TECHNICAL SPECIFICATION

ISO/IEC TS 27022

First edition
2021-03

Information technology — Guidance on information security management system processes

Reference number
ISO/IEC TS 27022:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Structure and usage of this document ... **2**
5 Overview ... **3**
6 Management processes ... **6**
6.1 General ... 6
6.2 Information security governance/management interface process ... 7
7 Core processes ... **9**
7.1 General ... 9
7.2 Security policy management process ... 9
7.3 Requirements management process ... 10
7.4 Information security risk assessment process ... 13
7.5 Information security risk treatment process ... 14
7.6 Security implementation management process ... 17
7.7 Process to control outsourced services ... 19
7.8 Process to assure necessary awareness and competence ... 21
7.9 Information security incident management process ... 22
7.10 Information security change management process ... 25
7.11 Internal audit process ... 27
7.12 Performance evaluation process ... 29
7.13 Information security improvement process ... 31
8 Support processes ... **33**
8.1 General ... 33
8.2 Records control process ... 33
8.3 Resource management process ... 35
8.4 Communication process ... 37
8.5 Information security customer relationship management process ... 39
Annex A (informative) **Statement of conformity to ISO/IEC 33004** ... **41**
Bibliography ... **43**

© ISO/IEC 2021 – 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.

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) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2021 – All rights reserved

Introduction

An information security management system (ISMS) includes a collection of interacting processes and is operated by performing those processes. This document provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them.

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

The PRM specified in this document describes the ISMS processes implied by ISO/IEC 27001. The PRM is intended to be used as a process implementation and operation guide.

Any organization can define processes with additional elements in order to tailor it to its specific environment and circumstances. Some processes cover general management aspects of an organization. These processes have been identified in order to support organizations in addressing the requirements of ISO/IEC 27001.

© ISO/IEC 2021 – All rights reserved

Information technology — Guidance on information security management system processes

1 Scope

This document defines a process reference model (PRM) for the domain of information security management, which is meeting the criteria defined in ISO/IEC 33004 for process reference models (see Annex A). It is intended to guide users of ISO/IEC 27001 to:

— incorporate the process approach as described by ISO/IEC 27000:2018, 4.3, within the ISMS;

— be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes

— support users in the operation of an ISMS – this document is complementing the requirements-oriented perspective of ISO/IEC 27003 with an operational, process-oriented point of view.

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.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
core process
process that delivers apparent and direct customer value and is derived from the *core competencies* (3.1) of the management systems

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO 38500:2015.

Note 2 to entry: In this definition, "core competency" is understood as the set of skills and know-how present within a management system, directly aligned with the objectives of the management system, supporting the achievement of the objectives and not elsewhere present within the organization at a competitive level.

3.2
integrated management system
IMS
management system that integrates all of an organization's systems – like information security management and business continuity management – and processes in to one complete framework, enabling an organization to work as a single unit with unified objectives

© ISO/IEC 2021 – All rights reserved

3.3
key goal indicator
indicator that is an ex-post measure for the achievement of a goal/objective

3.4
key performance indicator
indicator that is an ex-ante measure, which allow a prediction if a goal/objective is achieved in the future

3.5
management process
process that defines the objectives of the management system to achieve the strategic objectives set by the organization's governing body

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

3.6
support process
process that supports core processes by providing and managing necessary resources without delivering direct customer value

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

4 Structure and usage of this document

The objective of this document is to guide the users of ISO/IEC 27001 on the operation of the ISMS. No additional requirements are defined within this document.

It is not intended to be used “out of the box” without adapting it to the implementing organization and it should not be used as requirements within ISMS certification audits.

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 results. The PRM is closely aligned to the information security requirements as contained in ISO/IEC 27001:2013. Processes are differentiated in core, management and supporting processes. The PRM is also meeting the criteria defined in ISO/IEC 33004 for process reference models.

Each process of this PRM is described in terms of:

— process category;

— brief description;

— process flowchart;

— objective/purposes;

— input and results;

— activities/functions;

— references.

The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability/maturity required to fulfil the ISO/IEC 27001 requirements.

The PRM provides a detailed but generic blueprint regarding the core processes of an ISMS. The PRM is applicable to all organizations independent of their size, objectives, business model, location, etc. The ISMS PRM should be used as a prototype for an ISMS, which needs to be tailored to the objectives, needs and individual requirements of the implementing organization. The tailoring of the PRM can include omission of some of the listed processes, where they are inapplicable or would be reduced to vestigial form.

© ISO/IEC 2021 – All rights reserved