

ICS 35.030; 03.120.20
CCS L 70;A00



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

GB/T 25067-2020

Replacing GB/T 25067-2020

**Cybersecurity technology - Requirements for bodies providing
audit and certification of information security management
systems**

(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	
Introduction	
1.Scope	1
2 Normative References	1
3.Terms and Definitions	1

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 replaces GB/T 25067-2020 "Information Technology Security Management System Audit and Certification Body Requirements".

Compared with GB/T 25067-2020, the main technical changes in the "Requirements" standard are as follows, apart from structural adjustments and editorial modifications.

- a) Added terms and definitions such as "control," "external environment," and "information security" (see Chapter 3);
 - b) The requirements for managing conflicts of interest have been changed (see 5.2.2, 5.2.1 in the 2020 version);
 - c) The requirements for auditors' work experience, training experience, and auditing experience have been changed (see 7.2.2.2, 7.2.1.1 in the 2020 version);
 - d) The work experience requirements for technical specialists have been changed [see 7.2.2.3b), 7.2.1.1 in the 2020 version];
 - e) Added requirements for remote auditing (see 8.2.2, 9.1.3.3, 9.4.3.2);
 - f) Added a requirement to reference other standards in the certification documents (see 8.2.3);
 - g) Increased knowledge and skills required for auditing and certification functions (see Appendix A);
 - h) The requirements for calculating review time have been changed (see C.2.1, C.3.2, C.3.3, C.3.4, C.6, C.7, and B.2.1 in the 2020 version).
- B.3.2, B.3.3, B.6).

This document is equivalent to ISO /IEC 27006-1.2024 "Information security, network security and privacy protection - Information security management system audit".

Nuclear and Certification Body Requirements Part 1.General Rules.

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

---To align with my country's national cybersecurity standards, the standard's name has been changed to "Cybersecurity Technology - Information Security Management System Audit".

"and certification body requirements".

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).

Introduction

GB/T 27021.1-2017 specifies the requirements and provides guidelines for organizations that conduct management system audits and certifications. Compliance

Organizations that comply with GB/T 27021.1-2017 shall conduct audits of their Information Security Management System (ISMS) in accordance with GB/T 22080-2025.

When conducting certification activities, it is necessary to supplement GB/T 27021.1-2017 with some requirements and guidelines. This document provides these requirements and guidelines.

This document sets forth the requirements for organizations that provide ISMS audits and certifications; these organizations are referred to as certification bodies. This document specifies...

General requirements for ISMS certification bodies. Certification bodies must comply with these requirements to ensure they implement them in a competent, consistent, and impartial manner.

ISMS certification will promote the recognition and acceptance of these organizations and their certification results both domestically and internationally.

The main body of this document maintains the same structure as GB/T 27021.1-2017.

Network security technology information security management system audit and

Certification body requirements

1 Scope

This document, based on GB/T 27021.1-2017, specifies the requirements for ISMS auditing and certification bodies and provides guidelines.

Organizations providing ISMS certification demonstrate their competence and reliability in accordance with the requirements outlined in this document. The guidelines in this document provide

Further explanation of these requirements.

Note: This document can serve as a guideline for accreditation, peer review, or other auditing processes.

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 22080-2025 Network Security Technology - Information Security Management System Requirements (ISO /IEC 27001.2022, IDT)

GB/T 27021.1-2017 Requirements for Conformity Assessment Management Systems - Audit and Certification Bodies - Part 1. Requirements (ISO /IEC)

17021-1.2015, IDT)

3 Terms and Definitions

The terms and definitions defined in GB/T 27021.1-2017, as well as the following terms and definitions, apply to this document.

The URLs for the terminology databases maintained by ISO and IEC for standardization are as follows.

3.1

A document that indicates that the customer's ISMS complies with the specified ISMS standards and any supplementary documents required by the ISMS.

Note: This definition does not limit the number of files collectively referred to as authentication files.

3.2

control

Measures to maintain and/or change the risk (3.10).

Note 1: Control includes, but is not limited to, any process, policy, equipment, practice or other condition and/or action that maintains and/or changes risk (3.10).

Note 2: Control does not always achieve the desired change.

[Source. GB/T 22081-2024, 3.1.8]

3.3

external context

The external circumstances in which an organization (3.9) seeks to achieve its goals.

Note: The external environment may include the following aspects.

---Cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environments, whether international, national, regional, or local;