEC.06 Service availability management
TEC.07 Service continuity management
TEC.08 Service requirements
TEC.09 Technical data preservation and recovery

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