

ICS 35.030
CCS L 80



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

GB/T 44862-2024

**Cybersecurity technology - Cyber-resilience evaluation criteria
(English Translation)**

Issued on: October 26, 2024

Implemented on: May 1, 2025

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

Table of Contents

Preface	
1 Scope	
2 Normative references	
3 Terms and Definitions	
4 Abbreviations	
5 Overview	
5.1 Network Resilience	
5.2 Evaluation Index System	
5.3 Standard Structure	
6 Network Resilience Indicators	
6.1 Prevention Capabilities	
6.1.1 Situational Awareness	
6.1.2 Inspection and Analysis	
6.1.3 Collaborative Defense	
6.1.4 Supply Chain Management	
6.2 Ability to bear	
6.2.1 Emergency Response	
6.2.2 Limitation of Losses	
6.2.3 Containment	
6.2.4 Survivability	
6.3 Resilience	
6.3.1 Disaster Backup	
6.3.2 Business Continuity	
6.3.3 Data and Business Recovery	
6.4 Adaptability	
6.4.1 Self-management	
6.4.2 Refactoring	
6.4.3 Node Adaptability	
6.4.4 Network Adaptability	
7 Evaluation Methods	
Appendix A (Normative) Network Resilience Evaluation Table	

Appendix B (Informative) Examples of Network Resilience Indicators under Extreme Scenarios and Extreme Cybersecurity Incidents

Appendix C (Informative) Analysis of Network Resilience Requirements for Complex Information Systems

Appendix D (Informative) Network Resilience Architecture Design Methodology

Reference

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

1 Scope

This document specifies the network resilience evaluation criteria and provides a network resilience evaluation index system and evaluation methods.

This document is applicable to the self-assessment of network resilience by organizations, the third-party assessment of network resilience by cybersecurity service agencies, and the Design, build, and enhance the network resilience of organizations.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 20988 Information security technology Information system disaster recovery specification

GB/T 25069-2022 Information Security Technical Terminology

GB/T 30146-2023 Security and Resilience Business Continuity Management System Requirements

GB/T 43269-2023 Information security technology - Criteria for the assessment of cybersecurity emergency response capabilities

3 Terms and Definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

3.1 Cyberresilience

When the network faces adverse conditions, pressure, attacks or lost components, it should have the ability to prevent, withstand, recover and adapt to ensure Maintain the stability of system functions and structures, achieve orderly and effective responses to major network security incidents, and ensure the stable operation of key businesses.

Note: The term "network" in this document refers to a network composed of computers or other information terminals and related equipment that receives and sends information according to certain rules and procedures. A system for collecting, storing, transmitting, exchanging and processing information.

3.2 Critical business

Once a cybersecurity incident occurs, it may seriously affect the network security and stability of an organization or customer, causing significant business losses.

3.3 Survivability

The ability of the system to continue to run basic business functions and complete key business operations in the event of an attack, failure, malfunction or interruption.

Note: Failure means that a system or component loses its purpose or function as designed, and although it can operate, it cannot output the correct results.

A state in which a system or device cannot perform its specified functions. Basic business functions refer to the basic functional units that constitute business functions, such as processes, threads, or algorithms. Modules, etc. [Source: ISO /IEC /IEEE 24765-2017, 3.4060, with modifications]

4 Abbreviations

The following abbreviations apply to this document.