INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

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 27001:2022(E)

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.

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 or www.iec.ch/members_experts/refdocs).

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.

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

This third edition cancels and replaces the second edition (ISO/IEC 27001:2013), 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.

Introduction

0.1 General

This 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 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 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 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 document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This 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 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 document.

2 Normative references

The following documents 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;

b) the relevant requirements of these interested parties;

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;

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 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;

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;

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 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;

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 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

   NOTE 3 The information security controls listed in Annex A are not exhaustive and additional 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));

— 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 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 monitored;

e) 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:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed; and

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) how to communicate.

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this 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 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 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 requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

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

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 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 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;

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;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

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

9.2 Internal audit

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

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.

10.2 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;

   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.

Documented information shall be available as evidence of:

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

g) the results of any corrective action.

Annex A
(normative)

Information security controls reference

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

Table A.1 — Information security controls

5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
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.
5.5	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.8	Information security in project management	**Control** Information security shall be integrated into project management.
5.9	Inventory of information and other associated assets	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.
5.10	Acceptable use of information and other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
5.11	Return of assets	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Table A.1 *(continued)*

5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
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.
5.14	Information transfer	**Control** 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.
5.15	Access control	**Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.18	Access rights	**Control** 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.
5.19	Information security in supplier relationships	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
5.20	Addressing information security within supplier agreements	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
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.
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.

Table A.1 *(continued)*

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.
5.26	Response to information security incidents	**Control** Information security incidents shall be responded to in accordance with the 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.
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.
5.37	Documented operating procedures	**Control** 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.
6.3	Information security awareness, education and training	**Control** 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.
6.4	Disciplinary process	**Control** 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.
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.
6.6	Confidentiality or non-disclosure agreements	**Control** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
6.7	Remote working	**Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
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**	
7.1	Physical security perimeters	**Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.
7.2	Physical entry	**Control** Secure areas shall be protected by appropriate entry controls and access points.
7.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms and facilities shall be designed and implemented.
7.4	Physical security monitoring	**Control** Premises shall be continuously monitored for unauthorized physical access.

Table A.1 *(continued)*

7.5	Protecting against physical and environmental threats	**Control** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
7.6	Working in secure areas	**Control** Security measures for working in secure areas shall be designed and implemented.
7.7	Clear desk and clear screen	**Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
7.8	Equipment siting and protection	**Control** Equipment shall be sited securely and protected.
7.9	Security of assets off-premises	**Control** Off-site assets shall be protected.
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.
7.11	Supporting utilities	**Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Cabling security	**Control** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
7.13	Equipment maintenance	**Control** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
7.14	Secure disposal or re-use of equipment	**Control** 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**	
8.1	User end point devices	**Control** Information stored on, processed by or accessible via user end point devices shall be protected.
8.2	Privileged access rights	**Control** The allocation and use of privileged access rights shall be restricted and managed.
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.
8.4	Access to source code	**Control** Read and write access to source code, development tools and software libraries shall be appropriately managed.

Table A.1 *(continued)*

8.5	Secure authentication	**Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
8.6	Capacity management	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	**Control** Protection against malware shall be implemented and supported by appropriate user awareness.
8.8	Management of technical vulnerabilities	**Control** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures 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.
8.15	Logging	**Control** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
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.
8.17	Clock synchronization	**Control** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

Table A.1 *(continued)*

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.
8.19	Installation of software on operational systems	**Control** Procedures and measures shall be implemented to securely manage software installation on operational systems.
8.20	Networks security	**Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
8.21	Security of network services	**Control** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
8.22	Segregation of networks	**Control** Groups of information services, users and information systems shall be segregated in the organization's networks.
8.23	Web filtering	**Control** Access to external websites shall be managed to reduce exposure to malicious content.
8.24	Use of cryptography	**Control** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
8.25	Secure development life cycle	**Control** Rules for the secure development of software and systems shall be established and applied.
8.26	Application security requirements	**Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications.
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 development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in development and acceptance	**Control** Security testing processes shall be defined and implemented in the development life cycle.
8.30	Outsourced development	**Control** The organization shall direct, monitor and review the activities related to outsourced system development.
8.31	Separation of development, test and production environments	**Control** Development, testing and production environments shall be separated and secured.
8.32	Change management	**Control** Changes to information processing facilities and information systems shall be subject to change management procedures.
8.33	Test information	**Control** Test information shall be appropriately selected, protected and managed.

Table A.1 *(continued)*

8.34	Protection of information systems during audit testing	**Control** 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 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

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

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

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*

ICS 03.100.70; 35.030

Price based on 19 pages

国际标准

ISO/IEC 27001

第三版
2022-10

信息安全、网络安全和隐私保护 - 信息安全管理系统 - 要求

信息安全、网络安全和生命保护
私人 - 信息安全管理系统 - 要求

参考号 ISO/IEC 27001:2022(E)

受版权保护的文件

ISO版权局
CP 401 - Ch. de Blandonnet 8
CH-1214 Vernier, Geneva 电
话。+41 22 749 01 11
电子邮件：copyright@iso.org
网站：www.iso.org
发表于瑞士

内容

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他国际组织，政府和非政府组织，与ISO和IEC联络，也参加了工作。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有所描述。特别要注意的是，不同类型的文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives 或 www.iec.ch/members_experts/refdocs）。

请注意，本文件中的某些内容可能是专利权的对象。ISO和IEC不负责识别任何或所有此类专利权。在本文件编写过程中发现的任何专利权的细节将出现在导言中和/或ISO收到的专利声明清单（见www.iso.org/patents）或IEC收到的专利声明清单（见https:/ patents.iec.ch）上。

本文件中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，见www.iso.org/iso/foreword.html。在IEC中，见www.iec.ch/understanding-standards。

本文件由联合技术委员会ISO/IEC JTC 1，*信息技术*，小组委员会SC 27，*信息安全、网络安全和隐私保护*编写。

第三版取消并取代了第二版（ISO/IEC 27001:2013），并对其进行了技术修订。它还纳入了技术更正ISO/IEC 27001:2013/Cor 1:2014和ISO/IEC 27001:2013/Cor 2:2015。

主要变化如下。

- 该文本已与管理体系标准的统一结构和ISO/IEC 27002:2022保持一致。

对本文件的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html 和 www.iec.ch/national-committees。

简介

0.1 一般

编写本文件是为了提供建立、实施、维护和持续改进信息安全管理系统的要求。采用信息安全管理系统是一个组织的战略决策。一个组织的信息安全管理系统的建立和实施受到该组织的需求和目标、安全要求、使用的组织流程以及组织的规模和结构的影响。所有这些影响因素都会随着时间的推移而改变。

信息安全管理系统通过应用风险管理过程来维护信息的保密性、完整性和可用性，并使有关各方相信风险得到了充分的管理。

重要的是，信息安全管理系统是组织流程和整体管理结构的一部分，并与之相结合，在流程、信息系统和控制的设计中考虑到信息安全。预计信息安全管理系统的实施将根据组织的需要进行扩展。

本文件可供内部和外部人士使用，以评估组织满足其自身信息安全要求的能力。

本文件中要求的顺序并不反映它们的重要性，也不意味着它们被实施的顺序。列表中的项目仅用于参考目的。

ISO/IEC 27000描述了信息安全管理系统的概述和词汇，参考了信息安全管理系统系列标准（包括ISO/IEC 27003[2]、ISO/IEC 27004[3]和ISO/IEC 27005[4]），并附有相关术语和定义。

0.2 与其他管理系统标准的兼容性

本文件采用了ISO/IEC指令第1部分ISO综合补编附件SL中定义的高层结构、相同的子条款标题、相同的文本、通用术语和核心定义，因此与采用附件SL的其他管理体系标准保持兼容。

附件SL中定义的这种通用方法对于那些选择运行一个符合两个或更多管理体系标准要求的单一管理体系的组织来说将是非常有用的。

信息安全、网络安全和隐私保护 - 信息安全管理系统 - 要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进信息安全管理系统的要求。本文件还包括根据组织的需要对信息安全风险进行评估和处理的要求。本文件中规定的要求是通用的，旨在适用于所有组织，无论其类型、规模或性质如何。当一个组织声称符合本文件时，不包括第4至10条规定的任何要求是不可接受的。

2 规范性参考资料

以下文件在文中被提及，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅适用于所引用的版本。对于未注明日期的参考文件，适用于所参考文件的最新版本（包括任何修正案）。

ISO/IEC 27000，*信息技术-安全技术-信息安全管理系统-概述和词汇*

3 术语和定义

在本文件中，适用ISO/IEC 27000中的术语和定义。

ISO和IEC在以下地址维护用于标准化的术语数据库。

— ISO在线浏览平台：可在https://www.iso.org/obp

— IEC Electropedia：可在https://www.electropedia.org/

4 组织的背景

4.1 了解组织和其背景

组织应确定与其目的相关的、影响其实现信息安全管理系统预期结果能力的外部和内部问题。

注意 确定这些问题是指建立ISO 31000:2018[5]第5.4.1条中考虑的组织的外部和内部环境。

4.2 了解有关各方的需求和期望

该组织应确定：

a) 与信息安全管理系统有关的有关各方。

b) 这些相关方的相关要求。

c) 这些要求中的哪些将通过信息安全管理系统来解决。

注意 相关方的要求可以包括法律和法规要求以及合同义务。

4.3 确定信息安全管理系统的范围

组织应确定信息安全管理系统的边界和适用性，以确定其范围。

在确定这一范围时，该组织应考虑： 1:

a) 4.1中提到的外部和内部问题。

b) 4.2中提到的要求。

c) 本组织开展的活动与其他组织开展的活动之间的接口和依赖关系。

该范围应作为文件信息提供。

4.4 信息安全管理制度

组织应根据本文件的要求，建立、实施、维护并持续改进信息安全管理系统，包括所需的流程及其相互作用。

5 领导人

5.1 领导和承诺

最高管理层应通过以下方式展示对信息安全管理系统的领导和承诺。

a) 确保信息安全政策和信息安全目标得到确立，并与组织的战略方向相一致。

b) 确保将信息安全管理系统的要求纳入组织的流程。

c) 确保信息安全管理系统所需的资源是可用的。

d) 传达有效的信息安全管理和符合信息安全管理系统要求的重要性。

e) 确保信息安全管理系统实现其预期结果。

f) 指导和支持人员为信息安全管理系统的有效性作出贡献。

g) 促进持续改进；以及

h) 支持其他相关的管理角色，以展示他们的领导力，因为这适用于他们的责任领域。

注意 本文件中提到的 "业务 "可被广义地解释为指那些对组织存在的目的具有核心意义的活动。

5.2 政策

最高管理层应制定一项信息安全政策，该政策应。

a) 与本组织的宗旨相适应。

b) 包括信息安全目标（见6.2），或为设定信息安全目标提供框架。

c) 包括承诺满足与信息安全有关的适用要求。

d) 包括对持续改进信息安全管理系统的承诺。信息安全政策应：1:

e) 可作为文件信息提供； f)，在组织内进行

交流。

g) 酌情向有关方面提供。

5.3 组织角色、责任和权力

最高管理层应确保在组织内分配和传达与信息安全有关的角色的责任和权限。

最高管理层应指定以下责任和权力：。

a) 确保信息安全管理系统符合本文件的要求。

b) 向最高管理层报告信息安全管理系统的绩效。

注意 最高管理层也可以分配责任和权限来报告组织内的信息安全管理系统的表现。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般

在对信息安全管理系统进行规划时，组织应考虑4.1中提到的问题和4.2中提到的要求，并确定需要应对的风险和机会，以。

a) 确保信息安全管理系统能够实现其预期结果。

b) 防止或减少不受欢迎的影响。

c) 实现持续的改进。本组织应计

划：

d) 应对这些风险和机遇的行动；以及

e) 如何

1) 将这些行动纳入其信息安全管理系统流程并加以实施；以及

2) 评估这些行动的有效性。

6.1.2 信息安全风险评估

组织应定义并应用一个信息安全风险评估程序，该程序应：1:

a) 建立和维护信息安全风险标准，其中包括。

   1) 风险接受标准；以及

   2) 执行信息安全风险评估的标准。

b) 确保重复的信息安全风险评估产生一致、有效和可比较的结果。

c) 识别信息安全风险。

   1) 应用信息安全风险评估程序，确定与信息安全管理系统范围内的信息的保密性、完整性和可用性损失有关的风险；以及

   2) 确定风险所有者。

d) 分析信息安全风险。

   1) 评估如果6.1.2 c) 1)中确定的风险发生，将导致的潜在后果。
   实现。

   2) 评估6.1.2 c) 1)中确定的风险发生的现实可能性；以及

   3) 确定风险水平。

e) 对信息安全风险进行评估。

   1) 将风险分析的结果与6.1.2 a)中确定的风险标准进行比较；以及

   2) 对所分析的风险进行优先排序，以便进行风险处理。

组织应保留有关信息安全风险评估的文件化信息
过程。

6.1.3 信息安全风险处理

组织应定义并应用信息安全风险处理流程，以： 1:

a) 选择适当的信息安全风险处理方案，同时考虑到风险评估结果。

b) 确定实施所选择的信息安全风险处理方案所需的所有控制措施。

   注1 组织可以根据需要设计控制措施，或从任何来源确定控制措施。

c) 将上述6.1.3 b)中确定的控制措施与附件A中的控制措施进行比较，核实没有遗漏任何必要的控制措施。

   注2附件 A包含一份可能的信息安全控制措施的清单。本文件的使用者是
   针对附件A，以确保没有忽略必要的信息安全控制。

   注3 附件A中所列的信息安全控制措施并非详尽无遗，如有需要，还可包括其他信息安全控制措施。

d) 编制一份包含以下内容的适用性声明。

   — 必要的控制（见6.1.3 b）和c））。

— 纳入它们的理由。

— 是否实施了必要的控制措施；以及

— 排除任何附件A的控制的理由。

e) 制定一个信息安全风险处理计划；以及

f) 获得风险所有者对信息安全风险处理计划的批准和对剩余信息安全风险的接受。

组织应保留有关信息安全风险处理的文件化信息
过程。

注4 本文件中的信息安全风险评估和处理过程与ISO 31000[5]中提供的原则和通用准则相一致。

6.2 信息安全目标和实现这些目标的规划

该组织应在相关职能部门和级别建立信息安全目标。信息安全目标应： 1:

a) 与信息安全政策相一致。

b) 是可衡量的（如果切实可行）。

c) 考虑到适用的信息安全要求，以及风险评估和风险处理的结果。

d) 被监测。

e) 被告知。

f) 酌情更新。

g) 可作为文件信息提供。

组织应保留有关信息安全目标的文件化信息。在计划如何实现其信息安全目标时，该组织应确定。

h) 将要做什么。

i) 将需要哪些资源。

j) 谁将负责。

k) 何时完成；以及

l) 如何对结果进行评估。

6.3 变化的规划

当组织确定需要对信息安全管理系统进行更改时，应以有计划的方式进行更改。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进信息安全管理系统所需的资源。

7.2 能力

该组织应：

a) 确定在其控制下从事影响其信息安全绩效的工作的人员的必要能力。

b) 确保这些人在适当的教育、培训或经验的基础上胜任。

c) 在适用的情况下，采取行动以获得必要的能力，并评估所采取行动的有效性；以及

d) 保留适当的文件资料作为能力的证明。

注意 适用的行动可以包括，例如：为现有雇员提供培训、指导或重新分配；或雇用或签约合格人员。

7.3 认识

在组织控制下从事工作的人应了解。

a) 信息安全政策。

b) 他们对信息安全管理系统的有效性的贡献，包括改进信息安全性能的好处；以及

c) 不符合信息安全管理系统要求的影响。

7.4 沟通

组织应确定与信息安全管理系统有关的内部和外部沟通的需求，包括：1:

a) 关于沟通的内容。

b) 何时沟通。

c) 与谁沟通。

d) 如何沟通。

7.5 记录的信息

7.5.1 一般

该组织的信息安全管理系统应包括。

a) 本文件所要求的文件信息；以及

b) 由组织确定为信息安全管理系统有效性所必需的文件化信息。

注意 信息安全管理系统的文件化信息的范围可能因不同的组织而不同。

1) 组织的规模及其活动、流程、产品和服务的类型。

2) 过程的复杂性和它们之间的相互作用；以及

3) 人的能力。

7.5.2 创建和更新

在创建和更新记录的信息时，组织应确保适当的。

a) 识别和描述（如标题、日期、作者或参考号）。

b) 格式（如语言、软件版本、图形）和媒体（如纸张、电子）；以及

c) 审查和批准是否合适和充分。

7.5.3 对文件资料的控制

信息安全管理系统和本文件所要求的文件化信息应得到控制，以确保。

a) 在需要的地方和时间，它是可用的和适合使用的；以及

b) 它得到充分的保护（例如，防止失去保密性、不当使用或失去完整性）。

对于文件化信息的控制，组织应酌情处理以下活动。

c) 分发、访问、检索和使用。

d) 储存和保存，包括保存可读性。

e) 对变化的控制（如版本控制）；以及f) 保

留和处置。

对于组织确定为信息安全管理系统的规划和运行所必需的外部来源的文件信息，应酌情予以识别和控制。

注意 访问权可以意味着关于只查看文件信息的权限，或查看和改变文件信息的权限和权力等的决定。

8 运作

8.1 业务规划和控制

组织应通过以下方式计划、实施和控制满足要求所需的过程，并实施第6条中确定的行动。

— 为这些过程制定标准。

— 根据标准实施对流程的控制。

应在必要的范围内提供有记录的信息，以使人们相信这些过程已按计划进行。

组织应控制计划中的变更，并审查非预期变更的后果，必要时采取行动以减轻任何不利影响。

组织应确保与信息安全管理体系相关的外部提供的流程、产品或服务得到控制。

8.2 信息安全风险评估

组织应按计划的时间间隔或在提出或发生重大变化时进行信息安全风险评估，同时考虑到6.1.2 a)中确定的标准。

组织应保留信息安全风险评估结果的文件信息。

8.3 信息安全风险处理

该组织应实施信息安全风险处理计划。

组织应保留信息安全风险处理结果的文件资料。

9 业绩评估

9.1 监测、测量、分析和评价

该组织应确定：

a) 需要监测和测量的内容，包括信息安全流程和控制。

b) 监测、测量、分析和评估的方法（如适用），以确保结果有效。所选择的方法应产生可比较和可重复的结果，才能被认为是有效的。

c) 应在何时进行监测和测量。

d) 谁来监督和衡量。

e) 何时对监测和测量的结果进行分析和评估；f) 谁来分析和评估这些结果。

应提供有记录的资料作为结果的证据。

组织应评估信息安全性能和信息安全管理系统的有效性。

9.2 内部审计

9.2.1 一般

组织应按计划的时间间隔进行内部审计，以提供关于信息安全管理系统是否存在的信息。

a) 符合

1) 组织本身对其信息安全管理系统的要求。

2) 本文件的要求。

b) 有效地实施和维护。

9.2.2 内部审计方案

该组织应计划、建立、实施和保持审计方案，包括频率、方法、责任、规划要求和报告。

在制定内部审计方案时，组织应考虑相关流程的重要性和以往审计的结果。

该组织应：

a) 确定每项审计的审计标准和范围。

b) 选择审计员并进行审计，确保审计过程的客观性和公正性。

c) 确保将审计结果报告给相关管理层。

应提供有记录的信息，作为实施审计方案和审计结果的证据。

9.3 管理审查

9.3.1 一般

最高管理层应按计划的时间间隔审查组织的信息安全管理系统，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理审查投入

管理审查应包括对以下方面的考虑。

a) 以往管理审查的行动状况。

b) 与信息安全管理系统有关的外部和内部问题的变化。

c) 与信息安全管理系统有关的有关各方的需求和期望的变化。

d) 关于信息安全性能的反馈，包括以下方面的趋势。

1) 不符合要求的情况和纠正措施。

2) 监测和测量结果。

3) 审计结果。

4) 实现信息安全目标。

e) 有关各方的反馈。

f) 风险评估的结果和风险处理计划的状况。

g) 持续改进的机会。

9.3.3 管理审查结果

管理审查的结果应包括与持续改进机会有关的决定以及对信息安全管理系统进行修改的任何需要。

应提供有记录的信息作为管理审查结果的证据。

10 改进

10.1 持续改进

组织应不断提高信息安全管理系统的适宜性、充分性和有效性。

10.2 不合格品和纠正措施

当发生不符合要求的情况时，组织应： 1:

a) 对不符合要求的情况作出反应，并视情况而定。

   1) 采取行动来控制和纠正它。

   2) 处理后果。

b) 评估是否需要采取行动，消除不符合要求的原因，以使其不再发生或在其他地方发生，方法是：

   1) 审查不符合要求的情况。

   2) 确定不符合要求的原因；以及

   3) 确定是否存在或可能发生类似的不符合规定的情况。

c) 实施任何需要的行动。

d) 审查所采取的任何纠正措施的有效性；以及

e) 必要时，对信息安全管理系统进行修改。纠正措施应与所遇到的不符合项的影响相

适应。记载的信息应可作为以下的证据。

f) 不符合要求的性质和随后采取的任何行动。

g) 任何纠正行动的结果。

附件A
(规范性)

信息安全控制措施参考

表A.1中所列的信息安全控制措施是直接来自于并符合 ed那些
在ISO/IEC 27002:2022[1]第5至8条中列出，并应在6.1.3的范围内使用。

表A.1 - 信息 安全控制措施

5	**组织控制**	
5.1	信息安全政策	**控制** 信息安全政策和特定主题的政策应去细化，由管理层批准，公布，传达给相关人员和相关利益方并得到他们的认可，并在计划的时间间隔和发生重大变化时进行审查。
5.2	信息安全角色和 职责	**控制** 应根据组织的需要界定和分配信息安全角色和责任。
5.3	职责分离	**控制** 相互冲突的职责和相互冲突的责任领域应加以区分。
5.4	管理责任	**控制** 管理层应要求所有人员按照既定的信息安全政策、组织的特定高层政策和程序应用信息安全。
5.5	与当局联系	**控制** 该组织应建立并保持与有关当局的联系。
5.6	有特别兴趣的联系 团体	**控制** 该组织应与特殊利益集团或其他专业安全论坛和专业协会建立并保持联系。
5.7	威胁情报	**控制** 应收集和分析与信息安全威胁有关的信息，以产生威胁情报。
5.8	项目管理中的信息安全	**控制** 信息安全应被纳入项目管理。
5.9	信息和其他相关资产的库存	**控制** 应制定和维护一份信息和其他相关资产的清单，包括所有者。
5.10	可接受的信息和其他相关资产的使用	**控制** 应确定、记录和实施可接受的使用规则以及处理信息和其他相关资产的程序。
5.11	资产的回报	**控制** 人员和其他相关方在其就业、合同或协议改变或终止时，应归还其拥有的所有组织资产。

表A.1（*续*）

5.12	信息的分类	**控制** 应根据组织的信息安全需求，基于保密性、完整性、可用性和相关利益方的要求对信息进行分类。
5.13	信息的标示	**控制** 应根据组织采用的信息分类方案，制定并实施一套适当的信息标签程序。
5.14	信息传输	**控制** 对于组织内部以及组织与其他各方之间的所有类型的传输设施，应制定信息传输规则、程序或协议。
5.15	访问控制	**控制** 应根据业务和信息安全要求，制定和实施控制信息和其他相关资产的物理和逻辑访问的规则。
5.16	身份管理	**控制** 应管理身份的整个生命周期。
5.17	认证信息	**控制** 认证信息的分配和管理应受到管理程序的控制，包括就认证信息的适当处理向人员提供建议。
5.18	访问权	**控制** 对信息和其他相关资产的访问权，应根据组织关于访问控制的特定主题政策和规则进行规定、审查、修改和删除。
5.19	供应商关系中的信息安全	**控制** 应确定并实施流程和程序，以管理与使用供应商的产品或服务有关的信息安全风险。
5.20	在供应商协议中解决信息安全问题	**控制** 应根据供应商关系的类型，与每个供应商建立和商定相关的信息安全要求。
5.21	管理信息和通信技术（ICT）供应链中的信息安全	**控制** 应定义并实施流程和程序，以管理与ICT产品和服务供应链相关的信息安全风险。
5.22	对供应商服务的监测、审查和变革管理	**控制** 组织应定期监测、审查、评估和管理供应商信息安全实践和服务提供方面的变化。
5.23	使用的信息安全 云服务	**控制** 应根据组织的信息安全要求制定获取、使用、管理和退出云服务的流程。
5.24	信息安全事件管理规划和准备工作	**控制** 组织应通过定义、建立和沟通信息安全事件管理流程、角色和责任，为管理信息安全事件进行规划和准备。

表A.1（*续*）

5.25	对组建中的安全事件进行评估和决策	**控制** 组织应评估信息安全事件并决定是否将其归类为信息安全事件。
5.26	对信息安全的反应 事件	**控制** 对信息安全事件的处理应符合以下规定 记载的程序。
5.27	从信息安全事件中学习	**控制** 从信息安全事件中获得的知识应被用来加强和改善信息安全控制。
5.28	收集证据	**控制** 组织应建立和实施程序，以确认、收集、获取和保存与信息安全事件有关的证据。
5.29	改革期间的信息安全 中断	**控制** 组织应计划如何在中断期间将信息安全维持在适当的水平。
5.30	为业务连续性做好ICT准备	**控制** 应根据业务连续性目标和信通技术连续性要求，规划、实施、维护和测试信通技术的准备情况。
5.31	法律、法定、监管和合同要求	**控制** 与信息安全有关的法律、法定、监管和合同要求以及组织满足这些要求的方法应被识别、记录并保持更新。
5.32	知识产权	**控制** 本组织应实施适当的程序来保护知识产权。
5.33	记录的保护	**控制** 记录应受到保护，防止丢失、破坏、伪造、未经授权的访问和未经授权的发布。
5.34	个人身份信息（PII）的隐私和保护	**控制** 该组织应根据适用的法律和法规以及合同要求，确定并满足有关保存隐私和保护PII的要求。
5.35	信息安全的独立审查	**控制** 组织管理信息安全的方法及其实施，包括人员、流程和技术，应按计划的时间间隔，或在发生重大变化时进行独立审查。
5.36	遵守信息安全的政策、规则和标准	**控制** 应定期审查对组织的信息安全政策、最高级别的特定政策、规则和标准的遵守情况。
5.37	文件化的操作程序	**控制** 信息处理设施的操作程序应被记录下来，并提供给需要的人员。

表A.1（续）

6	**人员控制**	
6.1	筛选	**控制** 在加入组织之前，应考虑到适用的法律、法规和道德规范，对所有成为人员的候选人进行背景核查，并与业务要求、要访问的信息的分类和感知的风险相称。
6.2	雇用条款和条件	**控制** 雇佣合同协议应说明人员和组织的信息安全责任。
6.3	信息安全意识、教育和培训	**控制** 该组织的人员和有关各方应接受适当的信息安全意识、教育和培训，并定期更新与他们工作职能相关的该组织的信息安全政策、特定主题的政策和程序。
6.4	纪律处分程序	**控制** 应正式确定和通报纪律程序，以对违反信息安全政策的人员和其他相关方采取行动。
6.5	终止或改变就业后的责任	**控制** 应界定、执行并向有关人员和其他有关方面传达在终止或改变就业后仍然有效的信息安全责任和义务。
6.6	保密或不披露协议	**控制** 应确定、记录、定期审查并由人员和其他有关各方签署反映本组织保护信息需求的保密或不披露协议。
6.7	远程工作	**控制** 当人员在远程工作时，应实施安全措施，以保护在组织场所之外访问、处理或存储的信息。
6.8	信息安全事件的再移植	**控制** 组织应提供一种机制，使人员能够通过适当的渠道及时报告观察到的或怀疑的信息安全事件。
7	**物理控制**	
7.1	物理安全周界	**控制** 应定义并使用安全周界来保护包含信息和其他相关资产的区域。
7.2	实际进入	**控制** 安全区域应受到适当的入口控制和访问点的保护。
7.3	确保办公室、房间和设施的安全	**控制** 办公室、房间和设施的实体安全应予设计和已实施。
7.4	实体安全监测	**控制** 应持续监测房舍是否有未经授权的物理访问。

表A.1（*续*）

7.5	防范物理和环境威胁	**控制** 应设计和实施对物理和环境威胁的保护，如自然灾害和其他有意或无意的对基础设施的物理威胁。
7.6	在安全区域工作	**控制** 在安全区工作的安全措施应设计和已实施。
7.7	清晰的桌子和清晰的屏幕	**控制** 应确定并适当执行关于纸张和可移动存储介质的桌面清晰规则和关于信息处理设施的屏幕清晰规则。
7.8	设备选址和保护	**控制** 设备应放置在安全的地方并受到保护。
7.9	房地外资产的安全	**控制** 场外资产应得到保护。
7.10	存储介质	**控制** 应根据组织的分类计划和处理要求，在获取、使用、运输和处置的整个生命周期对存储介质进行管理。
7.11	支持公用事业	**控制** 信息处理设施应受到保护，不受电力故障和其他支持性公用设施故障造成的干扰。
7.12	布线的安全性	**控制** 输送电力、数据或支持性信息服务的电缆应受到保护，以免被拦截、干扰或损坏。
7.13	设备维护	**控制** 应正确维护设备，以确保信息的可用性、完整性和保密性。
7.14	安全处置或重新使用设备	**控制** 含有存储介质的设备项目应进行核查，以确保在处置或重新使用之前，任何敏感数据和授权软件已被删除或安全地覆盖。
8	**技术控制**	
8.1	用户端点设备	**控制** 存储在用户终端设备上、由用户终端设备处理或通过用户终端设备访问的信息应受到保护。
8.2	特权访问权	**控制** 特权访问权的分配和使用应受到限制和管理。
8.3	信息访问限制	**控制** 对信息和其他相关资产的访问应根据既定的特定主题访问控制政策加以限制。
8.4	获取源代码	**控制** 对源代码、开发工具和软件库的读写权限应进行适当的管理。

表A.1（续）

8.5	安全认证	**控制** 安全认证技术和程序应根据信息访问限制和特定主题的访问控制政策来实施。
8.6	能力管理	**控制** 应根据当前和预期的能力要求，监测和调整资源的使用。
8.7	防范恶意软件	**控制** 对恶意软件的保护应通过适当的用户意识来实施和支持。
8.8	技术脆弱性的管理	**控制** 应获得有关正在使用的信息系统的技术脆弱性的信息，评估组织对这种脆弱性的暴露，并采取适当的措施。
8.9	配置管理	**控制** 应建立、记录、实施、监测和审查硬件、软件、服务和网络的配置，包括安全配置。
8.10	信息删除	**控制** 存储在信息系统、设备或任何其他存储介质中的信息在不再需要时应被删除。
8.11	数据屏蔽	**控制** 数据屏蔽的使用应符合组织关于访问控制的特定主题政策和其他相关的特定主题政策，以及业务要求，并考虑到适用的立法。
8.12	防止数据泄漏	**控制** 数据泄漏预防措施应适用于处理、存储或传输敏感信息的系统、网络和任何其他设备。
8.13	信息备份	**控制** 信息、软件和系统的备份副本应根据商定的特定主题的备份政策进行维护和定期测试。
8.14	信息处理设施的冗余度	**控制** 信息处理设施的实施应具有足够的冗余度，以满足可用性要求。
8.15	伐木	**控制** 应制作、存储、保护和分析记录活动、异常、故障和其他相关事件的日志。
8.16	监测活动	**控制** 应监测网络、系统和应用程序的异常行为，并采取适当的行动来评估潜在的信息安全事件。
8.17	时钟同步	**控制** 该组织使用的信息处理系统的时钟应与批准的时间源同步。

表A.1（*续*）

8.18	使用有特权的实用程序	**控制** 对能够凌驾于系统和应用程序控制之上的实用程序的使用应受到限制和严格控制。
8.19	在业务系统上安装软件	**控制** 应实施程序和措施，以安全地管理运行系统上的软件安装。
8.20	网络安全	**控制** 网络和网络设备应得到安全、管理和控制，以保护系统和应用中的信息。
8.21	网络服务的安全性	**控制** 应确定、实施和监测网络服务的安全机制、服务水平和服务要求。
8.22	网络的隔离	**控制** 在组织的网络中，信息服务、用户和信息系统的群体应被隔离。
8.23	网络过滤	**控制** 应管理对外部网站的访问，以减少对恶意内容的接触。
8.24	使用密码学	**控制** 应规定并实施有效使用密码学的规则，包括密码钥匙管理。
8.25	安全开发生命周期	**控制** 应制定和应用软件和系统安全开发的规则。
8.26	应用安全要求	**控制** 在开发或获取应用程序时，应确定、规定和批准信息安全要求。
8.27	安全系统架构和 工程原理	**控制** 安全系统工程的原则应被建立、记录、维护并应用于任何信息系统的开发活动。
8.28	安全编码	**控制** 安全编码原则应适用于软件开发。
8.29	开发和验收中的安全测试	**控制** 安全测试流程应在开发生命周期中定义和实施。
8.30	外包开发	**控制** 该组织应指导、监督和审查与外包系统开发有关的活动。
8.31	开发、测试和生产环境的分离	**控制** 开发、测试和生产环境应分开并确保安全。
8.32	变革管理	**控制** 对信息处理设施和信息系统的变更应遵守变更管理程序。
8.33	测试信息	**控制** 测试信息应得到适当的选择、保护和管理。

表A.1（*续*）

8.34	审计测试期间对信息系统的保护	**控制** 审计测试和其他涉及运营系统评估的保证活动应在测试人员和适当的管理层之间进行规划和商定。

书目

[1] ISO/IEC 27002:2022, *信息安全、网络安全和隐私保护 ction - 信息安全控制*

[2] ISO/IEC 27003，*信息技术-安全技术-信息安全管理系统-指南*

[3] ISO/IEC 27004，*信息技术 - 安全技术 - 信息安全管理 - 监测、测量、分析和评价*

[4] ISO/IEC 27005，*信息安全、网络安全和隐私保护--管理信息安全风险指南*

[5] ISO 31000:2018，*风险管理--指南*

医学研究03.100.70; 35.030

按19页计算的价格