

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*



Please share your feedback about
the standard. Scan the QR code
with your phone or click the link
[Customer Feedback Form](#)



Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding the organization and its context.....	1
4.2 Understanding the needs and expectations of interested parties.....	1
4.3 Determining the scope of the information security management system.....	2
4.4 Information security management system.....	2
5 Leadership	2
5.1 Leadership and commitment.....	2
5.2 Policy.....	3
5.3 Organizational roles, responsibilities and authorities.....	3
6 Planning	3
6.1 Actions to address risks and opportunities.....	3
6.1.1 General.....	3
6.1.2 Information security risk assessment.....	4
6.1.3 Information security risk treatment.....	4
6.2 Information security objectives and planning to achieve them.....	5
7 Support	6
7.1 Resources.....	6
7.2 Competence.....	6
7.3 Awareness.....	6
7.4 Communication.....	6
7.5 Documented information.....	6
7.5.1 General.....	6
7.5.2 Creating and updating.....	7
7.5.3 Control of documented information.....	7
8 Operation	7
8.1 Operational planning and control.....	7
8.2 Information security risk assessment.....	8
8.3 Information security risk treatment.....	8
9 Performance evaluation	8
9.1 Monitoring, measurement, analysis and evaluation.....	8
9.2 Internal audit.....	8
9.2.1 General.....	8
9.2.2 Internal audit programme.....	9
9.3 Management review.....	9
9.3.1 General.....	9
9.3.2 Management review inputs.....	9
9.3.3 Management review results.....	9
10 Improvement	10
10.1 Continual improvement.....	10
10.2 Nonconformity and corrective action.....	10
Annex A (normative) Information security controls reference	11
Bibliography	19

ISO/IEC 27001:2022(E)

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.

- 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.

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*