INTERNATIONAL STANDARD

ISO/IEC 27009

First edition
2016-06-15

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

Reference number
ISO/IEC 27009:2016(E)

© ISO/IEC 2016

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

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

© ISO/IEC 2016 – All rights reserved

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

© 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*, SC 27, *IT Security techniques*.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

 © ISO/IEC 2016 – All rights reserved

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

1 Scope

This International Standard defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC 27001:2013, Annex A.

This International Standard ensures that additional or refined requirements are not in conflict with the requirements in ISO/IEC 27001.

This International Standard is applicable to those involved in producing sector-specific standards that relate to ISO/IEC 27001.

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 27000:2016, *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.

3.1
interpretation
explanation (in form of requirement or guidance) of an ISO/IEC 27001 requirement in a sector-specific context which does not invalidate any of the ISO/IEC 27001 requirements

3.2
refinement
sector-specific specification of an ISO/IEC 27001 requirement which does not remove or invalidate any of the ISO/IEC 27001 requirements

4 Overview of this International Standard

4.1 General

ISO/IEC 27001 is an International Standard that defines the requirements for establishing, implementing, maintaining and continually improving an information security management system.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

© ISO/IEC 2016 – All rights reserved

It 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, 2016*.[1]

ISO/IEC 27002 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 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

The control objective and controls of ISO/IEC 27002 are listed in Annex A of ISO/IEC 27001:2013 in a normative form. 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))".

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 emerging 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] Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;

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

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

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 International Standard provides requirements for how to add to, refine or interpret the requirements of ISO/IEC 27001 and how to add or modify the guidelines of ISO/IEC 27002 for sector-specific use.

This International Standard 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, will apply in the sector-specific context unchanged.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

4.2 Structure of this International Standard

Clause 5 provides requirements and guidance on how to define requirements that are additional to, refinement or interpretation of ISO/IEC 27001 requirements.

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

Annex A contains a template which should be used for sector-specific standards related to ISO/IEC 27001 and/or ISO/IEC 27002.

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

— Addition – see 5.2

© ISO/IEC 2016 – All rights reserved

— Refinement – see 5.3

— Interpretation – see 5.4.

Within this International Standard, the following concepts are used to adapt ISO/IEC 27002 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 International Standard 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 International Standard, particularly Annex A, will contain at least a minimum set of requirements (see clause 4.1 of the template in A.2).

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, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* uses such expansions. ISO/IEC 27018:2014, Annex A[5] 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.

5 Additional, refined or interpreted ISO/IEC 27001 requirements

5.1 General

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

Figure 1 — Construction of sector-specific requirements

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

5.2 Additional requirements

Specification of additional 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. Sector-specific additions to ISO/IEC 27001 requirements shall, where possible, follow the requirements and guidance set out in Annex A of this International Standard.

© ISO/IEC 2016 – All rights reserved

5.3 Refined requirements

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).

Sector-specific refinements of ISO/IEC 27001 requirements shall, where possible, follow the requirements and guidance set out in Annex A of this International Standard.

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 sectors-specific management system. This requirement could refine the general requirement in ISO/IEC 27001:2013, 7.2.

5.4 Interpreted requirements

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).

Sector-specific interpretations of ISO/IEC 27001 requirements shall, where possible, follow the requirements and guidance set out in Annex A of this International Standard.

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 27001:2013, 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 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

 © ISO/IEC 2016 – All rights reserved

Clauses, control objectives, controls, implementation guidance and other information additional to ISO/IEC 27002 shall, where possible, follow the requirements and guidance set out in Annex A of this International Standard.

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 through the addition of sector-specific control objectives, controls, implementation guidance and other information to the existing ISO/IEC 27002 content.

6.3 Modified guidance

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

No modification shall remove, invalidate or reduce any of the controls in ISO/IEC 27002.

Modified clauses, control objectives, controls, implementation guidance and other information from ISO/IEC 27002 shall, where possible, follow the requirements and guidance set out in Annex A of this International Standard.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

© ISO/IEC 2016 – All rights reserved

Annex A
(normative)

Template for developing sector-specific standards related to ISO/IEC 27001:2013 or ISO/IEC 27002:2013

A.1 Drafting instructions

Within A.2 the following formatting convention is used:

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

EXAMPLE For the sector telecommunications, the title of Clause 4 of the template in A.2, "<Sector>-specific requirements …", should read "Telecommunications-specific requirements …".

— 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.

— Text written without special formatting should be copied verbatim.

A sector-specific standard should use the following naming convention: Information security management system for <sector>.

A.2 Template

0 Introduction

{*Include how the requirements and/or guidance contained within this standard relate to the requirements specified within* ISO/IEC 27001 *and the guidance within* ISO/IEC 27002.}

1 Scope

{*Include appropriate scope statements including the relationship of this standard to* ISO/IEC 27001 *and* ISO/IEC 27002.}

2 Normative references

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

3 Terms and definitions

{*Ensure that* ISO/IEC 27000 *is included.*}

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

{*Always insert the following text.*}

4.1 Structure of this standard

This is a sector-specific <document type> related to ISO/IEC 27001.

{*If the sector-specific standard has sector-specific clauses, control objectives or controls additional to or modified from* ISO/IEC 27002 *insert the following text.*}

The <sector>-specific reference control objectives and controls are listed in Annex A.

{*Insert further subclauses describing sector-specific ISMS issues, if any.*}

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

 © ISO/IEC 2016 – All rights reserved

4.2 < Sector >-specific requirements

{*Insert one of the following two texts, as appropriate.*}

All requirements from ISO/IEC 27001:2013, Clauses 4 to 10 apply unchanged. {*or*}

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

{*Add all sector-specific requirements. For additional requirements, use clause/subclause numbering in the same format as* ISO/IEC 27001:2013*, but with a prefix of at least three letters for the sector. When adding a requirement, check first whether it is related to a requirement already existing in* ISO/IEC 27001:2013*. If it is, add the new requirement following the one it is related to and number it as appropriate. If there is no relation to an existing requirement, place the additional requirements after the* ISO/IEC 27001:2013*-related requirements, introducing new subsequent numbering of clauses, as suitable.*}

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

A requirement additional to ISO/IEC 27001:2013 <clause/sub-clause number> is:

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

ISO/IEC 27001:2013 requirement <clause/sub-clause 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 requirement <clause/sub-clause 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 requirement 6.1.3 c) is refined as follows:

Compare the controls determined in 6.1.3 b) above with those in ISO/IEC 27001:2013, Annex A and with Annex A of this <document type> to verify that no necessary controls have been omitted.

ISO/IEC 27001:2013 requirement 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls (see ISO/IEC 27001:2013, 6.1.3 b) and c)),

— justification for their inclusion,

— whether the necessary controls are implemented or not, and

— justification for excluding any of the controls in ISO/IEC 27001:2013, Annex A or Annex A of this <document type>.

{*To mandate the application of particular controls, always insert the following text next to* ISO/IEC 27001:2013, 6.1.3 d*) and identify the mandated controls in a suitable way, preferably by using (M) as a prefix for the control number.*}

The organization shall implement the mandatory controls identified by <X>.

5 <Sector>-specific guidance related to ISO/IEC 27002:2013

{*If the sector-specific standard has sector-specific clauses, control objectives, controls, implementation guidance or other information additional to or modified from* ISO/IEC 27002:2013*, insert them in this clause. Number additional clauses, control objectives or controls in the same format as* ISO/IEC 27002:2013*, but with a prefix of at least three letters for the sector. When adding or modifying control objectives,*

IECNORM.COM : Click to view the full PDF of ISO/IEC 27009:2016

© ISO/IEC 2016 – All rights reserved