INTERNATIONAL STANDARD

ISO/IEC 27009

Second edition
2020-04

Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements

Sécurité de l'information, cybersécurité et protection des données personnelles — Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences

Reference number
ISO/IEC 27009:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 ISO documents 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 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*.

This second edition cancels and replaces the first edition (ISO/IEC 27009:2016), which has been technically revised.

The main changes compared to the previous edition are as follows:

— the scope has been updated to more clearly reflect the content of this document;

— former Annex A has been divided into Annexes A and B;

— Annex C has been created.

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.

Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements

1 Scope

This document specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001, and complement or amend ISO/IEC 27002 to support a specific sector (domain, application area or market).

This document explains how to:

— include requirements in addition to those in ISO/IEC 27001,

— refine or interpret any of the ISO/IEC 27001 requirements,

— include controls in addition to those of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,

— modify any of the controls of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,

— add guidance to or modify the guidance of ISO/IEC 27002.

This document specifies that additional or refined requirements do not invalidate the requirements in ISO/IEC 27001.

This document is applicable to those involved in producing sector-specific standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirement 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*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

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
interpret
interpretation
explanation of an ISO/IEC 27001 requirement in a sector-specific context which does not invalidate any of the ISO/IEC 27001 requirements

Note 1 to entry: The explanation can pertain to either a requirement or guidance.

3.2
refine
refinement
supplementation or adaptation of an ISO/IEC 27001 requirement in a sector-specific context which does not remove or invalidate any of the ISO/IEC 27001 requirements

4 Overview of this document

4.1 General

ISO/IEC 27001 defines the requirements for establishing, implementing, maintaining and continually improving an information security management system. ISO/IEC 27001 states that its requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

ISO/IEC 27001:2013, Annex A, provides control objectives and controls. ISO/IEC 27001 requires an organization to "determine all controls that are necessary to implement the information security risk treatment option(s) chosen [see 6.1.3 b)]" and "compare the controls determined in 6.1.3 b) above with those in [ISO/IEC 27001:2013,] Annex A, and verify that no necessary controls have been omitted [see 6.1.3 c)]".

The guidance of control objectives and controls of ISO/IEC 27001:2013, Annex A, are included in ISO/IEC 27002.

ISO/IEC 27002 provides guidelines for information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment. The guidelines have a hierarchical structure that consists of clauses, control objectives, controls, implementation guidance and other information. The guidelines of ISO/IEC 27002 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

While ISO/IEC 27001 and ISO/IEC 27002 are widely accepted in organizations, including commercial enterprises, government agencies and not-for-profit organizations, there are needs for sector-specific versions of these standards.

EXAMPLES

The following documents have been developed to address these sector-specific needs are:

— ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

— ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*

— ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

— ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

— ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*

Other organizations have also produced standards addressing sector-specific needs.

Sector-specific standards should be consistent with the requirements of the information security management system. This document specifies requirements on how to create sector-specific standards that extend ISO/IEC 27001 and complement or amend ISO/IEC 27002 (see Clause 1).

This document assumes that all requirements from ISO/IEC 27001 that are not refined or interpreted, and all controls in ISO/IEC 27002 that are not modified, apply in the sector-specific context unchanged.

4.2 Structure of this document

Clause 5 provides requirements and guidance on how to make addition to, refinement or interpretation of ISO/IEC 27001 requirements.

Clause 6 provides requirements and guidance on how to provide control clauses, control objectives, controls, implementation guidance or other information that are additional to or modify ISO/IEC 27002 content.

Annex A contains a template which shall be used for sector-specific standards related to ISO/IEC 27001.

Annex B contains two templates which shall be used for sector-specific standards related to ISO/IEC 27002.

For sector-specific standards related to both ISO/IEC 27001 (see Clause 5) and ISO/IEC 27002 (see Clause 6), both Annex A and Annex B apply.

Annex C provides explanations about advantages and disadvantages of two different numbering approaches applied in the two templates in Annex B.

In this document, the following concepts are used to adapt ISO/IEC 27001 requirements for a sector:

— addition — see 5.2;

— refinement — see 5.3;

— interpretation — see 5.4.

In this document, the following concepts are used to adapt ISO/IEC 27002 guidance for a sector:

— addition — see 6.2;

— modification — see 6.3.

4.3 Expanding ISO/IEC 27001 requirements or ISO/IEC 27002 controls

Sector-specific standards related to ISO/IEC 27001 may add requirements or guidance to those of ISO/IEC 27001 or ISO/IEC 27002. The addition may expand the requirements or guidance beyond information security into their sector-specific topic.

EXAMPLE ISO/IEC 27018 uses such expansions. ISO/IEC 27018:2019, Annex A contains a set of controls aimed at the protection of personally identifiable information and, therefore, expands the scope of ISO/IEC 27018 to cover PII protection in addition to information security.

5 Addition to, refinement or interpretation of ISO/IEC 27001 requirements

5.1 General

Figure 1 illustrates how sector-specific requirements are constructed in relation to ISO/IEC 27001.

Figure 1 — Construction of sector-specific requirements

5.2 Addition of requirements to ISO/IEC 27001

Addition of requirements to ISO/IEC 27001 requirements is permitted.

EXAMPLE A sector which has additional requirements for an information security policy can add them to the requirements for the policy specified in ISO/IEC 27001:2013, 5.2.

No requirement that is added to those in ISO/IEC 27001 shall remove or invalidate any of the requirements defined in ISO/IEC 27001.

Where applicable, sector-specific additions to ISO/IEC 27001 requirements shall follow the requirements and guidance set out in Annex A.

5.3 Refinement of requirements in ISO/IEC 27001

Refinement of ISO/IEC 27001 requirements is permitted.

NOTE Refinements do not remove or invalidate any of the requirements in ISO/IEC 27001 (see 3.2).

Where applicable, sector-specific refinements of ISO/IEC 27001 requirements shall follow the requirements and guidance set out in Annex A.

EXAMPLE 1 A sector-specific standard could contain controls additional to ISO/IEC 27001:2013, Annex A. In this case, the requirements related to information security risk treatment in ISO/IEC 27001:2013, 6.1.3 c) and d) need to be refined to include the additional controls given in the sector-specific standard.

Specification of a particular approach to meeting requirements in ISO/IEC 27001 is also permitted.

EXAMPLE 2 A particular sector has a prescribed way to determine the competence of people working within the scope of the sector-specific management system. This requirement could refine the general requirement in ISO/IEC 27001:2013, 7.2.

5.4 Interpretation of requirements in ISO/IEC 27001

Interpretation of ISO/IEC 27001 requirements is permitted.

NOTE Interpretations do not invalidate any of the ISO/IEC 27001 requirements but explain them or place them into sector-specific context (see 3.1).

Where applicable, sector-specific interpretations of ISO/IEC 27001 requirements shall follow the requirements and guidance set out in Annex A.

6 Additional or modified ISO/IEC 27002 guidance

6.1 General

Figure 2 illustrates how ISO/IEC 27002 guidance can be added to or modified.

Figure 2 — Construction of sector-specific guidance

Each control shall only contain one instance of the word "should".

NOTE In ISO/IEC 27001, Information security risk treatment requires an organization to state controls that have been determined and justification of inclusions, and justification for exclusions of controls from ISO/IEC 27001:2013, Annex A. Having only one use of "should" within a control statement eliminates the possibility of ambiguity over the scope of the control.

6.2 Additional guidance

Addition of clauses, control objectives, controls, implementation guidance and other information to ISO/IEC 27002 is permitted.

Where applicable, clauses, control objectives, controls, implementation guidance and other information additional to ISO/IEC 27002 shall follow the requirements and guidance set out in Annex B.

Before specifying additional clauses, control objectives or controls, entities producing sector-specific standards related to ISO/IEC 27001 should consider whether a more effective approach would be to modify existing ISO/IEC 27002 content, or achieve the desired result just through the addition of sector-specific control objectives (instead of adding clauses), controls (instead of control objectives), implementation guidance and other information (instead of controls) to the existing ISO/IEC 27002 content.

6.3 Modified guidance

Clauses, controls and their control objectives contained in ISO/IEC 27002 shall not be modified.

If there is a sector-specific need to include a control objective that contradicts a control objective contained in ISO/IEC 27002, a new sector-specific control objective shall be introduced. The new control objective shall have at least one sector-specific control. If there is a sector-specific need to include a control that contradicts a control contained in ISO/IEC 27002, a new sector-specific control shall be introduced.

Modification of implementation guidance and other information from ISO/IEC 27002 is permitted.

Where applicable, modified clauses, control objectives, controls, implementation guidance and other information from ISO/IEC 27002 shall follow the requirements and guidance set out in Annex B.

Annex A
(normative)

Template for developing sector-specific standards related to ISO/IEC 27001 and optionally ISO/IEC 27002

A.1 Drafting instructions

In A.2, the following formatting conventions are used:

— the text in angle brackets should be replaced by suitable sector-specific text.

EXAMPLE For the telecommunications sector, the title of Clause 4 of the template in A.2, “<Sector>-specific requirements" is adapted as “Telecommunications-specific requirements".

— the text in braces and italics indicates how to use this part of the template; this text should be deleted in the final version of the sector-specific standard.

— the text written without special formatting should be copied verbatim.

A.2 Template

Introduction

{Include how the requirements contained within this document relate to the requirements specified within ISO/IEC 27001 and optionally how the guidance contained within the standard relate to the guidance in ISO/IEC 27002 if the sector-specific standard is also related to ISO/IEC 27002.}

{Insert the following text.}

This document is NOT a new management system standard independent of ISO/IEC 27001, but rather specifies <sector>-specific requirements that are composed of refinements of and/or additions to requirements in ISO/IEC 27001.

{If the sector-specific standard is also related to ISO/IEC 27002, insert the following text instead of the above.}

This document is NOT a new management system standard independent of ISO/IEC 27001, but rather:

a) specifies <sector>-specific requirements that are composed of refinements of and/or additions to requirements in ISO/IEC 27001; and

b) specifies <sector>-specific guidance that supports additions to and/or modifications of ISO/IEC 27002 (see Clause 6).

1 Scope

{Include appropriate scope statements including the relationship of the standard to ISO/IEC 27001 and optionally ISO/IEC 27002 if the sector-specific standard is also related to ISO/IEC 27002.}

2 Normative references

{Insert the relevant normative references, including ISO/IEC 27001 and optionally ISO/IEC 27002.}

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

3 Terms and definitions

{Insert the following text to ensure that ISO/IEC 27000 is included.}

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

4 <Sector>-specific requirements related to ISO/IEC 27001:2013

4.1 General

{Insert the following text.}

All requirements from ISO/IEC 27001:2013, Clauses 4 to 10, that do not appear below shall apply unchanged.

{Add all sector-specific requirements. When adding a requirement, check first whether it is related to a requirement already existing in ISO/IEC 27001. If additional requirements relate to existing requirements from ISO/IEC 27001, add a title to them with a prefix of at least three letters for the sector, followed by the subclause number and the original title of the subclause from ISO/IEC 27001.

EXAMPLE ***4.2 CLD 4.1 Understanding the organization and its context.***

If there is no relation to an existing requirement, place the additional requirement as a new subclause at the end after all other subclauses in Clause 4 of the sector-specific standard.}

{Optionally, a sector-specific standard may have a table which indicates the relationship between the (sub) clause of the sector-specific standard and those of ISO/IEC 27001. A table is a useful tool which helps readers understand the placement of the clauses of the sector-specific standard compared to those of ISO/IEC 27001.}

Table 1 — Correspondence of <sector>-specific requirements with ISO/IEC 27001

Subclause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks

{Indicate sector-specific requirements that are additional to the ISO/IEC 27001 requirements by insertion of the following text.}

In addition to ISO/IEC 27001:2013, <clause/subclause number>, the following applies.

{Indicate sector-specific requirements that refine ISO/IEC 27001:2013 requirements by insertion of the following text.}

ISO/IEC 27001:2013, <clause/subclause number> is refined as follows.

{Indicate sector-specific requirements that interpret ISO/IEC 27001:2013 requirements by insertion of the following text.}

ISO/IEC 27001:2013, <clause/subclause number> is interpreted as follows.

{If possible, show the added, refined or interpreted text by use of italics.}

{If the sector-specific standard has sector-specific controls, always insert the following text.}

ISO/IEC 27001:2013, 6.1.3 c), is refined as follows.