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)

© ISO/IEC 2022

Download from http://www.pinzhi.org/forum.php?mod=viewthread&tid=82246

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
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

More http://www.pinzhi.org/forum.php?mod=forumdisplay&fid=79

Contents

© ISO/IEC 2022 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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.

© ISO/IEC 2022 – All rights reserved

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.

--`,,,`,,`,`,,,,,,`,`,,`,`,`,,`,,-`-`,,`,,`,`,,`---

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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;

© ISO/IEC 2022 – All rights reserved

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.

--```,,``,`,,,,,`,```,`,``,```,,-`-`,,`,,`,`,,`---

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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*

--```,,``,`,,,,,`,```,`,``,```,,-`-`,,`,,`,`,,`---

© ISO/IEC 2022 – All rights reserved

ICS 03.100.70; 35.030

Price based on 19 pages

© ISO/IEC 2022 – All rights reserved

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

信息安全 网络安全 隐私保护 安全管理体系 要求

Reference number
ISO/IEC 27001:2022(E)

新版ISO管理体系标准解读

目录

新版ISO管理体系标准解读

新版ISO管理体系标准解读

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了世界标准化特定体系。作为 ISO 或 IEC 成员的国家机构通过各自组织为处理特定技术活动领域而设立的技术委员会参与制定国际标准。ISO 和 IEC 技术委员会在共同关心的领域合作。与 ISO/IEC 联络的其他国际组织、政府或非政府组织也参与了这项工作。

本文件及后续的开发与保持过程运用 ISO/IEC 指令第 1 部分，特别注意的是，不同类型的文件需要不同的批准标准。本文件是按照 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives or www.iec.ch/members experts/refdocs）。

注意本文件中的某些要素可能涉及到专利权的主题。ISO 和 IEC 不负责识别任何或所有的这些专利权。在文件编制时确定的任何专利权的细节会在专利声明和或在 ISO 专利清单中获取（见 www .iso .org/ patents）或 IEC 专利清单（见 https://patents.iec.ch）。

在本文件中使用的任何商品名都是为了方便用户而提供的信息，并不构成背书。

关于标准自愿性质的解释、ISO 特定术语和合格评定的相关表达的含义、以及关于在技术性贸易壁垒 （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，见 www.iec.ch/understanding-standards.

本文件由 ISO/IEC JTC 1 技术委员会 SC 27，信息安全、网络安全和隐私保护信息技术分委员会编写。

第三版文件经过技术性修订，取消和替代了第二版（ISO/IEC 27001：2013），也包括 ISO/IEC 27001:2013/C 或-1:2014 及 ISO/IEC 27001:2013/C 或-2:2015 的一些技术性勘误。

主要修订如下：

——文本与管理体系标准的协调结构及 ISO/IEC 27002：2022 保持一致。

本文件的任何反馈与问题宜直接与用户的国家标准机构联络。这些成员的完整列表可在 www.iso.org/members.html 或 www.iec.ch/national-committees 查找。

新版ISO管理体系标准解读

引言

0.1 总则

本文件提供了建立、实施、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略决策。组织信息安全管理体系的建立和实施受组织的需求和目标、信息安全要求、组织使用的过程、规模和结构的影响。所有这些影响因素都会随着时间而发生变化。

信息安全管理体系通过实施风险管理过程来保持信息的保密性、完整性和可用性，并为相关方树立风险得到充分管理的信心。

重要的是，信息安全管理体系是组织过程和整体管理结构的一部分并且融入其中，并且在过程、信息系统和控制的设计中要考虑到信息安全。期望的是，信息安全管理体系的实施程度应与组织的需求相符合。

本文件可被内部或外部各方用于评估组织的能力是否满足自身的信息安全要求。

本文件中所表述要求的顺序不反映各要求的重要性或暗示这些要求予以实现的顺序。条款的编号仅是为了参考。

ISO/IEC 27000 描述了信息管理体系的概要和词汇，引用了信息安全管理体系标准族（包括 ISO/IEC 27003，ISO/IEC 27004 及 ISO/IEC 27005）及相关的术语和定义。

0.2 与其他管理体系标准的兼容性

本文件应用 ISO/IEC 合并导则附录 SL 第 1 部分中定义的高阶结构，相同的条款标题、相同的文本、通用术语和核心定义，因此维护了与其他采用附录 SL 的管理体系标准具有兼容性。

附录 SL 中定义的通用途径对于选择实施单一管理体系来满足两个或以上管理体系标准要求的组织是有用的。

0.3 交流探讨

本文件翻译时，为区别 ISO/IEC27001:2022 与 2013 版本，其中变化的部分用下划线标出。另外为方便与其他管理体系标准间的兼容性理解，个别词汇采用了与 GB/T22080-2016 不同的表示，如：“purpose”采用“宗旨”而非“意图”，“responsibilities”采用“职责”而非“责任”等。新版国家标准 GB/T22080 正式发布后以其为准。

本文件由逯伟防组织翻译，仅限于相关人员学习交流，非商用，欢迎探讨。反馈可发邮件 lwf000@126.com 或微信公众号“新版 ISO 管理体系标准解读”（luweifang9001）。

新版ISO管理体系标准解读

信息安全　网络安全　隐私保护

信息安全管理体系 要求

1 范围

本文件规定了在组织环境下建立、实施、维护和持续改进信息安全管理体系的要求。本文件还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。本文件规定的要求是通用的，适用于各种类型、规格或性质的组织。当组织声称符合本文件时，不能排除第 4 章到第 10 章中所规定的任何要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27000 信息技术 安全技术 信息安全管理体系 概述和词汇

3　术语和定义

ISO/IEC 27000 界定的术语和定义适用于本文件。

ISO 和 IEC 保持的用于标准化术语数据库地址如下：

——ISO 在线浏览平台：https:// www .iso .org/ obp

——IEC 电子化平台：https:// www .electropedia .org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关的，且影响其实现信息安全管理体系预期结果的能力相关的外部和内部因素。

新版ISO管理体系标准解读

注：对这些因素的确定，参见 ISO 31000:2018，5.4.1 中建立外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定：

a）与信息安全管理体系有关的相关方；

b）这些相关方的相关要求；

c）需要通过信息安全管理体系应对的要求。

注：相关方的要求可包括法律法规要求和合同义务。

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界和适用性以建立其范围。

当确定范围时，组织应考虑：

a）4.1 中提到的外部和内部因素；

b）4.2 中提到的要求

c）组织实施活动之间及与其他组织间实施活动的接口和依赖关系。

范围应形成文件化信息并可获得。

4.4 信息安全管理体系

组织应根据本文件的要求，建立、实施、维护和持续改进信息安全管理体系，包括所需过程及其相互作用。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动证实其对信息安全管理体系的领导作用和承诺：

a）确保建立信息安全方针和信息安全目标，并与组织的战略方向相一致；

b）确保将信息安全管理体系的要求融合入组织的过程中；

c）确保信息安全管理体系所需的资源可获得；

d）沟通有效的信息安全管理以及符合信息安全管理体系要求的重要性；

e）确保信息安全管理体系达成其预期结果；

f）指导并支持相关人员为信息安全管理体系的有效性做出贡献；

g）促进持续改进；并

h）支持其他相关管理角色在其职责范围内发挥领导作用。

新版ISO管理体系标准解读

注：本文件使用的"业务"一词可广义地理解为涉及组织存在目的的核心活动。

5.2 方针

最高管理者应建立信息安全方针 ，该方针应：

a）与组织的宗旨相适宜；

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）包括对满足适用的信息安全相关要求的承诺；

d）包括对信息安全管理体系持续改进的承诺。

信息安全方针应：

e）形成文件化信息并可获取；

f）在组织内得到沟通；

g）适当时，可被相关方获取。

5.3 组织角色、职责和权限

最高管理者应确保与信息安全相关的角色、职责和权限在组织内得到分配和沟通。

最高管理者应分配职责和权限，以：

a）确保信息安全管理体系符合本文件的要求；

b）向最高管理者报告信息安全管理体系的绩效。

注：最高管理者也可分配在组织内报告信息安全管理体系绩效的职责和权限。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

当策划信息安全管理体系时，组织应考虑 4.1 中提到的因素和 4.2 中提到的要求，并确定需要应对的风险和机遇，以：

a）确保信息安全管理体系能够实现其预期结果；

b）预防或减少不良影响；

实现持续改进。

组织应策划：

d）应对这些风险和机遇的措施，并

e）如何：

1） 将这些措施融合到信息安全管理体系过程中，并予以实现；

新版ISO管理体系标准解读

2） 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应确定和实施信息安全风险评估过程，以：

a）建立并维护信息安全风险准则，包括：

1）风险可接受准则；

2）实施信息安全风险评估准则。

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)实施信息安全风险评估过程以识别与信息安全管理体系范围内与信息的保密性、完整性和可用性损失有关的风险；

2）识别风险所有者；

d）分析信息安全风险；

1）评估 6.1.2c)1 中所识别的风险发生后，可能导致的潜在后果；

2）评估 6.1.2c)1 中所识别的风险实际发生的可能性；

3）确定风险级别。

e）评价信息安全风险：

1）将风险分析的结果与 6.1.2a)中建立的风险准则进行比较；

2）为风险处置排序已分析风险的优先级

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处置

组织应确定并实施信息安全风险处置过程，以：

a）在风险评估结果的基础上，选择适当的信息安全风险处置选项；

b）确定实现已选的信息安全风险处置选项所必需的所有控制；

注 1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c）将 6.1.3b）确定的控制与附录 A 的控制进行比较，并验证没有忽略必要的控制；

注 2：附录 A 包括了可能的信息安全控制清单，本文件的用户可在附录 A 的指导下，确保所必需的信息安全控制措施没有被忽视。

注 3：附录 A 的信息安全控制清单并不是详尽的，如需要，可以附加信息安全控制。

d）制定一个适用性声明，包括：

——必要的控制[见 6.1.3b)和 c)]；

——包含这些控制的正当理由；

——是否实施了所必需的控制；

——排除附录 A 控制的正常理由。

新版ISO管理体系标准解读

e）制定正式的信息安全风险处置计划；

f）获得风险所有者对信息安全风险处置计划以及对信息安全残余风险接受的批准。

组织应保留有关信息安全风险处置过程的文件化信息。

注 4：本文件中的信息安全风险评估与处置过程与 ISO31000 中给出的原则和通用指南相匹配。

6.2 信息安全目标及其实现的策划

组织应在相关的职能和层级上建立信息安全目标。

信息安全目标应：

a）与信息安全方针相一致；

b）可测量（如可行）；

c）应考虑适用的信息安全要求，以及信息评估和信息处置的结果；

d）得到监视

e）得到沟通；

f）适当时更新；

g）作为文件化信息可获取。

组织应保留信息安全目标的文件化信息。

在策划如何实现信息安全目标时，组织应确定：

h）要做什么；

i）需要什么资源；

j）由谁负责；

k）什么时候完成；

l）如何评价结果。

6.3 变更策划

当组织确定需要变更信息安全管理体系时，变更应按计划的方式实施。

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体系所需的资源。

新版ISO管理体系标准解读

7.2 能力

组织应：

a）确定在组织控制下从事会影响信息安全绩效的工作人员所需的能力；

b）确保上述人员在适当的教育、培训、经验方面能够胜任；

c）适用时，采取措施以获得必要的能力，并评价所采取措施的有效性；

d）保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，如针对现有雇员提供培训、指导或重新分配；雇佣或签约有能力的人员。

7.3 意识

组织控制下的工作人员应意识到：

a）信息安全方针

b）其对信息安全管理体系有效性的贡献，包括改进信息安全绩效的益处；

c）不符合信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部沟通的需求，包括：

a）沟通什么；

b）何时沟通；

c）与谁沟通；

d）怎么沟通。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a）本文件要求的文件化信息；

组织的信息安全管理体系有效性所必需的文件化信息。

注：信息安全管理体系文件化信息的详略程度因组织而异，取决于：

1） 组织的规模及其活动、过程、产品和服务的类型；

2）过程及其相互作用的复杂程度；

3） 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

新版ISO管理体系标准解读

a）标识和说明（如标准、日期、作者或索引编号）；

b）形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；

c）评审和批准，以保持其适宜性和充分性。

7.5.3 文件化信息的控制

信息安全管理体系及本文件所要求的文件化信息应得到控制，以确保：

a）在需要的场合和时机，均可获得并适用；

b）予以妥善保护（如避免泄密、不当使用或缺失）；

为控制文件化信息，适用时，组织应进行以下活动：

c）分发、访问、检索和使用；

d）存储和防护，包括保持可读性

e）更改控制（如，版本控制）；

f）保留和处置。

组织确定策划和运行信息安全管理体系所必需的外来文件应得到适当的识别和控制。

注：访问可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

8 运行

8.1 运行策划与控制

为满足要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

——建立过程准则；

——按照过程准则实施过程控制。

应在必要的范围和程度上提供文件化信息，以确信过程已按照计划得到执行。

组织应控制计划的变更，并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保与信息安全管理体系相关的外部提供过程、产品和服务得到控制。

8.2 信息安全风险评估

组织应考虑 6.1.2a）所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。

组织应保留信息安全风险评估结果的文件化信息。

8.3 信息安全风险处置

组织应实施信息安全风险处置计划。

新版ISO管理体系标准解读

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a）需要监视和测量什么，包括信息安全过程和控制；

b）适用时的监视、测量、分析和评价的方法，以确保结果有效。选择的方法宜能产生可比较与可重现的结果以被认为是有效的。

c）何时应执行监视和测量；

d）谁应监视和测量；

e）何时应分析和评价监视和测量的结果；

f）谁应分析和评价这些结果。

应提供文件化信息以作为结果的证据。

组织应评价信息安全绩效和信息安全管理体系的有效性。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔实施内部审核，以提供有关信息安全管理体系的下列信息，是否：

a）符合：

1）组织自身对信息安全管理体系要求；

2）本文件的要求；

b）得到有效的实施和保持。

9.2.2 内部审核方案

组织应策划、制定、实施和维护审核方案，包括审核频次、方法、职责、策划要求和报告；

制定内部审核方案时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a）规定每次审核的审核准则和范围；

b）选择审核员并实施审核，确保审核过程的客观公正；

c）确保将审核结果报告给相关管理者。

新版ISO管理体系标准解读

应提供文件化信息，作为实施审核方案以及审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审应考虑：

a）以往管理评审提出措施的情况；

b）与信息安全管理体系相关的外部和内部因素的变化；

c）与信息安全管理体系有关的相关方需求和期望的变化；

d）有关信息安全绩效的反馈，包括以下方面的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

4）信息安全目标完成情况；

e）相关方反馈；

f）风险评估结果及风险处置计划的情况

g）持续改进的机会

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会相关的决定以及变更信息安全管理体系的任何需求。

组织应提供文件化信息，以作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进信息安全管理体系的适宜性、充分性和有效性。

10.2 不符合和纠正措施

当发生不符合时，组织应：

a）对不符合做出应对，适用时：

新版ISO管理体系标准解读

1）采取措施，以控制和纠正不符合；

2）处理后果；

b）通过下列活动，评价是否需要采取措施，以消除产生不符合的原因，避免其再次发生或在其他场合发生：

1）评审不符合；

2）确定不符合的原因；

3）确定是否存在或可能发生类似的不符合；

c）实施任何所需的措施；

d）评审任何所采取纠正措施的有效性；

e）必要时，对信息安全管理体系进行变更。

纠正措施应与不符合所产生的影响相适应。

应提供文件化信息以作为下列事项的证据：

f）不符合的性质以及所采取的任何后续措施；

g）任何纠正措施的结果。

新版ISO管理体系标准解读

附录A（规范性附录） 信息安全控制参考

表A.1所列的信息安全控制是直接源自并与ISO/IEC 27002:2022第5章至第8章相对应，并在6.1.3环境中被使用。

表A.1 信息安全控制

表A.1 续表		
5	组织控制	
5.1	信息安全策略	控制 信息安全策略和特定的主题策略应被定义，由管理者批准，发布、传递并被相关人员和有关相关方所认可，并按照策划的时间间隔或当发生重大变化时实施评审。
5.2	信息安全角色与职责	控制 应根据组织的需求定义、分配信息安全的角色和职责。
5.3	职责分离	控制 应分离有冲突的职责及其责任范围。
5.4	管理职责	控制 管理应要求所有人员按照组织制定的信息安全策略、特定主题策略和规程实施信息安全。
5.5	与职能机构的联系	控制 组织应建立和维护与相关职能机构的联系
5.6	与特定相关方的联系	控制 组织应建立和维护与特定相关方、其他专业安全论坛和专业协会联系
5.7	威胁情报	控制 应收集和分析与信息安全威胁相关的信息，以形成威胁情报
5.8	项目管理中的信息安全	控制 信息安全应整合进项目管理中。
5.9	信息及其他资产清单	控制 应当制定和维护信息和其他资产清单，包括其拥有者
5.10	信息和其他相关资产的可接受使用	控制 应识别可接受使用的准则、信息及其他相关资产处理规程，形成文件并实施。
5.11	资产归还	控制 人员和其他适当的相关方在任用、合同或协议的变更或终止时，应归还其占用的所有组织资产。

新版ISO管理体系标准解读

表 A.1 续表

5.12	信息的分级	控制 信息应按照组织的信息安全需求，基于保密性、完整性、可用性和有关相关方的要求进行分级。
5.13	信息的标记	控制 应按照组织采用的信息分级方案，制定并实现一组适当信息标记规程。
5.14	信息传输	控制 在组织内以及与其他各方之间的所有类型传输设备，都应制定信息传输规则、规程或协议
5.15	访问控制	控制 应基于业务和信息安全要求，建立和实施控制信息和其他相关资产的物理和逻辑访问控制规则。
5.16	身份管理	控制 应对身份的全生命周期实施管理
5.17	鉴别信息	控制 应通过管理过程控制鉴别信息的分配和管理，包括建议员工适当地处理鉴别信息。
5.18	访问权限	控制 应根据组织的特定主题策略和访问控制规则，提供、评审、调整和移除对于信息和其他相关资产的访问权限。
5.19	供应商关系的信息安全	控制 应确定和实施过程和规程，以管理与供应商的产品和服务相关的信息安全风险
5.20	在供应商协议中强调信息安全	控制 应基于供应商关系的类型与每个供应商建立相关的信息安全要求，并达成一致
5.21	ICT（信息与通信技术）供应链中的信息安全管理	控制 应确定和实施过程和规程，以管理与 ICT 产品和服务供应链相关的信息安全风险
5.22	供应商服务的监视、评审和变更管理	控制 组织应定期对供应商的信息安全履行和服务交付实施监视、评审、评价和管理变更。
5.23	云服务使用中的信息安全	控制 应根据组织信息安全要求建立云服务的获取、使用、管理和退出过程。
5.24	信息安全事件管理的策划和准备	控制 组织应通过确定、建立和沟通信息安全事件管理过程、准则和职责，进行信息安全事件管理的策划和准备
5.25	信息安全事态的评估和决策	控制 组织应评估信息安全事态并决定其是否归属于信息安全事件
5.26	信息安全事件的响应	控制 应按照文件化的规程响应信息安全事件

新版ISO管理体系标准解读

表 A.1 续表

5.27	从信息安全事件中的学习	控制 应利用在信息安全事件中获得的知识加强和改进信息安全控制
5.28	证据的收集	控制 组织应建立、实施规程来识别、收集、获取和保存与信息安全事态相关的证据
5.29	中断期间的信息安全	控制 组织应策划在中断期间保持适当级别的信息安全
5.30	关于业务连续性的 ICT 准备	控制 应基于业务连续目标和 ICT 连续要求策划、实施、保持和测试 ICT(信息通信技术)的准备情况。
5.31	法律法规、监管和合同要求	控制 与信息安全相关的法律、法规、监管和合同要求，以及组织为满足这些要求的方法，应得到识别、形成文件和保持更新
5.32	知识产权	控制 组织应建立适当的规程来保护知识产权。
5.33	记录保护控制	控制 记录应得到保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。
5.34	隐私和 PII（个人可识别信息）的保护	控制 组织应根据适用的法律法规和合同要求，识别并满足有关隐私保护和个人可识别信息的保护。
5.35	信息安全的独立评审	控制 应按照计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实现，包括人员、过程和技术进行独立评审
5.36	符合信息安全的策略、规则和标准	控制 应定期评审与组织的信息安全策略、特定主题策略、规则和标准的符合性
5.37	文件化的操作规程	控制 信息处理设施的操作规程应当形成文件并对所需用户可用。
6	人员控制	
6.1	审查	控制 在加入组织前，对所有拟任的候选人的背景实施验证核查，并考虑到适用的法律法规和道德规范，以及与业务要求、访问信息的等级和察觉的风险相适宜。
6.2	任用条款及条件	控制 员工合同协议中应声明员工和组织对信息安全的职责。
6.3	信息安全意识、教育和培训	控制 组织员工和有关相关方应按其工作职能，接受适当的信息安全意识、教育和培训，以及组织信息安全策略、特定主题策略及规程的定期更新的信息

新版ISO管理体系标准解读

表 A.1 续表

6.4	违规处理过程	控制 违规处理过程应正式地传达，以对违反信息安全策略的员工和其他有关相关方采取措施。
6.5	任用终止或变更后的责任	控制 任用终止或变更后仍有效的信息安全责任及其职责应当得到确定、执行和传达到相关员工和其他相关方
6.6	保密和不泄露协议	控制 应识别、形成文件、定期评审并与员工和其他有关相关方签署反映组织信息保护需要的保密性或不泄露协议
6.7	远程工作	控制 当员工远程工作时,应当采取措施以保护在组织场所外访问的、处理的或存储的信息。
6.8	信息安全事态报告	控制 组织应提供一种让员工通过适当渠道、及时报告观察到的或可疑的信息安全事态的机制
7	物理控制	
7.1	物理安全边界	控制 应定义和使用安全边界来保护包含信息和其他相关资产的区域。
7.2	物理入口	控制 安全区域应由适当的入口控制和访问点所保护。
7.3	办公室、房间和设备的安全保护	控制 应为办公室、房间和设施设计和实施物理安全措施。
7.4	物理安全监视	控制 应持续监视物理场所，以防止未经授权的物理访问。
7.5	物理和环境威胁的安全防护	控制 应设计和实施应对物理和环境威胁的安全防护，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 应设计和实施在安全区域工作的安全措施
7.7	清理桌面和屏幕	控制 应当确定并适当地执行针对纸质和可移动存储介质的清理桌面规则和针对信息处理设施的清理屏幕规则
7.8	设备安置和保护	控制 应安全地安置和保护设备
7.9	组织场所外的资产安全	控制 场外的资产应得到保护
7.10	存储介质	控制 应根据组织的分级方案和处理要求，对存储介质实施购买、使用、运送和处置的全生命周期管理。
7.11	支持性设施	控制 应保护信息处理设施使其免于由支持性设施的失效而引起的电源故障和其他中断。

新版ISO管理体系标准解读

表 A.1 续表

7.12	布缆安全	控制 应保证输送电力、传输数据或支持信息服务的电缆免受窃听、干扰或损坏。
7.13	设备维护	控制 设备应予以正确地维护，以确保信息的可用性、完整性和保密性
7.14	设备的安全处置或再利用	控制 包含储存介质的设备项目应进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全的重写
8	技术控制	
8.1	用户终端设备	控制 应保护用户终端设备上存储、处理或访问的信息。
8.2	特许访问权	控制 应限制并管理特许访问权的分配和使用。
8.3	信息访问限制	控制 应按照建立的特定主题访问控制策略限制对信息和其他相关资产的访问
8.4	对源代码的访问	控制 对源代码、开发工具和软件库的读写访问应得到适当的管理。
8.5	身份验证安全	控制 应当基于信息访问限制和访问控制的特定主题策略，实施身份验证技术和规程
8.6	容量管理	控制 应根据当前和预期的能力要求对资源的使用进行监视和调整
8.7	恶意软件防范	控制 应实施恶意软件防范，并通过适当的用户意识提供支持
8.8	技术脆弱性管理	控制 应获取在用信息系统的有关技术脆弱性信息，应评价组织对这些脆弱性的暴露状况并采取适当的措施。
8.9	配置管理	控制 硬件、软件、服务和网络的配置（包括安全配置）应得到建立、文件化、实施、维护和评审
8.10	信息删除	控制 不再需要时，应删除存储在信息系统、设备或任何其他介质中的信息
8.11	数据屏蔽	控制 应当根据组织的访问及其他相关的特定主题策略、业务要求使用数据屏蔽，并考虑到法律要求。
8.12	防止数据泄漏	控制 数据泄漏预防措施应用于处理、存储或传输敏感信息的系统、网络和任何其他终端设备。
8.13	信息备份	控制 按照既定的备份特定专题策略，对信息、软件和系统进行备份，

新版ISO管理体系标准解读

表 A.1 续表

		并定期测试
8.14	信息处理设施的冗余	控制 信息处理设施应当实现冗余，以满足可用性要求。
8.15	日志管理	控制 应产生、存储、保护和分析记录活动、异常、错误和其他事态的日志
8.16	监视活动	控制 应监视网络、系统和应用的异常行为，并采取适当的措施评估潜在的信息安全事件。
8.17	时钟同步	控制 组织使用的信息处理系统的时钟，应与批准的时间源同步。
8.18	特许权实用程序的应用	控制 对于可能超越系统和应用控制的实用程序的使用应予以限制并严格控制
8.19	运行系统的软件安装	控制 应实施规程和措施，以安全管理运行系统的安装软件
8.20	网络安全	控制 应安全管理和控制网络和网络设备，以保护系统和应用中的信息
8.21	网络服务安全	控制 网络服务的安全机制、服务级别和安全要求应予以确定、实施和维护
8.22	网络隔离	控制 应在组织的网络中隔离信息服务、用户和信息系统
8.23	网站过滤	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	密码使用	控制 应确定和实施有效使用密码的规则，包括密钥管理。
8.25	开发生命周期安全	控制 应建立和应用软件和系统的安全开发规则
8.26	应用程序安全要求	控制 当开发和获取应用程序时，应识别、规定和批准信息安全要求
8.27	安全系统架构和工程原则	控制 应建立、形成文件、维护系统安全工程原则，并应用到任何信息系统的开发活动
8.28	安全编码	控制 安全编码原则应用于软件开发。
8.29	开发和验收中的安全测试	控制 应在开发的生命周期中确定和实施安全测试过程
8.30	外包开发	控制 组织应指导、监视和评审与外包系统开发有关的活动
8.31	开发、测试与生	控制

新版ISO管理体系标准解读

表 A.1 续表

	产环境的隔离	应分离并保护开发、测试和生产环境。
8.32	变更管理	控制 信息处理设备和信息系统的变更应遵守变更管理规程
8.33	测试信息	控制 测试信息应适当地选择、保护和管理
8.34	审计测试期间的信息系统保护	控制 审计测试和其他涉及运行系统验证的评审活动应在测试人员和适宜的管理者之间得到策划和协商一致

新版ISO管理体系标准解读

参考文献

[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

新版ISO管理体系标准解读