

ICS 35.030

CCS L 80



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

GB/T 28450-2020

Replacing GB/T 28450-2020

**Cybersecurity technology - Guidelines for information security
management systems auditing
(English Translation)**

Issued on: May 25, 2026

Implemented on: December 1, 2026

**Issued by: State Administration for Market Regulation, Standardization
Administration of China**

Table of Contents

Preface	
1.Scope	1
2 Normative References	1
3.Terms and Definitions	1
4.Audit Principles	1
5.Management of the audit plan	1
5.1 General Provisions	1
5.2 Establish the objectives of the audit plan	1
5.3 Identify and evaluate the risks and opportunities of the audit plan	2
5.4 Establish an audit plan	2
5.5 Implement the audit plan	3
5.6 Monitoring and Auditing Scheme	4
5.7 Review and Improvement of the Audit Plan	4
6.Implementation of the audit	4
6.1 General Provisions	4
6.2 Initiation of the Audit	4
6.3 Preparation for the Audit Activity	4
6.4 Implementation of Audit Activities	5

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1.Structure and Drafting Rules of Standardization Documents".

Drafting.

This document supersedes GB/T 28450-2020 "Information Technology Security Technology - Guidelines for Auditing Information Security Management Systems" and is consistent with...

Compared with GB/T 28450-2020, apart from structural adjustments and editorial changes, the main technical changes are as follows.

---All sections on "General Principles," "Establishing Audit Programs," and "Identifying and Assessing Audit Program Risks" in the chapter "Management of Audit Programs" have been deleted.

Contents (see sections 5.1 and 5.3.4 of the 2020 edition);

---The section "Risks and Opportunities Identified When Planning an ISMS" in the chapter "Management of Audit Programs" has been removed [see 2020 edition].

5.2.1d)];

---The section on "Implementing the Audit Program" in the chapter on "Management of Audit Programs" has been deleted. Specifically, the section on "IS5.4.2 specifies the objectives, scope, and..." has been removed.

The "Evaluation of the process for maintaining and effectively improving the ISMS" in the "Guidelines" [see 5.4, 5.4.2.1b) of the 2020 edition];

---The section on "Distribution of Audit Reports" in the chapter on "Conducting the Audit" has been deleted. The original text stated, "When distributing audit reports, appropriate measures should be taken to ensure the reports are properly distributed."

"Confidentiality" (see 6.5 and 6.5.2.1 in the 2020 edition).

This document adopts the ISO /IEC 27007.2020 standard, "Information security, network security and privacy protection, information security management system audit".

guide".

The following minimal editorial changes have been made to this document.

---The standard's name has been changed to "Guidelines for Auditing Information Security Management Systems in the Field of Cybersecurity."

---Added Appendix A with a plan for the changes (see A.3.3);

---The order of continuous improvement and non-compliance corrective actions in Appendix A has been changed.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260).

1 Scope

Based on GB/T 19011-2021, this document provides guidelines for the management and auditing of Information Security Management System (ISMS) audit schemes.

Guidelines on implementation and ISMS auditor competence, etc.

This document is applicable to all organizations that need to understand or implement internal or external audits of ISMS, or that need to manage ISMS audit programs.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included.

For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies.

This document.

GB/T 19011-2021 Guidelines for Management System Auditing (ISO 19011.2018, IDT)

GB/T 29246-2023 Information Security Technology - Overview and Glossary of Information Security Management Systems (ISO /IEC 27000.2018)

IDT)

3 Terms and Definitions

The terms and definitions defined in GB/T 19011-2021 and GB/T 29246-2023 apply to this document.

4 Review Principles

The principles in Chapter 4 of GB/T 19011-2021 apply.

5.1 General Provisions

The guidelines in section 5.1 of GB/T 19011-2021 apply.

5.2.2 When establishing the objectives of the ISMS audit program, the following may be included.

- a) Information security requirements for identification;
- b) Requirements of GB/T 22080-2025;
- c) The auditee's performance level as reflected in the occurrence of information security incidents and events, and the effectiveness of the ISMS;

Note: For more information on performance monitoring, measurement, analysis and evaluation, see ISO /IEC 27004.

- d) Information security risks of relevant parties, namely the auditee and the audit commissioner.