

ICS 35.030
CCS L 80



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

GB/T 20985.1-2026

Replacing GB/T 20985.1-2017

**Cybersecurity technology - Cybersecurity incident management
- Part 1: Principles and process**

网络安全技术 网络安全事件管理 第1部分：原理和过程

(English Translation)

Issued on: July 2, 2026

Implemented on: February 1, 2027

Issued by: State Administration for Market Regulation

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative References	
3 Terms, Definitions, and Abbreviations	
3.1 Terms and Definitions	
3.2 Abbreviations	
4.1 Basic Concepts	
4.2 Incident Management Objectives	
4.3 Benefits of Structured Approaches	
4.4 Adaptability	
4.5 Abilities	
4.6 Communication	
4.7 Document	
5 Process	
5.1 Overview	
5.2 Planning and Preparation	
5.3 Discovery and Reporting	
5.4 Assessment and Decision-Making	
5.5 Response	
5.6 Summary of Experiences	
Appendix A (Informative) and its Relationship with Survey Standards	
Appendix B (Informative) Examples of Cybersecurity Incidents and Their Causes (18)	
B.1 Event Type	
B.2 Attack	
B.3 Information Gathering	
Comparison Table	
Appendix D (Informative) Considerations for Findings During the Incident Investigation	
References	

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 is Part 1 of GB/T 20985 "Network Security Technology - Network Security Incident Management". GB/T 20985 has been published.

The following parts were included.

---Part 1: Principles and Processes;

---Part 2: Event Response Planning and Preparation Guidelines this document replaces GB/T 20985.1-2017 "Information Technology Security Technology - Information Security Incident Management - Part 1: Incident Management" Compared with GB/T 20985.1-2017, the main technical changes in "Principles of Theory" are as follows, except for structural adjustments and editorial modifications.

- a) The description of the scope has been changed (see Chapter 1, Chapter 1 in the 2017 edition);
- b) The causes of cybersecurity incidents and events in the basic concepts have been changed (see 4.1, 2017 version 4.1);
- c) Enhanced event management capabilities (see 4.5), communication (see 4.6), and documentation content (see 4.7);
- d) Added content on cybersecurity incident and event handling activities (see 5.1);
- e) The content of the cybersecurity incident management plan has been changed (see 5.2, 2017 version 5.2);
- f) The content of post-discovery and post-reporting activities for cybersecurity incidents has been changed (see 5.3, 2017 version 5.3);
- g) The content of the cybersecurity incident response activities has been changed (see 5.5, 2017 version 5.5).

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

---Change the standard title to "Network Security Technology. Network Security Incident Management Part 1: Principles and Processes";

---Added the abbreviations "DoS" and "DDoS";

---The name of Appendix C has been changed; "Comparison Table of ISO/IEC 27001 and ISO/IEC 27035 (All Parts)" has been changed to...

"Comparison table between GB/T 22080-2025 and this document, GB/T 20985.2-2026 and ISO/IEC 27035-3:2020".

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

This document outlines the concepts, principles, and processes of cybersecurity incident management, providing a framework for planning and preparation, detection and reporting, assessment and decision-making.

A structured approach is provided for responding to events and summarizing experiences.

The guidance provided in this document regarding the cybersecurity incident management process and its key activities is universal and applicable to all types and regulations.

Organizations of a certain size or nature may adjust this guidance based on their business type, size, nature, and cybersecurity risk profile.

This document also applies to external organizations that provide cybersecurity incident management services.

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.

Note: GB/T 29246-2023 Information Security Technology - Overview and Glossary of Information Security Management Systems (ISO/IEC 27000:2018, IDT)

3.1 Terms and Definitions

The terms and definitions defined in ISO/IEC 27000 and 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.

3.1.1

A team comprised of appropriately skilled and trusted members of the organization is responsible for leading and managing all cybersecurity incident management activities, and

Coordinate with internal and external stakeholders throughout the entire event lifecycle.

Note: The team leader may be called the incident manager, appointed by top management, to be fully prepared to handle all types of incidents.

3.1.2

A team of appropriately skilled and trustworthy members of an organization responds to and handles incidents in a coordinated manner.

Note 1: There may be multiple IRTs, each IRT responds to and processes a certain aspect of the event.

Note 2: Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) are organizations, departments, regions, and countries that wish to coordinate emergency response efforts.

Specific examples of IRT for large-scale ICT and cybersecurity incidents.