TECHNICAL SPECIFICATION

# ISO/IEC TS 33052

First edition
2016-06-15

# Information technology — Process reference model (PRM) for information security management

*Technologies de l'information — Modèle de référence des procédés pour le management de la sécurité de l'information*

Reference number
ISO/IEC TS 33052:2016(E)

© ISO/IEC 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** ... **iv**

**Introduction** ... **v**

**1 Scope** ... **1**

**2 Normative references** ... **1**

**3 Terms and definitions** ... **1**

**4 Overview of the PRM** ... **1**

**5 Process descriptions** ... **2**

5.1 Introduction ... 2
5.2 ORG.1 Asset management ... 3
5.3 TEC.01 Capacity management ... 3
5.4 TEC.02 Change management ... 4
5.5 COM.01 Communication management ... 4
5.6 TEC.03 Configuration management ... 5
5.7 COM.02 Documentation management ... 5
5.8 ORG.2 Equipment management ... 6
5.9 ORG.3 Human resource employment management ... 7
5.10 COM.03 Human resource management ... 8
5.11 COM.04 Improvement ... 9
5.12 TEC.04 Incident management ... 9
5.13 ORG.4 Infrastructure and work environment ... 9
5.14 COM.05 Internal audit ... 11
5.15 TOP.1 Leadership ... 11
5.16 COM.06 Management review ... 12
5.17 COM.07 Non-conformity management ... 13
5.18 COM.09 Operational implementation and control ... 13
5.19 COM.08 Operational planning ... 15
5.20 COM.10 Performance evaluation ... 17
5.21 TEC.05 Product/service release ... 18
5.22 TEC.08 Product/Service/System requirements ... 18
5.23 COM.11 Risk and opportunity management ... 19
5.24 TEC.06 Service availability management ... 19
5.25 TEC.07 Service continuity management ... 20
5.26 ORG.5 Supplier management ... 20
5.27 TEC.09 Technical data preservation and recovery ... 21

**Annex A** (informative) **The relationship between management system requirements and a process reference model** ... **22**

**Annex B** (informative) **Statement of conformity to ISO/IEC 33004** ... **58**

**Bibliography** ... **60**

© 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.

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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


© ISO/IEC 2016 – All rights reserved

# Introduction

The purpose of this Technical Specification is to facilitate the development of a process assessment model (PAM) described in ISO/IEC TS 33072.

ISO/IEC 33002 describes the requirements for the conduct of an assessment. ISO/IEC 33020 describes the measurement scale for assessing the process quality characteristic of process capability. ISO/IEC 33001 describes the concepts and terminology used for process assessment.

A process reference model (PRM) is a model comprising definitions of processes described in terms of process purpose and outcomes, together with an architecture describing the relationships between the processes. Using the PRM in a practical application may require additional elements suited to the environment and circumstances.

The PRM specified in this Technical Specification describes the processes including the information security management system (ISMS) processes implied by ISO/IEC 27001. Each process of this PRM is described in terms of a purpose and outcomes and provides traceability to requirements. The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability required to fulfil the ISO/IEC 27001 requirements. The PRM is not intended to be used for a conformity assessment audit or as a process implementation reference guide.

The relationships between ISO/IEC TR 24774, ISO/IEC 27001, ISO/IEC 33002, ISO/IEC 33004, ISO/IEC 33020, ISO/IEC TS 33052 and ISO/IEC TS 33072 are shown in Figure 1.

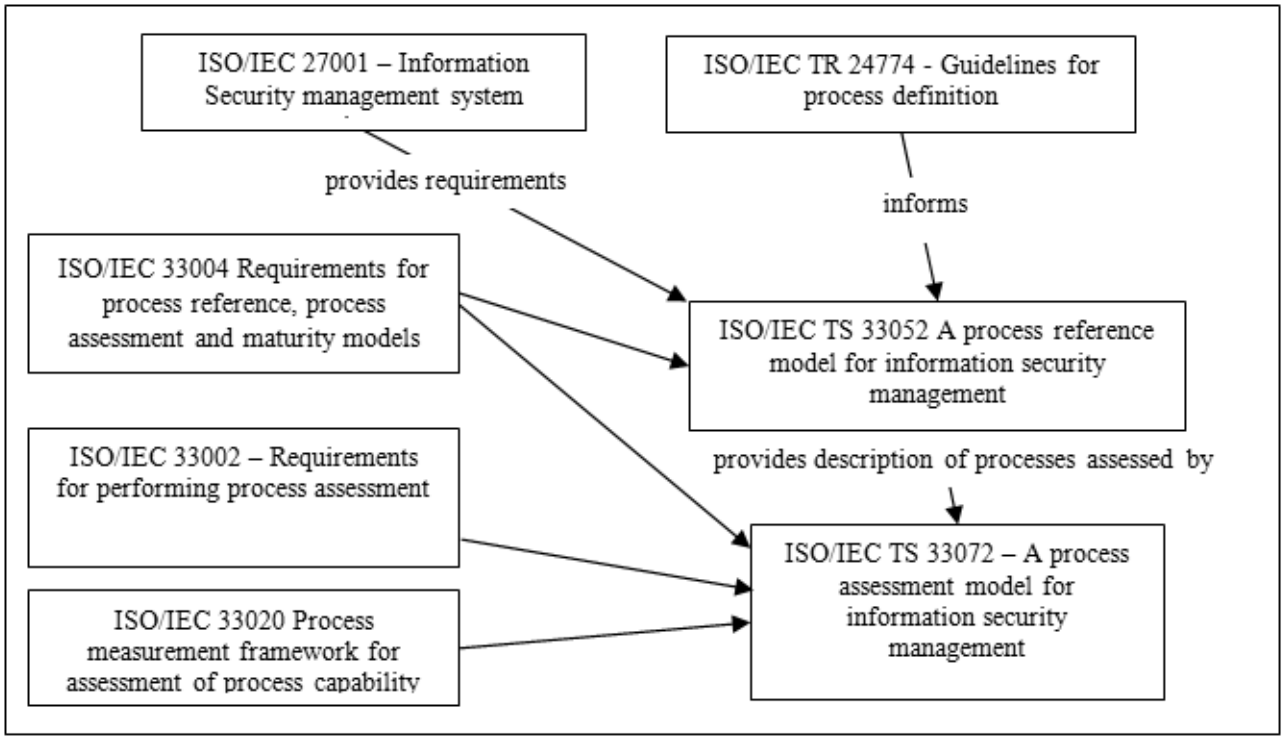



**Figure 1 — Relationships between relevant standards**

Any organization may define processes with additional elements in order to suit it to its specific environment and circumstances. Some processes cover general management aspects of an organization. These processes have been identified in order to give coverage to the requirements of ISO/IEC 27001.

The PRM does not provide the evidence required by ISO/IEC 27001. The PRM does not specify the interfaces between the processes.

© ISO/IEC 2016 – All rights reserved

This Technical Specification describes a PRM for information security management with descriptions of processes in Clause 5. Annex A provides the statement of conformity in accordance with ISO/IEC 33002.


© ISO/IEC 2016 – All rights reserved

# Information technology — Process reference model (PRM) for information security management

## 1 Scope

This Technical Specification defines a process reference model (PRM) for the domain of information security management. The model architecture specifies a process architecture for the domain and comprises a set of processes, with each described in terms of process purpose and outcomes.

## 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 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

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 27001 and ISO/IEC 33001 apply.

## 4 Overview of the PRM

This Clause describes the structure of a process reference model to support information security management. The process reference model includes processes, which can already exist in the context of a management system of a service provider.

Figure 2 identifies the processes derived from ISO/IEC 27001 requirements.

© ISO/IEC 2016 – All rights reserved