TECHNICAL SPECIFICATION

ISO/IEC TS 33072

First edition
2016-07-15

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

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.

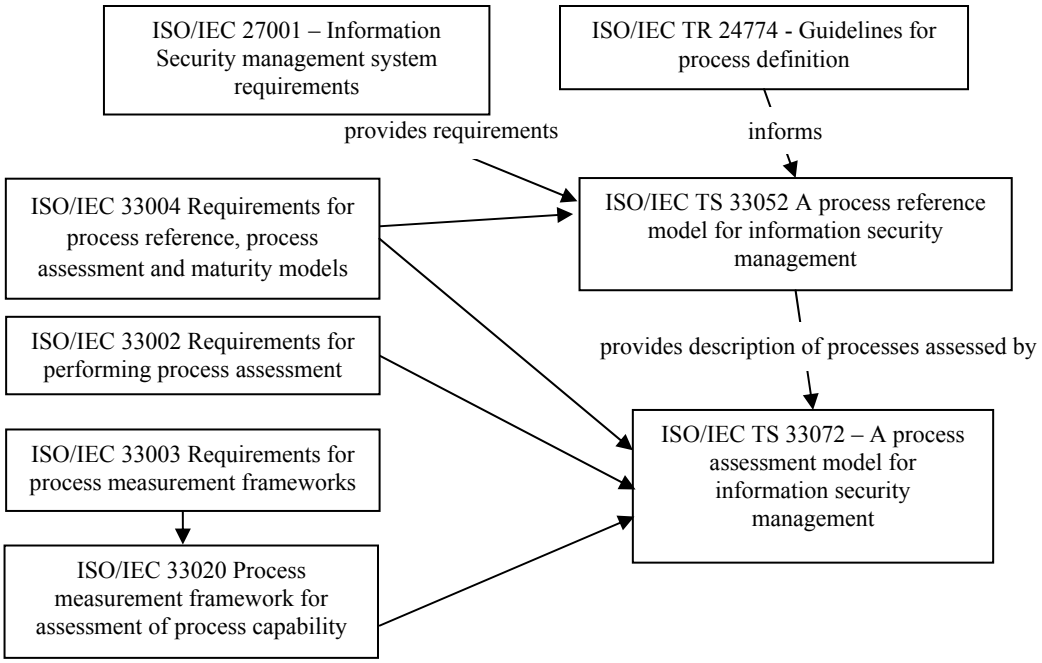

Figure 1 — Relationships between relevant standards

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;