

ICS 35.030
CCS L 80



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

GB/T 34942-2025

Replacing GB/T 34942-2017

**Cybersecurity technology - The assessment method for
security capability of cloud computing service**

网络安全技术 云计算服务安全能力评估方法

Issued on: August 1, 2025

Implemented on: February 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

Preface	VII
Introduction	VIII
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Abbreviations	2
5 Overview	2
5.1 Evaluation Principles	2
5.2 Assessment Content	3
5.3 Evaluating the evidence	3
5.4 Evaluation Implementation Process	3
5.5 Comprehensive Assessment	5
6 System Development and Supply Chain Security Assessment Methods	6
6.1 Resource Allocation	6
6.2 System Lifecycle	6
6.3 Procurement Process	7
6.4 System Documentation	9
6.5 Criticality Analysis	10
6.6 External Services	10
6.7 Developer Security Architecture	12
6.8 Development Process, Standards and Tools	13
6.9 Development Process Configuration Management	15
6.10 Developer Security Testing and Assessment	16
6.11 Training provided by developers	20
6.12 Component Authenticity	20
6.13 Unsupported System Components	21
6.14 Supply Chain Protection	22
7 System and Communication Protection Assessment Methods	25
7.1 Boundary Protection	25
7.2 Transmission confidentiality and integrity protection	28
7.3 Network Interruption	29
7.4 Trusted Path	30

7.5 Password Usage and Management	31
7.6 Device Access Protection	31
7.7 Mobile Code	33
7.8 Session Authentication	34
7.9 Malicious Code Protection	35
7.10 Memory Protection	37
7.11 System Virtualization Security	37
7.12 Network Virtualization Security	40
7.13 Storage Virtualization Security	41
7.14 Communication protection of security management functions	43
8 Access Control Assessment Methods	45
8.1 User identification and authentication	45
8.2 Identifier Management	46
8.3 Authentication Credential Management	47
8.4 Authentication Credentials Feedback	49
8.5 Cryptographic Module Authentication	49
8.6 Account Management	50
8.7 Enforcement of Access Control	51
8.8 Information Flow Control	52
8.9 Least Privilege	54
8.10 Unsuccessful Login Attempts	55
8.11 System Usage Notice	56
8.12 Previous Visit Notice	56
8.13 Concurrent Session Control	57
8.14 Session Lock	57
8.15 Actions to be taken if marking and identification are not carried out	58
8.16 Security Attributes	58
8.17 Remote Access	59
8.18 Wireless Access	60
8.19 Use of external information systems	61
8.20 Publicly accessible content	63
8.21 Global WAN (Web) Access Security	63
8.22 API Access Security	64
9 Data Protection Assessment Methodology	65
9.1 General Data Security	65

9.2 Media Access and Use	66
9.3 Residual Information Protection	69
9.4 Data Usage Protection	70
9.5 Data Sharing Protection	70
9.6 Data Migration Protection	71
10 Configuration Management Assessment Methods	72
10.1 Configuration Management Plan	72
10.2 Baseline Configuration	73
10.3 Change Control	75
10.4 Configuration Parameters	78
10.5 Principle of Minimum Functionality	79
10.6 Information System Component List	80
11 Maintenance Management Assessment Methods	82
11.1 Controlled Maintenance	82
11.2 Maintenance Tools	84
11.3 Remote Maintenance	85
11.4 Maintenance Personnel	86
11.5 Timely Maintenance	88
11.6 Bug Fixes	88
11.7 Safety Function Verification	89
11.8 Software and Firmware Integrity	90
12 Emergency Response Assessment Methods	91
12.1 Incident Handling Plan	91
12.2 Event Handling	93
12.3 Incident Report	94
12.4 Event Handling Support	95
12.5 Security Alert	96
12.6 Error Handling	97
12.7 Emergency Response Plan	98
12.8 Emergency Response Training	100
12.9 Emergency Drills	101
12.10 Information System Backup	102
12.11 Supporting Customers' Business Continuity Plans	104
12.12 Telecommunication Services	105
13 Audit Assessment Methods	106

13.1 Auditable Events	106
13.2 Audit Record Contents	107
13.3 Audit Record Storage Capacity	107
13.4 Response to Audit Process Failure	108
13.5 Audit review, analysis and reporting	109
13.6 Audit Processing and Report Generation	111
13.7 Timestamp	112
13.8 Audit Information Protection	113
13.9 Non-repudiation	114
13.10 Audit Record Retention	115
14 Risk Assessment and Continuous Monitoring Assessment Methodology	116
14.1 Risk Assessment	116
14.2 Vulnerability Scanning	117
14.3 Continuous Monitoring	118
14.4 Information System Monitoring	120
14.5 Spam Monitoring	122
15 Security Organization and Personnel	123
15.1 Security Policies and Procedures	123
15.2 Security Organization	124
15.3 Job Risks and Responsibilities	125
15.4 Personnel Screening	126
15.5 Staff Resignation	126
15.6 Personnel Transfer	128
15.7 Third-party personnel safety	128
15.8 Personnel Punishment	129
15.9 Safety Training	130
16 Physical and Environmental Security Assessment Methods	131
16.1 Physical Facilities and Equipment Site Selection	131
16.2 Physical and Environmental Planning	132
16.3 Physical Environment Access Authorization	134
16.4 Physical Environment Access Control	135
16.5 Output Device Access Control	137
16.6 Physical Access Monitoring	137
16.7 Visitor Access Records	138
16.8 Equipment Transport and Removal	139