

ICS 35.030



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 22080-2025

**Cybersecurity technology - Information security management
systems - Requirements**

网络安全技术 信息安全管理 体系 要求

(English Translation)

Issued on: June 30, 2025

Implemented on: January 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Foreword...	3
Introduction...	5
1 Scope...	6
2 Normative references...	6
3 Terms and definitions...	6
4 Organizational context...	7
4.1 Understanding the organization and its context...	7
4.2 Understanding stakeholder needs and expectations...	7
4.3 Determining the scope of the information security management system...	7
4.4 Information security management system...	8
5 Leadership...	8
5.1 Leadership and commitment...	8
5.2 Policy...	9
5.3 Organizational roles, responsibilities, authorities...	9
6 Planning...	9
6.1 Measures to address risks and opportunities...	9
6.2 Information security objectives and implementation plans...	12
6.3 Planning for change...	12
7 Support...	13
7.1 Resources...	13
7.2 Capabilities...	13
7.3 Awareness...	13
7.4 Communication...	13
7.5 Documented information...	14
8 Operation...	15
8.1 Operation planning and control...	15
8.2 Information security risk assessment...	15
8.3 Information security risk mitigation...	16
9 Performance evaluation...	16
9.1 Monitoring, measurement, analysis, evaluation...	16
9.2 Internal audit...	16
9.3 Management review...	17

10 Improvement...	18
10.1 Continual improvement...	18
10.2 Nonconformity and corrective action...	18
Appendix A (Normative) Information security control reference...	20
References...	28

1 Scope

This document specifies the requirements for establishing, implementing, maintaining, continually improving an information security management system within an organizational context. This document also specifies requirements for information security risk assessment and handling tailored to the organization's needs. The requirements specified in this document are general and applicable to organizations of all types, sizes, or natures. When an organization claims compliance with this document, it does not accept the exclusion of any requirements specified in Chapters 4 ~ 10.

2 Normative references

The following documents, through normative references herein, constitute essential provisions 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

Note: GB/T 29246-2023 Information security technology - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018, IDT)

3 Terms and definitions

The terms and definitions defined in ISO/IEC 27000 apply to this document.

The terminology databases maintained by ISO and IEC for standardization are available at the following URLs.

4.1 Understanding the organization and its context

The organization shall identify external and internal matters relevant to its intentions and affecting its ability to achieve the intended results of its information security management system.

The organization shall determine whether climate change 1) is a relevant matter.

Note: For the determination of these matters, see Article 5.4.1, Establishing the external and internal environment, in GB/T 24353-2022.

4.2 Understanding stakeholder needs and expectations

The organization shall determine.

- a) The stakeholders of the information security management system;
- b) The relevant requirements of these stakeholders;
- c) Which requirements will be addressed through the information security management system.

Note 1: Stakeholder requirements include legal, regulatory, contractual obligations.

Note 2: Stakeholders may raise requirements related to climate change.

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.

The organization shall determine the scope of the information security management system based on.

- a) The external and internal matters mentioned in 4.1;
- b) The requirements mentioned in 4.2;

1 For more information on climate change, see the joint communiqué of ISO and the International Accreditation

Forum (IAF) on adding climate change factors to management system standards.

- c) The interfaces and dependencies between the activities implemented by the organization and those implemented by other organizations.

The scope shall be documented and available.

4.4 Information security management system

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

5.1 Leadership and commitment

Top management shall demonstrate its leadership and commitment to the information security management system by.

- a) Ensuring that an information security policy and information security objectives are established and aligned with the organization's strategic direction;
- b) Ensuring that the requirements of the information security management system are integrated into the organization's business processes;
- c) Ensuring that the resources required for the information security management system are available;
- d) Communicating the importance of effective information security management and compliance with the requirements of the information security management system;
- e) Ensuring that the information security management system achieves its intended results;
- f) Guiding and supporting relevant personnel in contributing to the effectiveness of the information security management system;
- g) Promoting continual improvement;
- h) Supporting other relevant management roles in demonstrating their leadership within their responsibilities.

Note: The term "business" in this document can be broadly interpreted as activities that are central to the organization's intentions.

5.2 Policy

Top management shall establish an information security policy that.

- a) Is appropriate to the organization's intentions;
- b) Includes information security objectives (see 6.2) or provides a framework for setting information security objectives;
- c) Includes a commitment to meeting applicable information security requirements;
- d) Includes a commitment to the continual improvement of the information security management system.

The information security policy shall.

- a) Be documented and available;
- b) Be communicated within the organization;
- c) Be available to stakeholders, where appropriate.