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

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 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

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
8.3	Information security risk treatment	4.2.2 b) c)	Implement and operate the ISMS
		4.3.3	Control of records
9.1	Monitoring, measurement, analysis and evaluation – First paragraph	4.2.3 b), c)	Monitor and review the ISMS
		6 d)	Internal ISMS audits
9.1 a)	Monitoring, measurement, analysis and evaluation	4.2.3 a), c), d) g)	Monitor and review the ISMS
9.1 b)	Monitoring, measurement, analysis and evaluation	4.2.2 d)	Implement and operate the ISMS
9.1 c)	Monitoring, measurement, analysis and evaluation		New requirement
9.1 d)	Monitoring, measurement, analysis and evaluation		New requirement
9.1 e)	Monitoring, measurement, analysis and evaluation	4.2.3 b)	Monitor and review the ISMS
9.1 f)	Monitoring, measurement, analysis and evaluation		New requirement
9.1	Monitoring, measurement, analysis and evaluation – Last paragraph	4.2.3 h)	Monitor and review the ISMS
		4.3.3	Control of records
9.2	Internal audit – First paragraph	4.2.3 e)	Monitor and review the ISMS
		6	Internal ISMS audits
9.2 a) 1)	Internal audit	6 b)	Internal ISMS audits
9.2 a) 2)	Internal audit	6 a)	Internal ISMS audits
9.2 b)	Internal audit	6 c)	Internal ISMS audits
9.2 c)	Internal audit	6	Internal ISMS audits
9.2 d)	Internal audit	6	Internal ISMS audits
9.2 e)	Internal audit	6	Internal ISMS audits
9.2 f)	Internal audit	6	Internal ISMS audits
9.2 g)	Internal audit	4.3.1 h)	General
		4.3.3	Control of records
		6	Internal ISMS audits
9.3	Management review – First paragraph	4.2.3 f)	Monitor and review the ISMS
		5.1 h)	Management commitment
		5.2.1 e)	Provision of resources
		7.1	General
9.3 a)	Management review	7.2 g)	Review input
9.3 b)	Management review	4.2.3 d) 1), 2), 3), 4), 5), 6)	Monitor and review the ISMS
		7.2 c), e), h)	Review input
9.3 c)	Management review	7.2 f)	Review input
9.3 c) 1)	Management review	7.2 d)	Review input

Table 1 *(continued)*

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
9.3 c) 2)	Management review	7.2 f)	Review input
9.3 c) 3)	Management review	7.2 a)	Review input
9.3 c) 4)	Management review		New requirement
9.3 d)	Management review	7.2 b)	Review input
9.3 e)	Management review	7.2 e), f)	Review input
9.3 f)	Management review	7.2 i)	Review input
9.3	Management review – Penultimate paragraph	4.2.3 d), g)	Monitor and review the ISMS
		7.1	General
		7.3	Review output
9.3	Management review – Last paragraph	4.3.3	Control of records
		7.1	General
10.1 a)	Nonconformity and corrective action	8.2	Corrective action
10.1 a) 1)	Nonconformity and corrective action	8.2	Corrective action
10.1 a) 2)	Nonconformity and corrective action	8.2	Corrective action
10.1 b)	Nonconformity and corrective action	8.2 c)	Corrective action
		8.3 b)	Preventive action
10.1 b) 1)	Nonconformity and corrective action	8.2 a)	Corrective action
10.1 b) 2)	Nonconformity and corrective action	8.2 b)	Corrective action
10.1 b) 3)	Nonconformity and corrective action	8.2 a)	Corrective action
		8.3 a)	Preventive action
10.1 c)	Nonconformity and corrective action	4.2.4 b)	Maintain and improve the ISMS
		8.2 d)	Corrective action
10.1 d)	Nonconformity and corrective action	8.2 f)	Corrective action
10.1 e)	Nonconformity and corrective action		New requirement
10.1	Nonconformity and corrective action – Last paragraph		New requirement
10.1 f)	Nonconformity and corrective action	8.2 b), c), d)	Corrective action
10.1 g)	Nonconformity and corrective action	8.2 e)	Corrective action
10.2	Continual improvement	4.2.4 a), b), d)	Maintain and improve the ISMS
		5.2.1 f)	Provision of resources
		8.1	Continual improvement

Requirements deleted from ISO/IEC 27001:2005 by clause:

4.2.1	4.2.1 i)	4.2.3 a) 1)	4.2.3 a) 2)	4.2.3 a) 4)	4.2.3 a) 5)	4.2.3(h)
4.3.1	4.3.1 c)	4.3.2	4.3.3			
5.2.1 b)	5.2.1 d)					
8.3 d)	8.3					

5 Comparison between revised editions of ISO/IEC 27002

5.1 Comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013

The Table 2 below is a comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013

Table 2 — Comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013

ISO IEC 27002:2005		ISO IEC 27002:2013	
5	Security policy		
5.1	Information security policy	5.1	Management direction for information security
5.1.1	Information security policy document	5.1.1	Policies for information security
5.1.2	Review of the information security policy	5.1.2	Review of the policies for information security
6	Organization of information security		
6.1	Internal organization		
6.1.1	Management commitment to information security	7.2.1	Management responsibilities
6.1.2	Information security co-ordination		Deleted
6.1.3	Allocation of information security responsibilities	6.1.1	Information security roles and responsibilities
6.1.4	Authorization process for information processing facilities		Deleted
6.1.5	Confidentiality agreements	13.2.4	Confidentiality or nondisclosure agreements
6.1.6	Contact with authorities	6.1.3	Contact with authorities
6.1.7	Contact with special interest groups	6.1.4	Contact with special interest groups
6.1.8	Independent review of information security	18.2.1	Independent review of information security
6.2	External parties		
6.2.1	Identification of risks related to external parties		Deleted
6.2.2	Addressing security when dealing with customers		Deleted
6.2.3	Addressing security in third party agreements	15.1.2	Addressing security within supplier agreements
7	Asset management		
7.1	Responsibility for assets		
7.1.1	Inventory of assets	8.1.1	Inventory of assets
7.1.2	Ownership of assets	8.1.2	Ownership of assets
7.1.3	Acceptable use of assets	8.1.3	Acceptable use of assets
7.2	Information classification		
7.2.1	Classification guidelines	8.2.1	Classification of Information

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
7.2.2	Information labelling and handling	8.2.2	Labelling of information
		8.2.3	Handling of assets
8	Human resources security		
8.1	Prior to employment		
8.1.1	Roles and responsibilities	6.1.1	Information security roles and responsibilities
8.1.2	Screening	7.1.1	Screening
8.1.3	Terms and conditions of employment	7.1.2	Terms and conditions of employment
8.2	During employment		
8.2.1	Management responsibilities	7.2.1	Management responsibilities
8.2.2	Information security awareness, education and training	7.2.2	Information security awareness, education and training
8.2.3	Disciplinary process	7.2.3	Disciplinary process
8.3	Termination or change of employment		
8.3.1	Termination responsibilities	7.3.1	Termination or change of employment responsibilities
8.3.2	Return of assets	8.1.4	Return of assets
8.3.3	Removal of access rights	9.2.6	Removal or adjustment of access rights
9	Physical and environmental security		
9.1	Secure areas		
9.1.1	Physical security perimeter	11.1.1	Physical security perimeter
9.1.2	Physical entry controls	11.1.2	Physical entry controls
9.1.3	Securing offices, rooms and facilities	11.1.3	Securing offices, rooms and facilities
9.1.4	Protecting against external and environmental threats	11.1.4	Protecting against external and environmental threats
9.1.5	Working in secure areas	11.1.5	Working in secure areas
9.1.6	Public access, delivery and loading areas	11.1.6	Delivery and loading areas
9.2	Equipment security		
9.2.1	Equipment siting and protection	11.2.1	Equipment siting and protection
9.2.2	Supporting utilities	11.2.2	Supporting utilities
9.2.3	Cabling security	11.2.3	Cabling security
9.2.4	Equipment maintenance	11.2.4	Equipment maintenance
9.2.5	Security of equipment off-premises	11.2.6	Security of equipment and assets off-premises
9.2.6	Secure disposal or re-use of equipment	11.2.7	Secure disposal or re-use of equipment
9.2.7	Removal of property	11.2.5	Removal of assets
10	Communications and operations management		

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
10.1	Operational procedures and responsibilities		
10.1.1	Documented operating procedures	12.1.1	Documented operating procedures
10.1.2	Change management	12.1.2	Change management
10.1.3	Segregation of duties	6.1.2	Segregation of duties
10.1.4	Separation of development, test and operational facilities	12.1.4	Separation of development, testing and operational environments
10.2	Third party service delivery management		
10.2.1	Service delivery	15.2.1	Monitoring and review of supplier services
10.2.2	Monitoring and review of third party services	15.2.1	Monitoring and review of supplier services
10.2.3	Managing changes to third party services	15.2.2	Managing changes to supplier services
10.3	System planning and acceptance		
10.3.1	Capacity management	12.1.3	Capacity management
10.3.2	System acceptance	14.2.9	System acceptance testing
10.4	Protection against malicious and mobile code		
10.4.1	Controls against malicious code	12.2.1	Controls against malware
10.4.2	Controls against mobile code		Deleted
10.5	Back-up		
10.5.1	Information back-up	12.3.1	Information backup
10.6	Network security management		
10.6.1	Network controls	13.1.1	Network controls
10.6.2	Security of network services	13.1.2	Security of network services
10.7	Media handling		
10.7.1	Management of removable media	8.3.1	Management of removable media
10.7.2	Disposal of media	8.3.2	Disposal of media
10.7.3	Information handling procedures	8.2.3	Handling of assets
10.7.4	Security of system documentation		
10.8	Exchange of information		
10.8.1	Information exchange policies and procedures	13.2.1	Information transfer policies and procedures
10.8.2	Exchange agreements	13.2.2	Agreements on information transfer
10.8.3	Physical media in transit	8.3.3	Physical media transfer
10.8.4	Electronic messaging	13.2.3	Electronic messaging
10.8.5	Business information systems		Deleted
10.9	Electronic commerce services		

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
10.9.1	Electronic commerce	14.1.2	Securing application services on public networks
10.9.2	On-line transactions	14.1.3	Protecting application services transactions
10.9.3	Publicly available information		Deleted
10.10	Monitoring		
10.10.1	Audit logging	12.4.1	Event logging
10.10.2	Monitoring system use		Deleted
10.10.3	Protection of log information	12.4.2	Protection of log information
10.10.4	Administrator and operator logs	12.4.3	Administrator and operator logs
10.10.5	Fault logging	12.4.1	Event logging
10.10.6	Clock synchronization	12.4.4	Clock synchronisation
11	Access control		
11.1	Business requirement for access control		
11.1.1	Access control policy	9.1.1	Access control policy
11.2	User access management		
11.2.1	User registration	9.2.1	User registration and deregistration
		9.2.2	User access provisioning
11.2.2	Privilege management	9.2.3	Management of privileged access rights
11.2.3	User password management	9.2.4	Management of secret authentication information of users
11.2.4	Review of user access rights	9.2.5	Review of user access rights
11.3	User responsibilities		
11.3.1	Password use	9.3.1	Use of secret authentication information
11.3.2	Unattended user equipment	11.2.8	Unattended user equipment
11.3.3	Clear desk and clear screen policy	11.2.9	Clear desk and clear screen policy
11.4	Network access control		
11.4.1	Policy on use of network services	9.1.2	Access to networks and network services
11.4.2	User authentication for external connections		Deleted
11.4.3	Equipment identification in networks	13.1.1	Network controls
11.4.4	Remote diagnostic and configuration port protection		Deleted
11.4.5	Segregation in networks	13.1.3	Segregation in networks
11.4.6	Network connection control		Deleted
11.4.7	Network routing control		Deleted
11.5	Operating system access control		
11.5.1	Secure log-on procedures	9.4.2	Secure log-on procedures

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
11.5.2	User identification and authentication	9.2.1	User registration and deregistration
		9.2.2	User access provisioning
11.5.3	Password management system	9.4.3	Password management system
11.5.4	Use of system utilities	9.4.4	Use of privileged utility programs
11.5.5	Session time-out	9.4.2	Secure log-on procedures
11.5.6	Limitation of connection time	9.4.2	Secure log-on procedures
11.6	Application and information access control		
11.6.1	Information access restriction	9.4.1	Information access restriction
11.6.2	Sensitive system isolation	9.4.1	Information access restriction
11.7	Mobile computing and teleworking		
11.7.1	Mobile computing and communications	6.2.1	Mobile device policy
11.7.2	Teleworking	6.2.2	Teleworking
12	Information systems acquisition, development and maintenance		
12.1	Security requirements of information systems		
12.1.1	Security requirements analysis and specification	14.1.1	Information security requirements analysis and specification
12.2	Correct processing in applications		
12.2.1	Input data validation		Deleted
12.2.2	Control of internal processing		Deleted
12.2.3	Message integrity		Deleted
12.2.4	Output data validation		Deleted
12.3	Cryptographic controls		
12.3.1	Policy on the use of cryptographic controls	10.1.1	Policy on the use of cryptographic controls
12.3.2	Key management	10.1.2	Key management
12.4	Security of system files		
12.4.1	Control of operational software	12.5.1	Installation of software on operational systems
		12.6.2	Restrictions on software installation
12.4.2	Protection of system test data	14.3.1	Protection of test data
12.4.3	Access control to program source code	9.4.5	Access control to program source code
12.5	Security in development and support processes		
12.5.1	Change control procedures	14.2.2	System change control procedures
12.5.2	Technical review of applications after operating system changes	14.2.3	Technical review of applications after operating platform changes

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
12.5.3	Restrictions on changes to software packages	14.2.4	Restrictions on changes to software packages
12.5.4	Information leakage		Deleted
12.5.5	Outsourced software development	14.2.7	Outsourced development
12.6	Technical Vulnerability Management		
12.6.1	Control of technical vulnerabilities	12.6.1	Management of technical vulnerabilities
13	Information security incident management		
13.1	Reporting information security events and weaknesses		
13.1.1	Reporting information security events	16.1.2	Reporting information security events
13.1.2	Reporting security weaknesses	16.1.3	Reporting information security weaknesses
13.2	Management of information security incidents and improvements		
13.2.1	Responsibilities and procedures	16.1.1	Responsibilities and procedures
13.2.2	Learning from information security incidents	16.1.6	Learning from information security incidents
13.2.3	Collection of evidence	16.1.7	Collection of evidence
14	Business continuity management		
14.1	Information security aspects of business continuity management		
14.1.1	Including information security in the business continuity management process	17.1.1	Planning information security continuity
		17.1.2	Implementing information security continuity
14.1.2	Business continuity and risk assessment	17.1.1	Planning information security continuity
14.1.3	Developing and implementing continuity plans including information security	17.1.1	Planning information security continuity
		17.1.2	Implementing information security continuity
14.1.4	Business continuity planning framework		Deleted
14.1.5	Testing, maintaining and re-assessing business continuity plans	17.1.3	Verify, review and evaluate information security continuity
15	Compliance		
15.1	Compliance with legal requirements		
15.1.1	Identification of applicable legislation	18.1.1	Identification of applicable legislation and contractual requirements
15.1.2	Intellectual property rights (IPR)	18.1.2	Intellectual property rights
15.1.3	Protection of organizational records	18.1.3	Protection of records
15.1.4	Data protection and privacy of personal information	18.1.4	Privacy and protection of personally identifiable information

Table 2 *(continued)*

ISO IEC 27002:2005		ISO IEC 27002:2013	
15.1.5	Prevention of misuse of information processing facilities		Deleted
15.1.6	Regulation of cryptographic controls	18.1.5	Regulation of cryptographic controls
15.2	Compliance with security policies and standards, and technical compliance		
15.2.1	Compliance with security policies and standards	18.2.2	Compliance with security policies and standards
15.2.2	Technical compliance checking	18.2.3	Technical compliance review
15.3	Information systems audit considerations		
15.3.1	Information systems audit controls	12.7.1	Information systems audit controls
15.3.2	Protection of information systems audit tools		Deleted

5.2 Comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005

The Table 3 below is a comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005

Table 3 — Comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005

ISO IEC 27002:2013		ISO IEC 27002:2005	
5	Information security policies		
5.1	Management direction for information security	5	Information security policy
5.1.1	Policies for information security	5.1.1	Information security policy document
5.1.2	Review of the policies for information security	5.1.2	Review of the information security policy
6	Organization of information security		
6.1	Internal organization		
6.1.1	Information security roles and responsibilities	6.1.3	Allocation of information security responsibilities
		8.1.1	Roles and responsibilities
6.1.2	Segregation of duties	10.1.3	Segregation of duties
6.1.3	Contact with authorities	6.1.6	Contact with authorities
6.1.4	Contact with special interest groups	6.1.7	Contact with special interest groups
6.1.5	Information security in project management		New control
6.2	Mobile devices and teleworking		
6.2.1	Mobile device policy	11.7.1	Mobile computing and communications
6.2.2	Teleworking	11.7.2	Teleworking
7	Human resource security		
7.1	Prior to employment		
7.1.1	Screening	8.1.2	Screening

Table 3 *(continued)*

ISO IEC 27002:2013		ISO IEC 27002:2005	
7.1.2	Terms and conditions of employment	8.1.3	Terms and conditions of employment
7.2	During employment		
7.2.1	Management responsibilities	8.2.1	Management responsibilities
		6.1.1	Management commitment to information security
7.2.2	Information security awareness, education and training	8.2.2	Information security awareness, education and training
7.2.3	Disciplinary process	8.2.3	Disciplinary process
7.3	Termination and change of employment		
7.3.1	Termination or change of employment responsibilities	8.3.1	Termination responsibilities
8	Asset management		
8.1	Responsibility for assets		
8.1.1	Inventory of assets	7.1.1	Inventory of assets
8.1.2	Ownership of assets	7.1.2	Ownership of assets
8.1.3	Acceptable use of assets	7.1.3	Acceptable use of assets
8.1.4	Return of assets	8.3.2	Return of assets
8.2	Information classification		
8.2.1	Classification of Information	7.2.1	Classification guidelines
8.2.2	Labelling of information	7.2.2	Information labelling and handling
8.2.3	Handling of assets	7.2.2	Information labelling and handling
		10.7.3	Information handling procedures
8.3	Media handling		
8.3.1	Management of removable Media	10.7.1	Management of removable media
8.3.2	Disposal of media	10.7.2	Disposal of media
8.3.3	Physical media transfer	10.8.3	Physical media in transit
9	Access control		
9.1	Business requirements of access control		
9.1.1	Access control policy	11.1.1	Access control policy
9.1.2	Access to networks and network services	11.4.1	Policy on use of network services
9.2	User access management		
9.2.1	User registration and deregistration	11.2.1	User registration
9.2.2	User access provisioning	11.2.1	User registration
		11.2.2	Privilege management
9.2.3	Management of privileged access rights	11.2.2	Privilege management
9.2.4	Management of secret authentication information of users	11.2.3	User password management
9.2.5	Review of user access rights	11.2.4	Review of user access rights
9.2.6	Removal or adjustment of access rights	8.3.3	Removal of access rights

Table 3 *(continued)*

ISO IEC 27002:2013		ISO IEC 27002:2005	
9.3	User responsibilities		
9.3.1	Use of secret authentication information	11.3.1	Password use
9.4	System and application access control		
9.4.1	Information access restriction	11.6.1	Information access restriction
		11.6.2	Sensitive system isolation
9.4.2	Secure log-on procedures	11.5.1	Secure log-on procedures
		11.5.5	Session time-out
		11.5.6	Limitation of connection time
9.4.3	Password management system	11.5.3	Password management system
9.4.4	Use of privileged utility programs	11.5.4	Use of system utilities
9.4.5	Access control to program source code	12.4.3	Access control to program source code
10	Cryptography		
10.1	Cryptographic controls	12.3	Cryptographic controls
10.1.1	Policy on the use of cryptographic controls	12.3.1	Policy on the use of cryptographic controls
10.1.2	Key management	12.3.2	Key management
11	Physical and environmental security		
11.1	Secure areas	9.1	Secure areas
11.1.1	Physical security perimeter	9.1.1	Physical security perimeter
11.1.2	Physical entry controls	9.1.2	Physical entry controls
11.1.3	Securing offices, rooms and facilities	9.1.3	Securing offices, rooms and facilities
11.1.4	Protecting against external and environmental threats	9.1.4	Protecting against external and environmental threats
11.1.5	Working in secure areas	9.1.5	Working in secure areas
11.1.6	Delivery and loading areas	9.1.6	Public access, delivery and loading areas
11.2	Equipment		
11.2.1	Equipment siting and protection	9.2.1	Equipment siting and protection
11.2.2	Supporting utilities	9.2.2	Supporting utilities
11.2.3	Cabling security	9.2.3	Cabling security
11.2.4	Equipment maintenance	9.2.4	Equipment maintenance
11.2.5	Removal of assets	9.2.7	Removal of property
11.2.6	Security of equipment and assets off-premises	9.2.5	Security of equipment off-premises
11.2.7	Secure disposal or re-use of equipment	9.2.6	Secure disposal or re-use of equipment
11.2.8	Unattended user equipment	11.3.2	Unattended user equipment
11.2.9	Clear desk and clear screen policy	11.3.3	Clear desk and clear screen policy
12	Operations security		
12.1	Operational procedures and responsibilities		

Table 3 *(continued)*

ISO IEC 27002:2013		ISO IEC 27002:2005	
12.1.1	Documented operating procedures	10.1.1	Documented operating procedures
12.1.2	Change management	10.1.2	Change management
12.1.3	Capacity management	10.3.1	Capacity management
12.1.4	Separation of development, testing and operational environments	10.1.4	Separation of development, test and operational facilities
12.2	Protection from malware		
12.2.1	Controls against malware	10.4.1	Controls against malicious code
12.3	Backup		
12.3.1	Information backup	10.5.1	Information back-up
12.4	Logging and monitoring		
12.4.1	Event logging	10.10.1	Audit logging
12.4.2	Protection of log information	10.10.3	Protection of log information
12.4.3	Administrator and operator logs	10.10.4	Administrator and operator logs
12.4.4	Clock synchronisation	10.10.6	Clock synchronization
12.5	Control of operational software		
12.5.1	Installation of software on operational systems	12.4.1	Control of operational software
12.6	Technical vulnerability management		
12.6.1	Management of technical vulnerabilities	12.6.1	Control of technical vulnerabilities
12.6.2	Restrictions on software installation		New control
12.7	Information systems audit considerations		
12.7.1	Information systems audit controls	15.3.1	Information systems audit controls
13	Communications security		
13.1	Network security management		
13.1.1	Network controls	10.6.1	Network controls
		11.4.3	Equipment identification in networks
13.1.2	Security of network services	10.6.2	Security of network services
13.1.3	Segregation in networks	11.4.5	Segregation in networks
13.2	Information transfer		
13.2.1	Information transfer policies and procedures	10.8.1	Information exchange policies and procedures
13.2.2	Agreements on information transfer	10.8.2	Exchange agreement
13.2.3	Electronic messaging	10.8.4	Electronic messaging
	Confidentiality or nondisclosure agreements	6.1.5	Confidentiality agreements
14	System acquisition, development and maintenance		
14.1	Security requirements of information systems		

Table 3 *(continued)*

ISO IEC 27002:2013		ISO IEC 27002:2005	
14.1.1	Information security requirements analysis and specification	12.1.1	Security requirements analysis and specification
14.1.2	Securing application services on public networks	10.9.1	Electronic commerce
14.1.3	Protecting application services transactions	10.9.2	On-line transactions
14.2	Security in development and support processes		
14.2.1	Secure development policy		New control
14.2.2	System change control procedures	12.5.1	Change control procedures
14.2.3	Technical review of applications after operating platform changes	12.5.2	Technical review of applications after operating system changes
14.2.4	Restrictions on changes to software packages	12.5.3	Restrictions on changes to software packages
14.2.5	Secure system engineering principles		New control
14.2.6	Secure development environment		New control
14.2.7	Outsourced development	12.5.5	Outsourced software development
14.2.8	System security testing		New control
14.2.9	System acceptance testing	10.3.2	System acceptance
14.3	Test data		
14.3.1	Protection of test data	12.4.2	Protection of system test data
15	Supplier relationships		
15.1	Information security in supplier relationships		
15.1.1	Information security policy for supplier relationships		New control
15.1.2	Addressing security within supplier agreements	6.2.3	Addressing security in third party agreements
15.1.3	Information and communication technology supply chain		New control
15.2	Supplier service delivery management		
15.2.1	Monitoring and review of supplier services	10.2.1	Service delivery
		10.2.2	Monitoring and review of third party services
15.2.2	Managing changes to supplier services	10.2.3	Managing changes to third party services
16	Information security incident management		
16.1	Management of information security incidents and improvements		
16.1.1	Responsibilities and procedures	13.2.1	Responsibilities and procedures
16.1.2	Reporting information security events	13.1.1	Reporting information security events

Table 3 *(continued)*

ISO IEC 27002:2013		ISO IEC 27002:2005	
16.1.3	Reporting information security weaknesses	13.1.2	Reporting security weaknesses
16.1.4	Assessment of and decision on information security events		New control
16.1.5	Response to information security incidents		New control
16.1.6	Learning from information security incidents	13.2.2	Learning from information security incidents
16.1.7	Collection of evidence	13.2.3	Collection of evidence
17	Information security aspects of business continuity management		
17.1	Information security continuity		
17.1.1	Planning information security continuity	14.1.1	Including information security in the business continuity management process
17.1.2	Implementing information security continuity	14.1.3	Developing and implementing continuity plans including information security
17.1.3	Verify, review and evaluate information security continuity		New control
17.2	Redundancies		
17.2.1	Availability of information processing facilities		New control
18	Compliance		
18.1	Compliance with legal and contractual requirements		
18.1.1	Identification of applicable legislation and contractual requirements	15.1.1	Identification of applicable legislation
18.1.2	Intellectual property rights	15.1.2	Intellectual property rights (IPR)
18.1.3	Protection of records	15.1.3	Protection of organizational records
18.1.4	Privacy and protection of personally identifiable information	15.1.4	Data protection and privacy of personal information
18.1.5	Regulation of cryptographic controls	15.1.6	Regulation of cryptographic controls
18.2	Information security reviews		
18.2.1	Independent review of information security	6.1.8	Independent review of information security
18.2.2	Compliance with security policies and standards	15.2.1	Compliance with security policies and standards
18.2.3	Technical compliance review	15.2.2	Technical compliance checking

ICS 35.040
Price based on 19 pages