SLOVENSKI STANDARD
oSIST ISO/IEC DIS 27009:2019

01-september-2019

Informacijska tehnologija - Varnostne tehnike - Uporaba ISO/IEC 27001 za določen sektor - Zahteve

Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements

Technologies de l'information -- Techniques de sécurité -- Application de lISO/IEC 27001 à un secteur spécifique -- Exigences

Ta slovenski standard je istoveten z: **ISO/IEC DIS 27009:2019**

ICS:

03.100.70	Sistemi vodenja	Management systems
03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

oSIST ISO/IEC DIS 27009:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27009

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2019-06-28

Voting terminates on:
2019-09-20

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

Technologies de l'information — Techniques de sécurité — Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences

ICS: 03.100.70; 35.030

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27009:2019(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, *IT Security techniques*.

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 was updated to more clearly reflect the content of this document;

— the template in the previous Annex A was divided into two annexes – Annex A for a sector-specific standard related to ISO/IEC 27001:2013 and Annex B for a sector-specific standard related to ISO/IEC 27002:2013 (for a standard related to both ISO/IEC 27001:2013 and ISO/IEC 27002:2013, Annex A and Annex B can be jointly used in accordance with instructions provided in Annex A);

— Annex C was newly produced to provide explanation on two numbering approaches presented in B.2 and B.3 to help readers when they decide to apply one of the two approaches to their sector-specific standards.

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.

[Revision Criteria Notes:

In responding to the CD ballot for ISO/IEC 27009, WG 1 would like to draw National Bodies attention to the following revision criteria that has been identified and discussed at the previous WG 1 editing meetings (Berlin October 2017, Wuhan April 2018 and Gjøvik September 2018- see also WG 1 N1326 editors meeting report). WG 1 would therefore request National Body comments, that are submitted as a result of this ballot, take account of the criteria in order that the issues raised in this criteria are resolved and finalised.

Revision Criteria

a. *There should be two or three different templates;*

Two types of templates were discussed in response to the comments in N987 and N930 that clarification is necessary on how sector-specific standards can be produced in accordance with ISO/IEC 27009, Annex A.

These templates are: one for refinements of ISO/IEC 27001 and the other for additions or modifications to ISO/IEC 27002. Editors will include the two templates in the WD as a starting point.

Once this is finalized, the situation will be reviewed and it will be decided whether a combined template for ISO/IEC 27001 & ISO/IEC 27002 will be needed.

-->For a sector-specific standard that relates to both ISO/IEC 27001 and ISO/IEC 27002, it was decided to apply both Annex A and Annex B instead of having the combined template at the Gjøvik meeting.

b. *Explanatory text should be added in the template (and maybe also in the main body) to make things clearer for the end user of the new standards;*

It was agreed that ambiguity in the application of Annex A of ISO/IEC 27009, which was raised in N930, should be resolved by adding a sentence to explain that ISO/IEC 27009 is in place to enable entities, such as ISO committees, to produce sector-specific standards based on ISO/IEC 27001 and/or ISO/IEC 27002; it is not the intent that new management standards are produced.

--> The text was discussed and modified at the Wuhan meeting - see "0 Introduction" of Annex A and Annex B.

c. *No specific title for the sector-specific standards;*

It was confirmed that it was already agreed to remove the specific title for the sector-specific standards at the Abu-Dhabi meeting. Editors removed the text related to this point in this document. (--> this was resolved.)

d. *Numbering of the sector-specific controls;*

This topic was discussed in the ISO/IEC 27009 revision meeting and also in the meeting for SD 8 (27009 Use Cases). The final agreements made in these meetings are:

Both options (the one applied by ISO/IEC 27010, ISO/IEC 27011 and ISO/IEC 27017, and the one applied by ISO/IEC 27019) will be included in the text.

It was agreed that editors will include these two numbering approaches with descriptive text (background) for information so that the two approaches can be compared. An Editor's note asking for comments will also be included.

The ITTF secretariat kindly attended the meeting and advised us that ITTF can accept letter prefixes to ISO/IEC 27002 numbers, conceptually they then become unnumbered headings which are permissible.

--> at the Wuhan meeting, it was discussed and agreed to have both approaches in Annex B and add a new Annex C for guidance to the approaches – see Annex B and Annex C.

e. *The scope might need to be updated to clarify the purpose of the document*

It was pointed out that due care should be taken for scope change since it needs a ballot that will affect the schedule of the ISO/IEC 27009 revision, and agreed to add following editors' note from experts:

Editor's note: if there is any problems with the current scope and title, please provide explanation and example if you have any such cases.

--> The scope was modified based on the comments to the editors' note and agreed at the Wuhan meeting –, the JTC 1 endorsed the scope change (see SC 27 WG 1 N1468). It was also decided that 27009 is for those who produce sector-specific standards that extend ISO/IEC 27001:2013 and complement or amend ISO/IEC 27002, which mean that the sector-specific standards solely based on ISO/IEC 27002 without any link to ISO/IEC 27001 are out of the scope of 27009.)

As the general structure and content of ISO/IEC 27009:2016 were agreed to by all National Bodies, it was also agreed that the above points constitute the targets of the revision at the meeting in Berlin, October 2017.]

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

1 Scope

This document specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001:2013, and complement or amend ISO/IEC 27002:2013 to support a specific sector (domain, application area or market).

This document explains how to;

— include requirements in addition to those in ISO/IEC 27001:2013,

— refine or interpret any of the ISO/IEC 27001:2013 requirements,

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

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

— add guidance to or modify the guidance of ISO/IEC 27002:2013.

This document specifies that additional or refined requirements do not invalidate the requirements in ISO/IEC 27001:2013.

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

ISO/IEC 27002:2013, *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:

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

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

3.1
interpret
interpretation
explanation of an ISO/IEC 27001:2013 requirement in a sector-specific context which does not invalidate any of the ISO/IEC 27001:2013 requirements

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

3.2
refine
refinement
supplementation or adaptation of an ISO/IEC 27001:2013 requirement in a sector-specific context which does not remove or invalidate any of the ISO/IEC 27001:2013 requirements

4 Overview of this document

4.1 General

ISO/IEC 27001:2013 is an International Standard that defines the requirements for establishing, implementing, maintaining and continually improving an information security management system. ISO/IEC 27001:2013 states that its requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

NOTE Management system standards within ISO are built in accordance with *ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2018*.[1]

ISO/IEC 27001:2013 includes normative Annex A which provides control objectives and controls. ISO/IEC 27001:2013 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 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 27002:2013.”

ISO/IEC 27002:2013 is an International Standard that 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 27002:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

While ISO/IEC 27001:2013 and ISO/IEC 27002:2013 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 of standards which have been developed to address these sector-specific needs are:

— ISO/IEC 27010[2], Information security management for inter-sector and inter-organizational communications;

— ISO/IEC 27011[3], Code of practice for information security controls based on ISO/IEC 27002:2013 for telecommunications organizations;

— ISO/IEC 27017[4], Code of practice for information security controls based on ISO/IEC 27002:2013 for cloud services;

— ISO/IEC 27018[5], Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; and

— ISO/IEC 27019:2017[6], Information security controls for the energy utility industry.

Organizations outside of ISO/IEC 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 27001:2013 and complement or amend ISO/IEC 27002:2013 (see Clause 1).

This document assumes that all requirements from ISO/IEC 27001:2013 that are not refined or interpreted, and all controls in ISO/IEC 27002:2013 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 27001:2013 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 27002:2013 content.

Annex A contains a template which should be used for sector-specific standards related to ISO/IEC 27001:2013.

Annex B contains two templates which should be used for sector-specific standards related to ISO/IEC 27002:2013.

For sector-specific standards related to both ISO/IEC 27001:2013 (see Clause 5) and ISO/IEC 27002:2013 (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.

Within this document, the following concepts are used to adapt ISO/IEC 27001:2013 requirements for a sector:

— Addition – see 5.2;

— Refinement – see 5.3;

— Interpretation – see 5.4.

Within this document, the following concepts are used to adapt ISO/IEC 27002:2013 guidance for a sector:

— Addition – see 6.2;

— Modification – see 6.3.

NOTE Any sector-specific guidance that is developed following the requirements and guidance in this document cannot be contained within a Technical Report. The ISO/IEC Directives[1] define a Technical Report as a document that does not contain requirements, and any sector-specific standard developed based on this document contains requirements (see Clause 4 of the template in A.2, Clause 5 of the template in B.2, and 4.2 of the template in B.3).

4.3 Expanding ISO/IEC 27001:2013 requirements or ISO/IEC 27002:2013 controls

Sector-specific standards related to ISO/IEC 27001:2013 may add requirements or guidance to those of ISO/IEC 27001:2013 or ISO/IEC 27002:2013. The addition may expand the requirements or guidance beyond information security into their sector-specific topic.

EXAMPLE ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* uses such expansions. ISO/IEC 27018:2014[5], Annex A contains a set of controls aimed at the protection of personally identifiable information and, therefore, expands the scope of ISO/IEC 27018[5] to cover PII protection in addition to information security.