INTERNATIONAL STANDARD

ISO/IEC 27001

Redline version
compares Third edition to
Second edition

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:redline:2022(E)

IMPORTANT — PLEASE NOTE

This is a provisional mark-up copy and uses the following colour coding:

Text example 1	— indicates added text (in green)
~~Text example 2~~	— indicates removed text (in red)
□	— indicates added graphic figure
☒	— indicates removed graphic figure
1.x ...	— Heading numbers containg modifications are highlighted in yellow in the Table of Contents

All changes in this document have yet to reach concensus by vote and as such should only be used internally for review purposes.

DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.~~

~~International Standards are~~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 ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

~~The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.~~

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of 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. In the IEC, see www.iec.ch/understanding-standards.

~~ISO/IEC 27001~~This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 27, ~~*IT Security techniques*~~*Information security, cybersecurity and privacy protection*.

This ~~second~~third edition cancels and replaces the ~~first~~second edition (ISO/IEC 27001:~~2005~~2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

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 and www.iec.ch/national-committees.

~~0~~ Introduction

0.1 General

This ~~International Standard~~document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This ~~International Standard~~document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this ~~International Standard~~document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This ~~International Standard~~document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This ~~International Standard~~document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This ~~International Standard~~document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this ~~International Standard~~document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this ~~International Standard~~document.

2 Normative references

The following documents~~, in whole or in part, are normatively referenced in this document and are indispensable for its application~~ are referred to in the text in such a way that some or all of their content constitutes requirements 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*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

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

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

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; ~~and~~

b) the relevant requirements of these interested parties ~~relevant to information security.~~;

c) which of these requirements will be addressed through the information security management system.

NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2; ~~and~~

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this ~~International Standard~~document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization’s processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; ~~and~~

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization; ~~and~~

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this ~~International Standard; and~~document;

b) reporting on the performance of the information security management system to top management.

NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; ~~and~~

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

   1) integrate and implement the actions into its information security management system processes; and

   2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

   1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

   2) identify the risk owners;

d) analyses the information security risks:

   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

   3) determine the levels of risk;

e) evaluates the information security risks:

   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

   NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE ~~1~~2 Annex A contains a ~~comprehensive~~ list of ~~control objectives and~~possible information security controls. Users of this ~~International Standard~~document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE ~~2~~3 ~~Control objectives are implicitly included in the controls chosen. The control objectives and~~The information security controls listed in Annex A are not exhaustive and additional ~~control objectives and controls may be~~information security controls can be included if needed.

d) produce a Statement of Applicability that contains ~~the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A~~:

- the necessary controls (see 6.1.3 b) and c));
- justification for their inclusion;
- whether the necessary controls are implemented or not; and
- the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE 4 The information security risk assessment and treatment process in this ~~International Standard~~document aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be ~~communicated~~monitored; ~~and~~

e) ~~be updated as appropriate.~~be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

~~f~~h) what will be done;

~~g~~i) what resources will be required;

~~h~~j) who will be responsible;

~~i~~k) when it will be completed; and

~~j~~l) how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization’s control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) ~~who shall communicate; and~~ how to communicate.

~~e) the processes by which communication shall be effected.~~

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this ~~International Standard~~document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this ~~International Standard~~document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access ~~implies~~can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet ~~information security~~ requirements, and to implement the actions determined in ~~6.1. The organization shall also implement plans to achieve information security objectives determined in~~Clause 6, by: ~~6.2~~.

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

~~The organization shall keep documented information~~Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that ~~outsourced processes are determined and~~externally provided processes, products or services that are relevant to the information security management system are controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

~~The organization shall evaluate the information security performance and the effectiveness of the information security management system.determine:~~

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

~~NOTE The methods selected should produce comparable and reproducible results to be considered valid.~~

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated; ~~and~~

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall ~~retain appropriate documented information as evidence of the monitoring and measurement results~~evaluate the information security performance and the effectiveness of the information security management system.

9.2 Internal audit

~~The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:~~

~~a) conforms to~~

~~1) the organization's own requirements for its information security management system; and~~

~~2) the requirements of this International Standard;~~

~~b) is effectively implemented and maintained.~~

~~The organization shall:~~

~~c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;~~

~~d) define the audit criteria and scope for each audit;~~

~~e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;~~

~~f) ensure that the results of the audits are reported to relevant management; and~~

~~g) retain documented information as evidence of the audit programme(s) and the audit results.~~

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

~~Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.~~

~~The management review shall include consideration of:~~

~~a) the status of actions from previous management reviews;~~

~~b) changes in external and internal issues that are relevant to the information security management system;~~

~~c) feedback on the information security performance, including trends in:~~

~~1) nonconformities and corrective actions;~~

~~2) monitoring and measurement results;~~

~~3) audit results; and~~

~~4) fulfilment of information security objectives;~~

~~d) feedback from interested parties;~~

~~e) results of risk assessment and status of risk treatment plan; and~~

~~f) opportunities for continual improvement.~~

~~The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.~~

~~The organization shall retain documented information as evidence of the results of management reviews.~~

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

~~10.1~~ 10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

   1) take action to control and correct it; ~~and~~

   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity; and

   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

~~The organization shall retain documented information as evidence of:~~

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, ~~and~~

g) the results of any corrective action.

~~10.2 Continual improvement~~

~~The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.~~

Annex A
(normative)

~~Reference control objectives and controls~~

Information security controls reference

The ~~control objectives and~~information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:~~2013~~2022[1], Clauses 5 to ~~18 and are to~~8, and shall be used in context with ~~Clause~~ 6.1.3.

Table A.1 — ~~Control objectives and~~Information security controls

~~A.5 Information security policies~~		
5	**Organizational controls**	
~~A.5.1 Management direction for information security~~		
~~Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.~~		
~~A.5.1.1~~ 5.1	Policies for information security	**Control** ~~A set of policies for information security~~Information security policy and topic-specific policies shall be defined, approved by management, published ~~and communicated to employees and relevant external parties~~, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
~~A.5.1.2~~	~~Review of the policies for information security~~	~~*Control*~~ ~~The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.~~
~~A.6 Organization of information security~~		
~~A.6.1 Internal organization~~		
~~Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.~~		
~~A.6.1.1~~ 5.2	Information security roles and responsibilities	**Control** ~~All information security~~Information security roles and responsibilities shall be defined and allocated according to the organization needs.
~~A.6.1.2~~ 5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated ~~to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets~~.
5.4	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.
~~A.6.1.3~~ 5.5	Contact with authorities	**Control** ~~Appropriate contacts~~The organization shall establish and maintain contact with relevant authorities ~~shall be maintained~~.

Table A.1 *(continued)*

~~A.6.1.4~~ 5.6	Contact with special interest groups	**Control** ~~Appropriate contacts~~The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations~~shall be maintained~~.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
~~A.6.1.5~~ 5.8	Information security in project management	**Control** Information security shall be ~~addressed in project management, regardless of the type of the project~~integrated into project management.
~~**A.6.2 Mobile devices and teleworking**~~		
~~Objective: To ensure the security of teleworking and use of mobile devices.~~		
~~A.6.2.1~~	~~Mobile device policy~~	~~*Control*~~ ~~A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.~~
~~A.6.2.2~~	~~Teleworking~~	~~*Control*~~ ~~A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.~~
~~**A.7 Human resource security**~~		
~~**A.7.1 Prior to employment**~~		
~~Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.~~		
~~A.7.1.1~~	~~Screening~~	~~*Control*~~ ~~Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.~~
~~A.7.1.2~~	~~Terms and conditions of employment~~	~~*Control*~~ ~~The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.~~
~~**A.7.2 During employment**~~		
~~Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.~~		
~~A.7.2.1~~	~~Management responsibilities~~	~~*Control*~~ ~~Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.~~
~~A.7.2.2~~	~~Information security awareness, education and training~~	~~*Control*~~ ~~All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.~~
~~A.7.2.3~~	~~Disciplinary process~~	~~*Control*~~ ~~There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.~~

Table A.1 *(continued)*

~~**A.7.3 Termination and change of employment**~~		
~~Objective: To protect the organization's interests as part of the process of changing or terminating employment.~~		
~~A.7.3.1~~	~~Termination or change of employment responsibilities~~	~~*Control*~~ ~~Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.~~
~~**A.8 Asset management**~~		
~~**A.8.1 Responsibility for assets**~~		
~~Objective: To identify organizational assets and define appropriate protection responsibilities.~~		
~~A.8.1.1~~ 5.9	Inventory of information and other associated assets	**Control** ~~Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.~~ An inventory of information and other associated assets, including owners, shall be developed and maintained.
~~A.8.1.2~~	~~Ownership of assets~~	~~*Control*~~ ~~Assets maintained in the inventory shall be owned.~~
~~A.8.1.3~~ 5.10	Acceptable use of information and other associated assets	**Control** Rules for the acceptable use ~~of information and of assets associated with information and information processing facilities~~and procedures for handling information and other associated assets shall be identified, documented and implemented.
~~A.8.1.4~~ 5.11	Return of assets	**Control** ~~All employees and external party users~~Personnel and other interested parties as appropriate shall return all ~~of~~the ~~organizational~~organization's assets in their possession upon change or termination of their employment, contract or agreement.
~~**A.8.2 Information classification**~~		
~~Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.~~		
~~A.8.2.1~~ 5.12	Classification of information	**Control** Information shall be classified ~~in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification~~according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
~~A.8.2.2~~ 5.13	Labelling of information	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
~~A.8.2.3~~	~~Handling of assets~~	~~*Control*~~ ~~Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.~~
~~**A.8.3 Media handling**~~		
~~Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.~~		

Table A.1 *(continued)*

~~A.8.3.1~~ 5.14	~~Management of removable media~~Information transfer	**Control** ~~Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.~~ Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
~~A.8.3.2~~	~~Disposal of media~~	~~*Control*~~ ~~Media shall be disposed of securely when no longer required, using formal procedures.~~
~~A.8.3.3~~	~~Physical media transfer~~	~~*Control*~~ ~~Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.~~
~~**A.9 Access control**~~		
~~**A.9.1 Business requirements of access control**~~		
~~Objective: To limit access to information and information processing facilities.~~		
~~A.9.1.1~~ 5.15	Access control ~~policy~~	**Control** ~~An access control policy~~Rules to control physical and logical access to information and other associated assets shall be established~~, documented and reviewed~~ and implemented based on business and information security requirements.
~~A.9.1.2~~	~~Access to networks and network services~~	~~*Control*~~ ~~Users shall only be provided with access to the network and network services that they have been specifically authorized to use.~~
~~**A.9.2 User access management**~~		
~~Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.~~		
~~A.9.2.1~~	~~User registration and de-registration~~	~~*Control*~~ ~~A formal user registration and de-registration process shall be implemented to enable assignment of access rights.~~
~~A.9.2.2~~	~~User access provisioning~~	~~*Control*~~ ~~A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.~~
~~A.9.2.3~~ 5.16	~~Management of privileged access rights~~Identity management	**Control** ~~The allocation and use of privileged access rights shall be restricted and controlled.~~ The full life cycle of identities shall be managed.
~~A.9.2.4~~ 5.17	~~Management of secret authentication information of users~~Authentication information	**Control** ~~The allocation of secret~~Allocation and management of authentication information shall be controlled ~~through~~by a ~~formal management process~~management process, including advising personnel on appropriate handling of authentication information.
~~A.9.2.5~~ 5.18	~~Review of user access~~Access rights	**Control** ~~Asset owners shall review users’ access rights at regular intervals.~~ Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.

Table A.1 *(continued)*

~~A.9.2.6~~ 5.19	~~Removal or adjustment of access rights~~Information security in supplier relationships	**Control** ~~The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.~~ Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
~~**A.9.3 User responsibilities**~~		
~~Objective: To make users accountable for safeguarding their authentication information.~~		
~~A.9.3.1~~ 5.20	~~Use of secret authentication information~~Addressing information security within supplier agreements	**Control** ~~Users shall be required to follow the organization's practices in the use of secret authentication information.~~ Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
~~**A.9.4 System and application access control**~~		
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review and change management of supplier services	**Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
~~Objective: To prevent unauthorized access to systems and applications.~~		
5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
5.25	Assessment and decision on information security events	**Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents.
~~A.9.4.1~~ 5.26	~~Information access restriction~~Response to information security incidents	**Control** ~~Access to information and application system functions shall be restricted~~Information security incidents shall be responded to in accordance with the ~~access control policy~~documented procedures.
5.27	Learning from information security incidents	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

Table A.1 *(continued)*

5.28	Collection of evidence	**Control** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.
5.29	Information security during disruption	**Control** The organization shall plan how to maintain information security at an appropriate level during disruption.
5.30	ICT readiness for business continuity	**Control** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
5.31	Legal, statutory, regulatory and contractual requirements	**Control** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.
5.32	Intellectual property rights	**Control** The organization shall implement appropriate procedures to protect intellectual property rights.
5.33	Protection of records	**Control** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
5.34	Privacy and protection of personal identifiable information (PII)	**Control** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
5.35	Independent review of information security	**Control** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
5.36	Compliance with policies, rules and standards for information security	**Control** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.
~~A.9.4.2~~ 5.37	~~Secure log-on~~ Documented operating procedures	**Control** ~~Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.~~ Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

Table A.1 *(continued)*

6	**People controls**	
6.1	Screening	**Control** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
6.2	Terms and conditions of employment	**Control** The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security.
~~A.9.4.3~~ 6.3	~~Password management system~~Information security awareness, education and training	**Control** ~~Password management systems shall be interactive and shall ensure quality passwords.~~ Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
~~A.9.4.4~~ 6.4	~~Use of privileged utility programs~~Disciplinary process	**Control** ~~The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.~~ A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.
~~A.9.4.5~~	~~Access control to program source code~~	~~*Control*~~ ~~Access to program source code shall be restricted.~~
~~**A.10 Cryptography**~~		
~~**A.10.1 Cryptographic controls**~~		
~~Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.~~		
6.5	Responsibilities after termination or change of employment	**Control** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.
~~A.10.1.1~~ 6.6	~~Policy on the use of cryptographic controls~~Confidentiality or non-disclosure agreements	**Control** ~~A policy on the use of cryptographic controls for~~Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be ~~developed and implemented~~identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
~~A.10.1.2~~ 6.7	~~Key management~~Remote working	**Control** ~~A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.~~ Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.

Table A.1 *(continued)*

~~**A.11 Physical and environmental security**~~		
~~**A.11.1 Secure areas**~~		
~~Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.~~		
6.8	Information security event reporting	**Control** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7	**Physical controls**	
~~A.11.1.1~~ 7.1	Physical security ~~perimeter~~perimeters	**Control** Security perimeters shall be defined and used to protect areas that contain ~~either sensitive or critical information and information processing facilities~~information and other associated assets.
~~A.11.1.2~~ 7.2	Physical entry ~~controls~~	**Control** Secure areas shall be protected by appropriate entry controls ~~to ensure that only authorized personnel are allowed access~~and access points.
~~A.11.1.3~~ 7.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms and facilities shall be designed and ~~applied~~implemented.
7.4	Physical security monitoring	**Control** Premises shall be continuously monitored for unauthorized physical access.
~~A.11.1.4~~ 7.5	Protecting against ~~external~~physical and environmental threats	**Control** ~~Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.~~ Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
~~A.11.1.5~~ 7.6	Working in secure areas	**Control** ~~Procedures~~Security measures for working in secure areas shall be designed and ~~applied~~implemented.
~~A.11.1.6~~ 7.7	~~Delivery and loading areas~~Clear desk and clear screen	**Control** ~~Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from~~Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities ~~to avoid unauthorized access~~shall be defined and appropriately enforced.
~~**A.11.2 Equipment**~~		
~~Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.~~		
~~A.11.2.1~~ 7.8	Equipment siting and protection	**Control** Equipment shall be sited ~~and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access~~securely and protected.
7.9	Security of assets off-premises	**Control** Off-site assets shall be protected.

Table A.1 *(continued)*

7.10	Storage media	**Control** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.
~~A.11.2.2~~ 7.11	Supporting utilities	**Control** ~~Equipment~~Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
~~A.11.2.3~~ 7 .12	Cabling security	**Control** ~~Power and telecommunications cabling carrying~~Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
~~A.11.2.4~~ 7.13	Equipment maintenance	**Control** Equipment shall be ~~correctly~~ maintained correctly to ensure ~~its continued availability and integrity~~availability, integrity and confidentiality of information.
~~A.11.2.5~~	~~Removal of assets~~	~~*Control*~~ ~~Equipment, information or software shall not be taken off-site without prior authorization.~~
~~A.11.2.6~~	~~Security of equipment and assets off-premises~~	~~*Control*~~ ~~Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.~~
~~A.11.2.7~~ 7.14	Secure disposal or re-use of equipment	**Control** ~~All items~~Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
8	**Technological controls**	
~~A.11.2.8~~ 8.1	~~Unattended user equipment~~User end point devices	**Control** ~~Users shall ensure that unattended equipment has appropriate protection.~~ Information stored on, processed by or accessible via user end point devices shall be protected.
~~A.11.2.9~~ 8.2	~~Clear desk and clear screen policy~~Privileged access rights	**Control** ~~A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.~~ The allocation and use of privileged access rights shall be restricted and managed.
~~**A.12 Operations security**~~		
~~**A.12.1 Operational procedures and responsibilities**~~		
8.3	Information access restriction	**Control** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
~~Objective: To ensure correct and secure operations of information processing facilities.~~		

Table A.1 *(continued)*

~~A.12.1.1~~ 8.4	~~Documented operating procedures~~Access to source code	**Control** ~~Operating procedures shall be documented and made available to all users who need them.~~ Read and write access to source code, development tools and software libraries shall be appropriately managed.
~~A.12.1.2~~ 8.5	~~Change management~~Secure authentication	**Control** ~~Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.~~ Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
~~A.12.1.3~~ 8.6	Capacity management	**Control** The use of resources shall be monitored~~, tuned and projections made of future capacity requirements to ensure the required system performance~~ and adjusted in line with current and expected capacity requirements.
~~A.12.1.4~~	~~Separation of development, testing and operational environments~~	~~*Control*~~ ~~Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.~~
~~**A.12.2 Protection from malware**~~		
~~Objective: To ensure that information and information processing facilities are protected against malware.~~		
~~A.12.2.1~~ 8.7	~~Controls~~Protection against malware	**Control** ~~Detection, prevention and recovery controls to protect~~Protection against malware shall be implemented~~, combined with~~ and supported by appropriate user awareness.
~~**A.12.3 Backup**~~		
~~Objective: To protect against loss of data.~~		
~~A.12.3.1~~	~~Information backup~~	~~*Control*~~ ~~Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.~~
~~**A.12.4 Logging and monitoring**~~		
~~Objective: To record events and generate evidence.~~		
~~A.12.4.1~~	~~Event logging~~	~~*Control*~~ ~~Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.~~
~~A.12.4.2~~	~~Protection of log information~~	~~*Control*~~ ~~Logging facilities and log information shall be protected against tampering and unauthorized access.~~
~~A.12.4.3~~	~~Administrator and operator logs~~	~~*Control*~~ ~~System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.~~
~~A.12.4.4~~	~~Clock synchronisation~~	~~*Control*~~ ~~The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.~~

Table A.1 *(continued)*

~~A.12.5 Control of operational software~~		
~~Objective: To ensure the integrity of operational systems.~~		
~~A.12.5.1~~	~~Installation of software on operational systems~~	~~*Control*~~ ~~Procedures shall be implemented to control the installation of software on operational systems.~~
~~A.12.6 Technical vulnerability management~~		
~~Objective: To prevent exploitation of technical vulnerabilities.~~		
~~A.12.6.1~~ 8.8	Management of technical vulnerabilities	**Control** Information about technical vulnerabilities of information systems ~~being used~~in use shall be obtained ~~in a timely fashion~~, the ~~organization's~~organization's exposure to such vulnerabilities shall be evaluated and appropriate measures ~~taken to address the associated risk~~shall be taken.
8.9	Configuration management	**Control** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
8.10	Information deletion	**Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
8.11	Data masking	**Control** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.
8.12	Data leakage prevention	**Control** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
8.13	Information backup	**Control** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.14	Redundancy of information processing facilities	**Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
~~A.12.6.2~~ 8.15	~~Restrictions on software installation~~Logging	**Control** ~~Rules governing the installation of software by users shall be established and implemented.~~ Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
~~A.12.7 Information systems audit considerations~~		
8.16	Monitoring activities	**Control** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
~~Objective: To minimise the impact of audit activities on operational systems.~~		

Table A.1 *(continued)*

~~A.12.7.1~~ 8.17	~~Information systems audit controls~~Clock synchronization	**Control** ~~Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.~~ The clocks of information processing systems used by the organization shall be synchronized to approved time sources.
~~**A.13 Communications security**~~		
8.18	Use of privileged utility programs	**Control** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.
~~**A.13.1 Network security management**~~		
~~Objective: To ensure the protection of information in networks and its supporting information processing facilities.~~		
8.19	Installation of software on operational systems	**Control** Procedures and measures shall be implemented to securely manage software installation on operational systems.
~~A.13.1.1~~ 8.20	~~Network controls~~Networks security	**Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
~~A.13.1.2~~ 8.21	Security of network services	**Control** Security mechanisms, service levels and ~~management~~service requirements of ~~all~~ network services shall be identified ~~and included in network services agreements, whether these services are provided in-house or outsourced~~, implemented and monitored.
~~A.13.1.3~~ 8.22	Segregation ~~in~~of networks	**Control** Groups of information services, users and information systems shall be segregated ~~on~~in the organization’s networks.
~~**A.13.2 Information transfer**~~		
~~Objective: To maintain the security of information transferred within an organization and with any external entity.~~		
~~A.13.2.1~~	~~Information transfer policies and procedures~~	~~*Control*~~ ~~Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.~~
~~A.13.2.2~~	~~Agreements on information transfer~~	~~*Control*~~ ~~Agreements shall address the secure transfer of business information between the organization and external parties.~~
~~A.13.2.3~~	~~Electronic messaging~~	~~*Control*~~ ~~Information involved in electronic messaging shall be appropriately protected.~~
~~A.13.2.4~~	~~Confidentiality or non-disclosure agreements~~	~~*Control*~~ ~~Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented.~~
~~**A.14 System acquisition, development and maintenance**~~		
~~**A.14.1 Security requirements of information systems**~~		
~~Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.~~		

Table A.1 *(continued)*

~~A.14.1.1~~ 8.23	~~Information security requirements analysis and specification~~Web filtering	**Control** ~~The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.~~ Access to external websites shall be managed to reduce exposure to malicious content.
~~A.14.1.2~~	~~Securing application services on public networks~~	~~*Control*~~ ~~Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.~~
~~A.14.1.3~~	~~Protecting application services transactions~~	~~*Control*~~ ~~Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.~~
~~**A.14.2 Security in development and support processes**~~		
~~Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.~~		
8.24	Use of cryptography	**Control** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
~~A.14.2.1~~ 8.25	Secure development ~~policy~~life cycle	**Control** Rules for the secure development of software and systems shall be established and applied~~to developments within the organization~~.
~~A.14.2.2~~	~~System change control procedures~~	~~*Control*~~ ~~Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.~~
~~A.14.2.3~~ 8.26	~~Technical review of applications after operating platform changes~~Application security requirements	**Control** ~~When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.~~ Information security requirements shall be identified, specified and approved when developing or acquiring applications.
~~A.14.2.4~~	~~Restrictions on changes to software packages~~	~~*Control*~~ ~~Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.~~
~~A.14.2.5~~ 8.27	Secure system architecture and engineering principles	**Control** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system ~~implementation efforts~~development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
~~A.14.2.6~~ 8.29	~~Secure development environment~~Security testing in development and acceptance	**Control** ~~Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.~~ Security testing processes shall be defined and implemented in the development life cycle.

Table A.1 *(continued)*

~~A.14.2.7~~ 8.30	Outsourced development	**Control** The organization shall ~~supervise and monitor the activity of~~direct, monitor and review the activities related to outsourced system development.
~~A.14.2.8~~	~~System security testing~~	~~*Control*~~ ~~Testing of security functionality shall be carried out during development.~~
~~A.14.2.9~~	~~System acceptance testing~~	~~*Control*~~ ~~Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.~~
~~**A.14.3 Test data**~~		
~~Objective: To ensure the protection of data used for testing.~~		
~~A.14.3.1~~	~~Protection of test data~~	~~*Control*~~ ~~Test data shall be selected carefully, protected and controlled.~~
~~**A.15 Supplier relationships**~~		
~~**A.15.1 Information security in supplier relationships**~~		
~~Objective: To ensure protection of the organization's assets that is accessible by suppliers.~~		
~~A.15.1.1~~ 8.31	~~Information security policy for supplier relationships~~Separation of development, test and production environments	**Control** ~~Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.~~ Development, testing and production environments shall be separated and secured.
~~A.15.1.2~~	~~Addressing security within supplier agreements~~	~~*Control*~~ ~~All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.~~
~~A.15.1.3~~	~~Information and communication technology supply chain~~	~~*Control*~~ ~~Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.~~
~~**A.15.2 Supplier service delivery management**~~		
~~Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.~~		
~~A.15.2.1~~	~~Monitoring and review of supplier services~~	~~*Control*~~ ~~Organizations shall regularly monitor, review and audit supplier service delivery.~~
~~A.15.2.2~~	~~Managing changes to supplier services~~	~~*Control*~~ ~~Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.~~
~~**A.16 Information security incident management**~~		
~~**A.16.1 Management of information security incidents and improvements**~~		
~~Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.~~		

Table A.1 *(continued)*

~~A.16.1.1~~	~~Responsibilities and procedures~~	~~*Control*~~ ~~Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.~~
~~A.16.1.2~~	~~Reporting information security events~~	~~*Control*~~ ~~Information security events shall be reported through appropriate management channels as quickly as possible.~~
~~A.16.1.3~~ 8.32	~~Reporting information security weaknesses~~Change management	**Control** ~~Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.~~ Changes to information processing facilities and information systems shall be subject to change management procedures.
~~A.16.1.4~~	~~Assessment of and decision on information security events~~	~~*Control*~~ ~~Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.~~
~~A.16.1.5~~	~~Response to information security incidents~~	~~*Control*~~ ~~Information security incidents shall be responded to in accordance with the documented procedures.~~
~~A.16.1.6~~ 8.33	~~Learning from information security incidents~~Test information	**Control** ~~Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.~~ Test information shall be appropriately selected, protected and managed.
~~A.16.1.7~~	~~Collection of evidence~~	~~*Control*~~ ~~The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.~~
~~**A.17 Information security aspects of business continuity management**~~		
~~**A.17.1 Information security continuity**~~		
~~Objective: Information security continuity shall be embedded in the organization's business continuity management systems.~~		
~~A.17.1.1~~	~~Planning information security continuity~~	~~*Control*~~ ~~The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.~~
~~A.17.1.2~~	~~Implementing information security continuity~~	~~*Control*~~ ~~The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.~~
~~A.17.1.3~~	~~Verify, review and evaluate information security continuity~~	~~*Control*~~ ~~The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.~~
~~**A.17.2 Redundancies**~~		
~~Objective: To ensure availability of information processing facilities.~~		

Table A.1 *(continued)*

~~A.17.2.1~~	~~Availability of information processing facilities~~	~~*Control*~~ ~~Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.~~
~~**A.18 Compliance**~~		
~~**A.18.1 Compliance with legal and contractual requirements**~~		
~~Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.~~		
~~A.18.1.1~~	~~Identification of applicable legislation and contractual requirements~~	~~*Control*~~ ~~All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.~~
~~A.18.1.2~~	~~Intellectual property rights~~	~~*Control*~~ ~~Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.~~
~~A.18.1.3~~	~~Protection of records~~	~~*Control*~~ ~~Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.~~
~~A.18.1.4~~	~~Privacy and protection of personally identifiable information~~	~~*Control*~~ ~~Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.~~
~~A.18.1.5~~	~~Regulation of cryptographic controls~~	~~*Control*~~ ~~Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.~~
~~**A.18.2 Information security reviews**~~		
~~Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.~~		
~~A.18.2.1~~	~~Independent review of information security~~	~~*Control*~~ ~~The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.~~
~~A.18.2.2~~	~~Compliance with security policies and standards~~	~~*Control*~~ ~~Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.~~
8.34	~~Technical compliance review~~Protection of information systems during audit testing	**Control** ~~Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.~~ Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.

Bibliography

[1] ISO/IEC 27002:~~2013~~2022, *Information ~~technology — Security Techniques — Code of practice for information~~security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management ~~system implementation guidance~~systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — ~~Measurement~~Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *~~Information technology — Security techniques — Information security risk management~~Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:~~2009~~2018, *Risk management — ~~Principles and guidelines~~Guidelines*

~~[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement – Procedures specific to ISO*, 2012~~

ICS 03.100.70; 35.030