TECHNICAL REPORT

ISO/IEC TR 27023

First edition
2015-07-01

Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

Technologies de l'information — Techniques de sécurité — Mappage des édtions révisées de l'ISO/IEC 27001 et de l'ISO/IEC 27002

Reference number
ISO/IEC TR 27023:2015(E)

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

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*.

Introduction

Both standards, ISO/IEC 27001 and ISO/IEC 27002, have been revised as part of the normal standards maintenance process, and the results of this revision process are contained in ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

This Technical Report contains the following tables:

— Clause 4, Table 1 — Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005;

— Clause 5, Table 2 — Comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013;

— Clause 5, Table 3 — Comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005.

These tables can be used to determine where requirements or controls in the old standards went, or where requirements or controls in the new standards have come from. Where a relationship is stated, it does not mean that the content is identical.

This Technical Report is designed to provide a factual correspondence between the old and new editions of ISO/IEC 27001 and ISO/IEC 27002 respectively, and so by intention it does not provide any explanatory commentary on why a change has been made or the significance of the change. Users of this Technical Report need to evaluate the significance of the changes in context with regard to their particular application and implementation of the revised editions of these standards.

For ISO/IEC 27002, the comparison was based on control objectives, controls, and implementation guidance.

Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

1 Scope

The purpose of this Technical Report is to show the corresponding relationship between the revised versions of ISO/IEC 27001 and ISO/IEC 27002.

This Technical Report will be useful to all users migrating from the 2005 to the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002.

2 Normative references

The following referenced documents are indispensable for the application 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 27000:2014, *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 contained in ISO/IEC 27000:2014 apply.

4 Comparison between revised editions of ISO/IEC 27001

Table 1 — Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
4.1	Understanding the organization and its context	8.3	Preventive action
4.2 a)	Understanding the needs and expectations of interested parties		New requirement
4.2 b)	Understanding the needs and expectations of interested parties	5.2.1 c)	Provision of resources
		7.3 c) 4)	Review output
		7.3 c) 5)	Review output
4.3	Determining the scope of the information security management system	4.2.1 a)	Establish the ISMS
4.3 a)	Determining the scope of the information security management system	4.2.1 a)	Establish the ISMS
		4.2.3 f)	Monitor and review the ISMS
4.3 b)	Determining the scope of the information security management system	4.2.3 f)	Monitor and review the ISMS

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
4.3 c)	Determining the scope of the information security management system		New requirement
4.3	Determining the scope of the information security management system – Last sentence	4.3.1 b)	General
		4.3.2 f)	Control of documents
4.4	Information security management system	4.1	General requirements
		5.2.1 a)	Provision of resources
5.1 a)	Leadership and commitment	4.2.1 b) 3)	Establish the ISMS
		5.1 a), b)	Management commitment
5.1 b)	Leadership and commitment		New requirement
5.1 c)	Leadership and commitment	5.1 e)	Management commitment
5.1 d)	Leadership and commitment	5.1 d)	Management commitment
5.1 e)	Leadership and commitment	5.1 b), g), h)	Management commitment
5.1 f)	Leadership and commitment	5.1 b), g), h)	Management commitment
5.1 g)	Leadership and commitment	5.1 a), d), g), h)	Management commitment
5.1 h)	Leadership and commitment	5.1	Management commitment
5.2	Policy – First sentence	4.2.1 b) 5)	Establish the ISMS
		5.1 a)	Management commitment
5.2 a)	Policy	4.2.1 b)	Establish the ISMS
5.2 b)	Policy	4.2.1 b) 1)	Establish the ISMS
5.2 c)	Policy	4.2.1 b) 2)	Establish the ISMS
	Policy	4.3.3	Control of records
5.2 d)	Policy	5.1 d)	Management commitment
5.2 e)	Policy	4.3.1 a)	General
5.2 f)	Policy	5.1 d)	Management commitment
5.2 g)	Policy	4.3.2 f)	Control of documents
5.3	Organizational roles, responsibilities and authorities – First sentence	5.1 c)	Management commitment
		6	Internal ISMS audits
5.3 a)	Organizational roles, responsibilities and authorities	4.3.3	Control of records
		5.1 c)	Management commitment
		6	Internal ISMS audits
5.3 b)	Organizational roles, responsibilities and authorities	4.3.3	Control of records
		5.1 c)	Management commitment
		6	Internal ISMS audits
6.1.1	Actions to address risks and opportunities – General	4.2.1 d)	Establish the ISMS
		8.3 a)	Preventive action
6.1.1 a)	Actions to address risks and opportunities – General		New requirement

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
6.1.1 b)	Actions to address risks and opportunities – General		New requirement
6.1.1 c)	Actions to address risks and opportunities – General		New requirement
6.1.1 d)	Actions to address risks and opportunities – General	4.2.1 e) 4)	Establish the ISMS
	Actions to address risks and opportunities – General	8.3 b), c)	Preventive action
6.1.1 e) 1)	Actions to address risks and opportunities – General	4.2.2 a)	Implement and operate the ISMS
	Actions to address risks and opportunities – General	8.3 c)	Preventive action
6.1.1 e) 2)	Actions to address risks and opportunities – General	8.3 e)	Preventive action
6.1.2	Information security risk assessment – First sentence	4.2.1 c) 1)	Establish the ISMS
6.1.2 a)	Information security risk assessment		New requirement
6.1.2 a) 1)	Information security risk assessment	4.2.1 b) 4), c) 2	Establish the ISMS
	Information security risk assessment	5.1 f)	Management commitment
6.1.2 a) 2)	Information security risk assessment		New requirement
6.1.2 b)	Information security risk assessment	4.2.1 c)	Establish the ISMS
6.1.2 c)	Information security risk assessment	4.2.1 d)	Establish the ISMS
6.1.2 c) 1)	Information security risk assessment	4.2.1 d) 1), 2), 3), 4)	Establish the ISMS
6.1.2 c) 2)	Information security risk assessment	4.2.1 d) 1)	Establish the ISMS
6.1.2 d) 1)	Information security risk assessment	4.2.1 e) 1)	Establish the ISMS
6.1.2 d) 2)	Information security risk assessment	4.2.1 e) 2)	Establish the ISMS
6.1.2 d) 3)	Information security risk assessment	4.2.1 e) 3)	Establish the ISMS
6.1.2 e) 1)	Information security risk assessment	4.2.1 e) 4)	Establish the ISMS
6.1.2 e) 2)	Information security risk assessment	4.2.1 e) 4)	Establish the ISMS
6.1.2	Information security risk assessment-Last sentence	4.3.1 d), e)	General
6.1.3	Information security risk treatment	4.2.1 f)	Establish the ISMS
6.1.3 a)	Information security risk treatment	4.2.1 f) 1), 2), 3), 4)	Establish the ISMS
6.1.3 b)	Information security risk treatment	4.2.1 g)	Establish the ISMS
6.1.3 c)	Information security risk treatment		New requirement
6.1.3 d)	Information security risk treatment	4.2.1 j) 1), 2), 3)	Establish the ISMS
	Information security risk treatment	4.3.1 i)	General
6.1.3 e)	Information security risk treatment	4.2.2 a)	Implement and operate the ISMS
6.1.3 f)	Information security risk treatment	4.2.1 h)	Establish the ISMS

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
6.1.3	Information security risk treatment-Last sentence	4.3.1 f)	General
6.2	Information security objectives and plans to achieve them-First sentence	5.1 b)	Management commitment
6.2 a)	Information security objectives and plans to achieve them	5.1 d)	Management commitment
6.2 b)	Information security objectives and plans to achieve them		New requirement
6.2 c)	Information security objectives and plans to achieve them		New requirement
6.2 d)	Information security objectives and plans to achieve them	5.1 d)	Management commitment
6.2 e)	Information security objectives and plans to achieve them	4.2.3 b)	Monitor and review the ISMS
6.2	Information security objectives and plans to achieve them-Last sentence	4.3.1 a)	General
6.2 f)	Information security objectives and plans to achieve them		New requirement
6.2 g)	Information security objectives and plans to achieve them		New requirement
6.2 h)	Information security objectives and plans to achieve them		New requirement
6.2 i)	Information security objectives and plans to achieve them		New requirement
6.2 j)	Information security objectives and plans to achieve them	4.2.3 b)	Monitor and review the ISMS
7.1	Resources	4.2.2 b), g)	Implement and operate the ISMS
		5.2.1	Provision of resources
7.2 a)	Competence	5.2.2 a)	Training, awareness and competence
7.2 b)	Competence	5.2.2	Training, awareness and competence
7.2 c)	Competence	5.2.2 b), c)	Training, awareness and competence
7.2 d)	Competence	5.2.2 d)	Training, awareness and competence
7.3 a)	Awareness		New requirement
7.3 b)	Awareness	4.2.2 e)	Implement and operate the ISMS
		5.2.2	Training, awareness and competence
7.3 c)	Awareness	4.2.2 e)	Implement and operate the ISMS
		5.2.2	Training, awareness and competence
7.4	Communication-First sentence	4.2.4 c)	Maintain and improve the ISMS
		5.1 d)	Management commitment
7.4 a)	Communication	4.2.4 c)	Maintain and improve the ISMS
		5.1 d)	Management commitment
7.4 b)	Communication		New requirement

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
7.4 c)	Communication	4.2.4 c)	Maintain and improve the ISMS
		5.1 d)	Management commitment
7.4 d)	Communication		New requirement
7.4 e)	Communication		New requirement
7.5.1 a)	General	4.3.1 a), b), h), i)	General
7.5.1 b)	General		New requirement
7.5.2 a)	Creating and updating	4.3.2 c), e), j)	Control of documents
		4.3.3	Control of records
7.5.2 b)	Creating and updating		New requirement
7.5.2 c)	Creating and updating	4.3.2 a), b)	Control of documents
7.5.3	Control of documented information – First sentence	4.3.2	Control of documents
7.5.3 a)	Control of documented information	4.3.2 d), f)	Control of documents
		4.3.3	Control of records
7.5.3 b)	Control of documented information	4.3.2	Control of documents
		4.3.3	Control of records
7.5.3 c)	Control of documented information	4.3.2 f), h), i)	Control of documents
		4.3.3	Control of records
7.5.3 d)	Control of documented information	4.3.2 f), h)	Control of documents
		4.3.3	Control of records
7.5.3 e)	Control of documented information	4.3.2 c) d)	Control of documents
7.5.3 f)	Control of documented information	4.3.2 f), j)	Control of documents
		4.3.3	Control of records
7.5.3	Control of documented information – Last paragraph	4.3.2 g)	Control of documents
8.1	Operational planning and control – First paragraph-first sentence		New requirement
8.1	Operational planning and control – First paragraph-second sentence	4.2.2 c)	Implement controls selected
		4.2.2 f)	Implement and operate the ISMS
8.1	Operational planning and control – Second paragraph	4.3.3	Control of records
8.1	Operational planning and control – Third paragraph		New requirement
8.1	Operational planning and control – Last paragraph	4.2.2 h)	Implement and operate the ISMS
		8.3 b), c)	Preventive action
8.2	Information security risk assessment	4.2.3 d)	Monitor and review the ISMS
		4.3.1 e)	General