

ICS 35.030
CCS L 80



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

GB/T 47692-2026

**Cybersecurity technology - Incident investigation principles
and processes**

网络安全技术 事件调查原则和过程

(English Translation)

Issued on: May 25, 2026

Implemented on: December 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Preface
1 Scope
2 Normative References
3 Terms and Definitions
4 Abbreviations 3.
5 Principles of Numerical Surveys
5.1 General Principles
5.2 Legality Principle
6 Digital Survey Process
6.1 Process Overview
6.2 Digital Survey Process Category
7 Preparatory Processes
7.1 Overview of Preparatory Processes
7.2 Scene Definition Process
7.3 Process for Identifying Potential Digital Evidence Sources
7.4 Planning the process for collecting, storing, and processing potential digital evidence before an event.
7.5 Analysis of Potential Digital Evidence Before Planning Events
7.6 Planning the Event Detection Process
7.7 Defining the System Architecture Process
7.8 System Architecture Implementation Process
7.9 Implementation of the process for collecting, storing, and processing potential digital evidence prior to the incident.
7.10 Conduct a pre-event analysis of potential digital evidence.
7.11 Implementing the event detection process
7.12 Implementation of the evaluation process
7.13 Improvement Process
8 Startup process class 9.
8.1 Overview of the Startup Process Class
8.2 Event Detection Process
8.3 Initial Response Process
8.4 Planning Process
8.5 Preparation Process

- 9 Obtaining the process class 10.
- 9.1 Overview of the Acquisition Process Class
- 9.2 Potential Digital Evidence Identification Process
- 9.3 Potential Digital Evidence Collection Process
- 9.4 The Process of Obtaining Potential Digital Evidence
- 9.5 Potential Digital Evidence Transfer Process
- 9.6 Potential Digital Evidence Storage and Preservation Process
- 10 Investigation Process Category
- 10.1 Overview of the Survey Process
- 10.2 The Process of Acquiring Potential Digital Evidence
- 10.3 The process of examining and analyzing potential digital evidence
- 10.4 The process of interpreting digital evidence
- 10.5 Reporting Process
- 10.6 Presentation Process
- 10.7 Investigation Conclusion Process
- 11 Parallel Process Classes
- 11.1 Overview of Parallel Process Classes
- 11.2 Authorization Process
- 11.3 Documentation Process
- 11.4 Management Information Flow Process
- 11.5 Preservation of the Chain of Custody Process
- 11.6 The Process of Preserving Digital Evidence
- 11.7 Interaction Process with Entities
- 12 Digital Survey Process Model
- Reference

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 modified to adopt ISO/IEC 27043:2015 "Principles and procedures for investigating information technology security incidents".

The technical differences between this document and ISO/IEC 27043:2015, and the reasons therefor, are as follows.

---Added normative reference to GB/T 25069-2022, and uses the existing definitions of this standard in the "Terms and Definitions" section, using the normative...

The national standard GB/T 29246-2023 replaces ISO/IEC 27000 to adapt to my country's technical requirements;

---The phrase "implementation process of evaluation results" in section 7.13 and other parts of the document has been changed to "improvement process" to enhance readability;

---Changed "Preparation regarding equipment (hardware and software), infrastructure, and personnel" in section 8.5 to "Preparation regarding equipment (hardware and software), policy..." the preparation work now includes a new strategic dimension, covering "preparations in areas such as infrastructure and personnel," making the overall preparation work more comprehensive.

---The fourth paragraph of section 9.4 has been deleted. "Experts and scholars in the field of digital surveys need to design methods applicable to network environments and real-time survey processes." the steps for appropriately acquiring potential digital evidence in scenarios such as cloud computing environments and massive data environments should be aligned with national standards.

---Version 9.5 has been revised to include "using cryptography that complies with national cryptography management requirements" to comply with Chinese laws.

The following editorial changes have been made to this document.

---The wording in Chapter 1 has been revised;

---The charts have been renumbered because the original preface, which included the charts, was removed;

---The abbreviation "DVR" has been removed; this abbreviation is not used in this document.

---The title of Chapter 5, "Digital Surveys," has been changed to "Principles of Digital Surveys" to better reflect the actual content of this chapter;

---The generalized description of international differences in section 5.2 has been revised, such as the possibility that different jurisdictions may have different statutory requirements, depending on the specific circumstances.

Specific laws of a jurisdiction, recommendations to seek legal guidance within a specific jurisdiction, etc., to align with national standards.

---Edited version 6.2 has been modified, changing the sub-procedures that were originally listed line by line in each process into a single paragraph for easier reading and to improve readability.

The sections on "Pre-Event Planning Collection" and "Pre-Event Potential Digital Evidence

Storage and Processing" are consistent with Chapter 7, with changes made to "Potential Digital Evidence".

"Digital Evidence Storage" is changed to "Potential Digital Evidence Storage and Preservation," consistent with Chapter 9: The "Potential Digital Evidence" category is added to the Investigation Process section.

"Evidence Acquisition" is consistent with Chapter 10;

---The description of the hierarchical structure of the digital survey process in the last paragraph of 6.2 has been revised and moved to the second paragraph of 6.1 for easier understanding;

---The addition of "class" or "group" after processes such as the preparatory process and the planning process indicates a collection of processes at different levels, for more...

Good regional division into levels makes it easier to understand;

---The section 7.1, "The input information generated by the above four objectives is referred to as the pre-known system input in the remainder of this document," has been deleted.

The wording has been revised in later texts to better suit Chinese expression habits;

---Changed "Laws of a specific jurisdiction" in section 7.4 to "Requirements of national laws and regulations";

---The clause in 7.12 that "this review especially needs to verify compliance with the legal provisions of the specific judicial system and the principles of digital forensics" has been amended to...

"This review especially needs to verify whether it complies with national laws and regulations and the principles of digital forensics."

---Merge paragraphs 3 and 4 of section 8.2;

---Simplify some meaningless statements in sections 8.3, 8.4, and 8.5, and delete the section about the preparatory process for numerical surveys in the second paragraph of section 8.4.

The objective-related content is omitted because it has already been described in section 7.1, and there is obvious repetition.

---The wording regarding different jurisdictions in 10.7 has been revised;

Appendix A (Informative Appendix) has been deleted because its content mainly involved comparisons with other international numerical survey models and was not relevant to this document.

Applicable;