

ICS 35.040
CCS L 80

GA

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

GA/T 2182-2024

**Information security technology - Evaluation requirements for
cybersecurity for critical information infrastructure**

信息安全技术 关键信息基础设施安全测评要求

(English Translation)

Issued on: December 26, 2024

Implemented on: May 1, 2025

Issued by: Ministry of Public Security

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative references	
3 Terms and Definitions	
4 Abbreviations	
5 Overview	
5.1 Critical Information Infrastructure Security Assessment and Network Security Level Assessment	
5.2 Critical Information Infrastructure Security Assessment Framework	
5.2.1 Framework composition	
5.2.2 Unit Assessment	
5.2.3 Relevance Assessment	
5.2.4 Overall Assessment	
5.2.5 Evaluation Conclusion	
6 Unit Assessment	
6.1 Analysis and Identification	
6.1.1 Business Identification	
6.1.2 Asset Identification	
6.1.3 Risk Identification	
6.1.4 Major Changes	
6.2 Safety Protection	
6.2.1 Network Security Level Protection	
6.2.2 Safety management system	
6.2.3 Safety management organization	
6.2.4 Safety Management Personnel	
6.2.5 Secure communication network	
6.2.6 Secure computing environment	
6.2.7 Safety Construction Management	
6.2.8 Security Operation and Maintenance Management	
6.2.9 Supply Chain Security Protection	
6.2.10 Data security protection	

- 6.3 Detection and Evaluation
 - 6.3.1 System
 - 6.3.2 Methods and contents
- 6.4 Monitoring and early warning
 - 6.4.1 System
 - 6.4.2 Monitoring
 - 6.4.3 Early Warning
- 6.5 Active Defense
 - 6.5.1 Converging exposed surfaces
 - 6.5.2 Attack detection and blocking
 - 6.5.3 Attack and Defense Drills
 - 6.5.4 Threat Intelligence
- 6.6 Incident Handling
 - 6.6.1 System
 - 6.6.2 Emergency plans and drills
 - 6.6.3 Response and Disposal
 - 6.6.4 Re-identification
- 6.7 Other safety requirements
- 7 Relevance Assessment
 - 7.1 Overview
 - 7.2 Information Collection and Summary
 - 7.3 Intrusion trace analysis
 - 7.4 Business Logic Security Analysis
 - 7.5 Simulation attack path design
 - 7.5.1 Longitudinal path
 - 7.5.2 Horizontal path
 - 7.5.3 Physical Path
 - 7.6 Penetration Testing
- 8 Overall Assessment
 - 8.1 Network Security Management and Control Capability Assessment
 - 8.1.1 Network Security Management and Control Capability Assessment Method
 - 8.1.2 Network security management and control capability assessment results
 - 8.2 Network security protection level assessment
 - 8.2.1 Network security protection level assessment method
 - 8.2.2 Network security protection level assessment results

8.3 Key business security risk analysis and assessment

8.3.1 Risk analysis and assessment methods

8.3.2 Risk assessment results

9 Evaluation Conclusion

Appendix A (Informative) Differences between critical information infrastructure security assessment and network security level assessment

Appendix B (Normative) Penetration Testing Requirements

Appendix C (Normative) Relationship between this document and GB/T 39204-2022, GB/T 22239-2019

Appendix D (Normative) Situations in which the comprehensive security protection capabilities of critical information infrastructure have major security deficiencies

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.

This document is consistent with GB/T 22239 "Basic requirements for information security technology network security level protection" and GB/T 28448 "Information security technology network security level protection basic requirements" "Network Security Level Protection Assessment Requirements" and GB/T 39204 "Information Security Technology Key Information Infrastructure Security Protection Requirements" Constitutes a series of standards for the security protection of critical information infrastructure.

Introduction

In order to cooperate with the implementation of the Cybersecurity Law of the People's Republic of China and the Regulations on the Security Protection of Critical Information Infrastructure, Based on the security level protection system, we fully draw on the relevant departments of our country to carry out network security review, network security inspection and other key areas.

We should fully absorb the measures taken by foreign countries in the security protection of key information infrastructure and combine them with the existing network security testing and Based on the evaluation and assessment results, requirements and standards for security assessment of critical information infrastructure are proposed.

Information security technology Critical information infrastructure security Assessment requirements

1 Scope

This document specifies the requirements and methods for conducting cybersecurity assessments on critical information infrastructure.

This document is applicable to the security testing and assessment of critical information infrastructure carried out by operators of critical information infrastructure and security testing and assessment service agencies.

Review work.

2 Normative references

The contents of the following documents constitute 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 20984-2022 Information security technology Information security risk assessment method
GB/T 22239-2019 Information security technology - Basic requirements for cybersecurity level protection
GB/T 25069-2022 Information Security Technical Terminology
GB/T 28448-2019 Information security technology network security level protection assessment requirements
GB/T 39204-2022 Information security technology - Security protection requirements for critical information infrastructure

3 Terms and definitions

GB/T 22239-2019, GB/T 25069-2022, GB/T 28448-2019 and GB/T 39204-2022 and the following terms and definitions apply to this document.

Public communications and information services, energy, transportation, water conservancy, finance, public services, e-government, national defense science and technology industry and other important industries and fields domains, and other important information that, if destroyed, loses function, or has its data leaked, may seriously endanger national security, national economy and people's livelihood, and public interests.

Requires network facilities, information systems, etc.

[Source. GB/T 39204-2022, 3.1] 3.2 Supply Chain A set of organizations that links multiple resources and processes together to establish a continuous supply relationship based on a service agreement or other purchasing agreement.

NOTE Each of these organizations may act as a demander, a supplier, or both.

[Source. GB/T 39204-2022, 3.2] 3.3 an organization's key business processes comprise