GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 28448-2019

Replacing GB/T 28448-2012

Information security technology - Evaluation requirement for classified protection of cybersecurity

信息安全技术

网络安全等级保护测评要求

Issued on: May 10, 2019 **Implemented on: December 01, 2019**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;

Standardization Administration of PRC.

Table of Contents

Foreword 4
Introduction 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 Abbreviations 10
5 Overview of testing-evaluation for classified cybersecurity protection 10
5.1 Method of testing-evaluation for classified cybersecurity protection 10
5.2 Single item testing-evaluation and overall testing-evaluation 12
6 Requirements for level 1 testing-evaluation 12
6.1 General requirements for security testing-evaluation 12
6.2 Extended requirements for testing-evaluation of cloud computing security 40
6.3 Extended requirements for testing-evaluation of mobile internet security 45
6.4 Extended requirements for testing-evaluation of IoT security 48
6.5 Extended requirements for testing-evaluation of industrial control system security 50
7 Requirements for level 2 testing-evaluation 55
7.1 General requirements for security testing-evaluation 55
7.2 Extended requirements for testing-evaluation of cloud computing security 122
7.3 Extended requirements for testing-evaluation of mobile internet security ... 137
7.4 Extended requirements for testing-evaluation of IoT security 143
7.5 Extended requirements for testing-evaluation of industrial control system security 147
8 Requirements for level 3 testing-evaluation 155
8.1 General requirements for security testing-evaluation 155
8.2 Extended requirements for testing-evaluation of cloud computing security 261
8.3 Extended requirements for testing-evaluation of mobile internet security ... 285
8.4 Extended requirements for testing-evaluation of IoT security 293

8.5 Extended requirements for testing-evaluation of industrial control system security 304
9 Requirements for level 4 testing-evaluation 315
9.1 General requirements for security testing-evaluation 315
9.2 Extended requirements for testing-evaluation of cloud computing security 428
9.3 Extended requirements for testing-evaluation of mobile internet security ... 454
9.4 Extended requirements for testing-evaluation of IoT security 463
9.5 Extended requirements for testing-evaluation of industrial control system security 475
10 Requirements for level 5 testing-evaluation 485
11 Overall testing-evaluation 486
11.1 Overview 486
11.2 Testing-evaluation of security control points 486
11.3 Testing-evaluation between security control points 486
11.4 Inter-area testing-evaluation 487
12 Testing-evaluation conclusion 487
12.1 Risk analysis and evaluation 487
12.2 Conclusion of testing-evaluation for classified cybersecurity protection ... 488
Appendix A (Informative) Testing-evaluation intensity 489
Appendix B (Informative) Security evaluation methods can be referred to by bigdata 493
Appendix C (Normative) Descriptions on numbering of testing-evaluation unit 531
References 533

Information security technology - Evaluation requirement for classified protection of cybersecurity

1 Scope

This standard stipulates the general requirements and extended requirements for testing-evaluation of security of classified protection targets.

This standard is applicable to security evaluation service agencies, operation and use units of classified protection targets, for competent departments to conduct security evaluation and provide guidance on the security status of classified protection targets; it is also applicable to network security functional departments when conducting supervision and inspection of the classified protection of cybersecurity.

Note: The level-5 classified protection target is an important supervision and management target, which has a special management mode and security evaluation requirements, so it is not described in this standard.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB 17859-1999 Classified criteria for security protection of computer information system

GB/T 22239-2019 Information security technology - Baseline for classified protection of cybersecurity

GB/T 25069 Information security technology - Glossary

GB/T 25070-2019 Information security technology - Technical requirements of security design for classified protection of cybersecurity

GB/T 28449-2018 Information security technology - Testing-evaluation process guide for classified protection of cybersecurity

GB/T 31167-2014 Information security technology - Security guide of cloud

corresponds to the requirement item (testing-evaluation index) included under the security control point. In the testing-evaluation of each requirement, it may use three testing-evaluation methods: interview, examine, test; it may also use one or two of them. The content of the testing-evaluation implementation fully covers the testing-evaluation requirements of all the requirement items in GB/T 22239-2019 and GB/T 25070-2019. When used, it shall, from the implementation of the testing-evaluation of single item, choose the testing-evaluation requirements of each requirement item in GB/T 22239-2019; meanwhile follow these testing-evaluation requirements to develop the testing-evaluation guidance, so as to standardize and guide testing-evaluation for classified cybersecurity protection activities.

According to the survey results, the business process and data flow of the classified protection targets are analyzed to determine the scope of the testing-evaluation work. Combined with the security level of the classified protection target, comprehensively analyze the functions and characteristics of each device and component in the system; determine the testing-evaluation target at technical level from the attributes of the importance, security, sharing, comprehensiveness, appropriateness of the classified protection target constituting the component; determine the personal and management documents related to it as the testing-evaluation target of the management level. The testing-evaluation targets can be described according to categories, including computer rooms, business application software, host operating systems, database management systems, network interconnection device, security device, interviewers, security management documents.

The testing-evaluation activities for classified cybersecurity protection involve testing-evaluation intensity, including testing-evaluation breadth (coverage) and testing-evaluation depth (intensity). For the implementation of testing-evaluations with a higher level of security protection, it shall choose a wider coverage of testing-evaluation targets and stronger testing-evaluation methods, to obtain more credible testing-evaluation evidence. For a detailed description of the testing-evaluation intensity, see Appendix A.

Each level of testing-evaluation requirements includes 5 parts: general requirements for security testing-evaluation, extended requirements for cloud computing security testing-evaluation, extended requirements for mobile internet security testing-evaluation, extended requirements for IoT security testing-evaluation, extended requirements for industrial control system security testing-evaluation. For bigdata, please refer to Appendix B for the security testing-evaluation method.

does not meet the index requirements of the testing-evaluation unit.

6.1.1.2 Anti-theft and anti-vandalism

6.1.1.2.1 Testing-evaluation unit (L1-PES1-02)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The device or main components shall be fixed and marked with signs that are not easily removed.

b) Testing-evaluation target: Computer room's device or main components.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the device or main components in the computer room are fixed;

2) It shall check whether the device or main components in the computer room are provided with obvious signs that are difficult to remove.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.1.3 Lightning protection

6.1.1.3.1 Testing-evaluation unit (L1-PES1-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Various cabinets, facilities and device shall be securely grounded through the grounding system.

b) Testing-evaluation target: Computer room.

c) Testing-evaluation's implementation: It shall check whether the cabinets, facilities and device in the computer room are grounded.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.1.1.4 Fire protection

6.1.1.4.1 Testing-evaluation unit (L1-PES1-04)

The testing-evaluation unit includes the following requirements:

2) It shall check whether the temperature and humidity are within the allowable range of device operation.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of the testing-evaluation unit

6.1.1.7 Electricity supply

6.1.1.7.1 Testing-evaluation unit (L1-PES1-07)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall configure voltage stabilizer and overvoltage protection device on the power supply line of the computer room.

b) Testing-evaluation target: Power supply facilities in the computer room.

c) Testing-evaluation's implementation: It shall check whether the power supply line is equipped with a voltage regulator and overvoltage protection device.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.1.2 Communication network security

6.1.2.1 Communication transmission

6.1.2.1.1 Testing-evaluation unit (L1-CNS1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall use verification technology to ensure the integrity of data during the communication process.

b) Testing-evaluation target: Device or components that provide verification technical functions.

c) Testing-evaluation's implementation: It shall check whether the verification technology is used to protect its integrity during data transmission.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

b) Testing-evaluation targets: Device or components that provide trusted verification.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the system boot program, system program, etc. of the boundary device are subject to trusted verification based on the root of trust;

2) It shall check whether an alarm is issued when the credibility of the border device is detected to be compromised.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.4 Computing environment security

6.1.4.1 Identity authentication

6.1.4.1.1 Testing-evaluation unit (L1-CES1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall identify and authenticate the identity of the logged-in user. The identification is unique; the identity authentication information has complexity requirements and is replaced regularly.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc., in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the user has adopted identity authentication measures when logging in;

2) It shall check the user list to confirm whether the user identity is unique;

3) It shall check whether there is no empty password user in the user configuration information;

4) It shall check the user's authentication information for complexity and

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check the settings of user account and permission;

2) It shall check whether the access rights of anonymous and default accounts have been disabled or restricted.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.4.2.2 Testing-evaluation unit (L1-CES1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall rename or delete the default account; modify the default password of the default account.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the default account has been renamed or the default account has been deleted;

2) It shall check whether the default password of the default account has been modified.

d) Unit judgment: If 1) or 2) is positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

1) It shall check whether the minimum installation principle is followed;

2) It shall confirm that unnecessary components and applications are not installed.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.4.3.2 Testing-evaluation unit (L1-CES1-07)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall close the unneeded system services, default sharing and high-risk ports.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device and control device, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether non-essential system services and default sharing are turned off;

2) It shall check whether there are no unnecessary high-risk ports.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.4.4 Malicious code prevention

6.1.4.4.1 Testing-evaluation unit (L1-CES1-08)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall install the anti-malware code software or the software with corresponding functions; regularly upgrade and update the anti-malicious code library.

b) Testing-evaluation targets: Operating systems (including host and virtual machine operating systems) and mobile terminals in devices such as terminals and servers.

b) Testing-evaluation targets: The information / network security supervisors and record form documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall be interviewed whether the information / network security supervisor provides a certain number of system administrators;

2) It shall check whether the staffing documents have the staffing status of each position.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.6.3 Authorization and approval

6.1.6.3.1 Testing-evaluation unit (L1-ORS1-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall, according to the responsibilities of various departments and positions, clearly define the authorization items, approval departments and approvers.

b) Testing-evaluation targets: The management system documents and record form documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the department's responsibilities documents clarify the approval items of each department;

2) It shall check whether the job responsibilities document specifies the approval items of each job.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.7 Security management personnel

6.1.7.1 Staff recruitment

6.1.7.1.1 Testing-evaluation unit (L1-HRS1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Special departments or personnel shall be

content and testing-evaluation methods and so on;

2) It shall check whether the security responsibility and disciplinary measures management documents or training documents contain specific security responsibilities and disciplinary measures.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.7.4 External personnel access management

6.1.7.4.1 Testing-evaluation unit (L1-HRS1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall be ensured that external personnel are authorized or approved before accessing the controlled area.

b) Testing-evaluation targets: The management system documents and record form documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the external personnel access management document clearly defines the scope of external personnel access (regions, systems, device, information, etc.), the conditions for external personnel to enter (access to important areas must be submitted in writing before approval), access control measures for external personnel to enter (accompanied or supervised by a dedicated person, etc.), etc.;

2) It shall check whether the written application document for external personnel to visit important areas has the approval signature that the approver allows access to, etc.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.8 Security construction management

6.1.8.1 Rating and filing

6.1.8.1.1 Testing-evaluation unit (L1-CMS1-01)

The testing-evaluation unit includes the following requirements:

such as the network security products obtained sales licenses.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.1.8.4 Project implementation

6.1.8.4.1 Testing-evaluation unit (L1-CMS1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall designate or authorize special departments or personnel to be responsible for the management of the project implementation process.

b) Testing-evaluation target: The record form documents.

c) Testing-evaluation's implementation: It shall check whether a special department or person is designated to carry out progress and quality control of the project implementation.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.1.8.5 Test acceptance

6.1.8.5.1 Testing-evaluation unit (L1-CMS1-05)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall carry out security test.

b) Testing-evaluation target: Person in charge of construction.

c) Testing-evaluation's implementation: It shall interview on whether the person in charge of construction conducted a security test acceptance.

d) Unit judgment: If the above testing-evaluation content is positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet the index requirements of this testing-evaluation unit.

6.1.8.6 System handover

6.1.8.6.1 Testing-evaluation unit (L1-CMS1-06)

The testing-evaluation unit includes the following requirements:

2) It shall check whether the media management record records the media archiving, use and regular inventory.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.9.3 Device maintenance management

6.1.9.3.1 Testing-evaluation unit (L1-MMS1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: All kinds of device (including backup and redundant device), lines shall be regularly maintained and managed by designated special departments or personnel.

b) Testing-evaluation targets: Device administrators and management system documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall interview the device administrator on whether various types of device and lines are regularly maintained by designated personnel or special departments;

2) It shall check whether the department or personnel position responsibility documents clearly define the responsible department for device maintenance and management.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.9.4 Vulnerability and risk management

6.1.9.4.1 Testing-evaluation unit (L1-MMS1-05)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall take necessary measures to identify security vulnerabilities and hidden dangers; repair the discovered security vulnerabilities and hidden dangers in time or after evaluating the possible impact.

b) Testing-evaluation target: The record form documents.

c) The implementation of the testing-evaluation includes the following:

2) It shall check whether the relevant approval records or processes control account application, account creation, account deletion, etc.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.9.6 Malicious code prevention management

6.1.9.6.1 Testing-evaluation unit (L1-MMS1-08)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall improve all users' awareness of anti-malicious code; check the malicious code before the external computer or storage device is connected to the system.

b) Testing-evaluation targets: Person in charge of operation-maintenance and management system documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall be interviewed whether the person in charge of operation-maintenance has taken the form of training and notification to enhance employees' awareness of anti-malicious code;

2) It shall check whether the malicious code prevention management system clearly conducts a malicious code check before an external computer or storage device is connected to the system.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.9.6.2 Testing-evaluation unit (L1-MMS1-09)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall make provisions for malicious code prevention requirements, including authorized use of anti-malware software, malicious code library upgrades, regular killing of malicious code, etc.

b) Testing-evaluation target: Management system documents.

c) Testing-evaluation’s implementation: It shall check whether the malicious code prevention management system includes the authorized use of anti-malware software, malicious code library upgrades, regular killing and so

6.1.9.8 Security incident handling

6.1.9.8.1 Testing-evaluation unit (L1-MMS1-12)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall report the security vulnerabilities and suspicious incidents discovered to the security management department in time.

b) Testing-evaluation targets: The person in charge of operation-maintenance and management system documents.

c) The implementation of the testing-evaluation includes the following:

1) It shall be interviewed whether the person in charge of operation-maintenance informs the user to report to the security management department in a timely manner when they discover security vulnerabilities and suspicious events;

2) It shall check whether there are corresponding reports or related documents after discovering security weaknesses and suspicious events.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.1.9.8.2 Testing-evaluation unit (L1-MMS1-13)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall clarify the reporting and handling process of security incidents; specify the management responsibilities for on-site processing of security incidents, incident reporting, later recovery.

b) Testing-evaluation target: Management system documents.

c) Testing-evaluation's implementation: It shall check whether the security incident reporting and handling process clarifies the work responsibilities related to the security incident, including the reporting organization (person), reported organization (person), disposal organization and other responsibilities.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.2.4.1.2 Testing-evaluation unit (L1-CES2-02)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Cloud service customers shall be allowed to set access control policies between different virtual machines.

b) Testing-evaluation targets: Virtual machines and security groups or related components.

c) Testing-evaluation's implementation: Check whether cloud service customers can set access control policies between different virtual machines.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.2.4.2 Data integrity and confidentiality

6.2.4.2.1 Testing-evaluation unit (L1-CES2-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall ensure that cloud service customer data, user personal information, etc. are stored in China. If it needs to leave the country, it shall follow the relevant national regulations.

b) Testing-evaluation targets: Database server, data storage device, management document records.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the server and data storage device where the cloud service customer data and user personal information are stored are located in China;

2) It shall check whether the above data complies with relevant national regulations when leaving the country.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.2.5.1.3 Testing-evaluation unit (L1-CMS2-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The authority and responsibility of the cloud service provider shall be specified in the service level agreement, including management scope, division of responsibilities, access authorization, privacy protection, code of conduct, liability for breach of contract.

b) Testing-evaluation target: Service level agreement or service contract.

c) Testing-evaluation's implementation: It shall check whether the service level agreement or service contract regulates the permissions and responsibilities of the security service provider and cloud service provider, including management scope, division of responsibilities, access authorization, privacy protection, code of conduct, breach of contract responsibility.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.2.5.2 Supply chain management

6.2.5.2.1 Testing-evaluation unit (L1-CMS2-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall ensure that the selection of suppliers complies with relevant national regulations.

b) Testing-evaluation target: Record form documents.

c) Implementation of testing-evaluation: It shall check whether the choice of cloud service provider complies with relevant national regulations.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.3 Extended requirements for testing-evaluation of mobile internet security

6.3.1 Security physical environment

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The wireless access device shall enable the access authentication function; meanwhile prohibit the use of WEP authentication; if using passwords, the length is not less than 8 characters.

b) Testing-evaluation target: Wireless access device.

c) Testing-evaluation's implementation: It shall check whether the access authentication function is turned on; whether it is authenticated using a method other than WEP; the key length is not less than 8 bits.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.3.3 Computing environment security

6.3.3.1 Management and control of mobile application

6.3.3.1.1 Testing-evaluation unit (L1-CES3-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall have the function of selecting the installation and operation of application software.

b) Testing-evaluation target: Mobile terminal management client.

c) Testing-evaluation's implementation: It shall check whether it has the function of selecting the installation and operation of application software.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

6.3.4 Security construction management

6.3.4.1 Procurement of mobile application software

6.3.4.1.1 Testing-evaluation unit (L1-CMS3-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall be ensured that the application software installed and run on the mobile terminal is from a reliable distribution channel or signed with a reliable certificate.

b) Testing-evaluation target: Mobile terminal.

and fire resistance.

b) Testing-evaluation target: Outdoor control device.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether it is placed in a box or device made of iron plates or other fireproof materials and fastened;

2) It shall check whether the box or device has the ability of ventilation, heat dissipation, anti-theft, rain-proof and fire prevention.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.5.1.1.2 Testing-evaluation unit (L1-PES5-02)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Outdoor control device shall be placed away from strong electromagnetic interference, strong heat sources, or other environments. If it cannot be avoided, emergency treatment and maintenance shall be done in time to ensure that the device operates normally.

b) Testing-evaluation target: Outdoor control device.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the location of placement is away from strong electromagnetic interference or heat sources;

2) It shall check whether there are records of emergency handling and maintenance.

d) Unit judgment: If 1) or 2) is positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.5.2 Communication network security

6.5.2.1 Network architecture

6.5.2.1.1 Testing-evaluation unit (L1-CNS5-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The industrial control system and other systems

6.5.3.1.1 Testing-evaluation unit (L1-ABS5-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Access control device shall be deployed between the industrial control system and other enterprise systems; access control policies shall be configured, to prohibit any general network services such as E-Mail, Web, Telnet, Rlogin, FTP, etc. that cross the regional boundary.

b) Testing-evaluation targets: Devices such as gatekeepers, firewalls, routers, switches, and other devices that provide access control functions.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the access control device is deployed at the network boundary between the industrial control system and other systems of the enterprise; whether the access control policy is configured;

2) It shall check the device security policy, to see if E-Mail, Web, Telnet, Rlogin, FTP and other general network services are prohibited from crossing the border.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.5.3.2 Wireless usage control

6.5.3.2.1 Testing-evaluation unit (L1-ABS5-02)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: All users (personnel, software processes or devices) participating in wireless communication shall be provided with unique identification and authentication.

b) Testing-evaluation target: Wireless communication network and device.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the user of wireless communication has used identity authentication measures when logging in;

2) It shall check whether the user's identity is unique.

d) Unit judgment: If both 1) and 2) are positive, it meets the index

d) Unit judgment: If 1) or 2) is positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

6.5.4.1.2 Testing-evaluation unit (L1-CES5-02)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: After sufficient testing-evaluation, carry out patch and firmware updates on the control device without affecting the security and stable operation of the system.

b) Testing-evaluation target: Control device.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether there is a test report or testing-evaluation record;

2) It shall check whether the control device's version, patch and firmware have been updated after testing.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7 Requirements for level 2 testing-evaluation

7.1 General requirements for security testing-evaluation

7.1.1 Security physical environment

7.1.1.1 Selection of physical location

7.1.1.1.1 Testing-evaluation unit (L2-PES1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The computer room site shall be selected in a construction with the capability of shockproof, windproof and rainproof.

b) Testing-evaluation targets: Record documents and computer room.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the construction has seismic approval documents for construction seismic fortification;

b) Testing-evaluation target: Acceptance documents of computer room.

c) Testing-evaluation's implementation: Check whether the acceptance documents of the computer room specify the fire resistance rating of the relevant construction materials.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.1.6 Waterproof and moisture-proof

7.1.1.6.1 Testing-evaluation unit (L2-PES1-09)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall take measures to prevent rainwater from penetrating through the windows, roofs and walls of the computer room.

b) Testing-evaluation target: Computer room.

c) Testing-evaluation's implementation: It shall check whether windows, roofs and walls have taken measures against rain penetration.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.1.6.2 Testing-evaluation unit (L2-PES1-10)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall take measures to prevent the transfer and penetration of water vapor condensation and underground water accumulation in the computer room.

b) Testing-evaluation target: Computer room.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether it takes measures to prevent condensation of water vapor in the computer room;

2) It shall check whether it take measures for draining underground water and preventing infiltration of underground water in the computer room.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or

7.1.1.9 Power supply

7.1.1.9.1 Testing-evaluation unit (L2-PES1-13)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall configure voltage stabilizer and overvoltage protection device on the power supply line of the computer room.

b) Testing-evaluation target: Power supply facilities in the computer room.

c) Testing-evaluation's implementation: It shall check whether the power supply line is equipped with a voltage regulator and overvoltage protection device.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.1.9.2 Testing-evaluation unit (L2-PES1-14)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall provide short-term backup power supply, to at least meet the normal operation requirements of the device in the event of power failure.

b) Testing-evaluation target: Standby power supply facility in the computer room.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the computer room is equipped with a backup power system such as UPS;

2) It shall check whether the backup power supply system such as UPS meets the normal operation requirements of the device in the event of power failure.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.1.10 Electromagnetic protection

7.1.1.10.1 Testing-evaluation unit (L2-PES1-15)

a) Testing-evaluation index: It shall avoid deployment of important network areas at the boundary; it shall take reliable technical isolation between important network areas and other network areas.

b) Testing-evaluation target: Network topology.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the network topology map is consistent with the actual network operating environment;

2) It shall check whether the important network area is not deployed at the network boundary;

3) It shall check whether reliable technical isolation means, such as gatekeepers, firewalls and device access control lists (ACLs), are adopted between important network areas and other network areas.

d) Unit judgment: If 1) to 3) are all positive, then meet the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meet the index requirements of the testing-evaluation unit.

7.1.2.2 Communication transmission

7.1.2.2.1 Testing-evaluation unit (L2-CNS1-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall adopt the verification technology to ensure the integrity of data during the communication process.

b) Testing-evaluation target: The device or components that provide verification technical functions.

c) Testing-evaluation's implementation: It shall check whether the verification technology is used to protect its integrity during data transmission.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.2.3 Trusted verification

7.1.2.3.1 Testing-evaluation unit (L2-CNS1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It may, based on the root of trust, carry out the

c) Testing-evaluation's implementation: It shall check whether mechanisms such as session authentication are used to provide explicit permission / denial of access to incoming and outgoing data streams.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.3.3 Intrusion prevention

7.1.3.3.1 Testing-evaluation unit (L2-ABS1-06)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall monitor the network attack behavior at key network nodes.

b) Testing-evaluation targets: The anti-APT attack system, network traceback system, anti-DDoS attack system, intrusion protection system, intrusion detection system or related components.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the following attack behaviors can be detected: port scanning, strong attacks, Trojan backdoor attacks, denial of service attacks, buffer overflow attacks, IP fragmentation attacks, network worm attacks, etc.;

2) It shall check whether the rule base version of the relevant system or device has been updated to the latest version;

3) It shall check whether relevant system or device configuration information or security policies can cover all key nodes of the network.

d) Unit judgment: If 1) to 3) are all positive, then meet the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meet the index requirements of the testing-evaluation unit.

7.1.3.4 Malicious code prevention

7.1.3.4.1 Testing-evaluation unit (L2-ABS1-07)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall detect and remove the malicious code at key network nodes; maintain the upgrade and update of the malicious code protection mechanism.

other audit-related information.

b) Testing-evaluation targets: Comprehensive security audit system, etc.

c) Testing-evaluation's implementation: It shall check whether the audit record information includes the date and time of the event, the user, the type of event, whether the event is successful, other audit-related information.

d) Unit judgment: If the above testing-evaluation content is implemented, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of the testing-evaluation unit.

7.1.3.5.3 Testing-evaluation unit (L2-ABS1-10)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The audit records shall be protected and regularly backed up to avoid unexpected deletion, modification, or overwriting.

b) Testing-evaluation targets: Comprehensive security audit system, etc.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether technical measures have been taken to protect audit records;

2) It shall check whether technical measures are taken to regularly back up the audit records; meanwhile check the backup policy.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.3.6 Trusted verification

7.1.3.6.1 Testing-evaluation unit (L2-ABS1-11)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It may, based on the root of trust, carry out trusted verification of the system boot program, system program, important configuration parameters and boundary protection application of the boundary device; issue alarm after detecting the damage of credibility; form the verification results into audit record and send it to the security management center.

3) It shall check whether there is no empty password user in the user configuration information;

4) It shall check whether the user's authentication information has complexity requirements and is replaced regularly.

d) Unit judgment: If all of 1) to 4) are positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of the testing-evaluation unit.

7.1.4.1.2 Testing-evaluation unit (L2-CES1-02)

a) Testing-evaluation index: It shall have a login failure handling function; it shall be configured and enabled to end the session, limit the number of illegal logins, automatically log out when the login connection times out.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the login failure handling function is configured and enabled;

2) It shall check whether the function of restricting illegal login is configured and enabled; take specific actions after illegal login reaches a certain number of times, such as account lockout;

3) It shall check whether the login connection timeout and auto logout functions are configured and enabled.

d) Unit judgment: If 1) to 3) are all positive, then meet the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meet the index requirements of the testing-evaluation unit.

7.1.4.1.3 Testing-evaluation unit (L2-CES1-03)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: When remote management is performed, it shall take necessary measures to prevent the eavesdropping of authentication

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall provide security audit function. The audit covers every user; it audits important user behaviors and important security events.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the security audit function is provided and turned on;

2) It shall check whether the scope of the security audit covers every user;

3) It shall check whether important user behaviors and important security events are audited.

d) Unit judgment: If 1) to 3) are all positive, then meet the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meet the index requirements of the testing-evaluation unit.

7.1.4.3.2 Testing-evaluation unit (L2-CES1-09)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The audit record shall include the date and time of the event, the user, the type of event, whether the event is successful, other audit-related information.

b) Testing-evaluation targets: The operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device, control device, business application system, database management system, middleware and system management software and system design documents, etc. in devices such as terminals and servers.

c) Testing-evaluation's implementation: It shall check whether the audit

devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device and control device, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the minimum installation principle is followed;

2) It shall check that unnecessary components and applications are not installed.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.4.4.2 Testing-evaluation unit (L2-CES1-12)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall turn off the unneeded system services, default sharing, high-risk ports.

b) Testing-evaluation targets: Operating systems (including host and virtual machine operating systems), network devices (including virtual network devices), security devices (including virtual security devices), mobile terminals, mobile terminal management systems, mobile terminal management client, sensor node device, gateway node device and control device, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether non-essential system services and default sharing are turned off;

2) It shall check whether there are no unnecessary high-risk ports.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.4.4.3 Testing-evaluation unit (L2-CES1-13)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The management terminal managed through the network shall be restricted by setting the terminal access method or network address range.

device, business application system, database management system, middleware and system management software, etc. in devices such as terminals and servers.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether there are no high-risk vulnerabilities, such as vulnerability scanning, penetration testing, etc.;

2) It shall check whether the vulnerabilities are patched in a timely manner after sufficient testing-evaluation.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.4.5 Malicious code prevention

7.1.4.5.1 Testing-evaluation unit (L2-CES1-16)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall install anti-malware code software or software with corresponding functions; meanwhile regularly upgrade and update the anti-malicious code library.

b) Testing-evaluation targets: Operating systems (including host and virtual machine operating systems) and mobile terminals in devices such as terminals and servers.

c) The content of the testing-evaluation implementation includes the following:

1) It shall check whether anti-malware software or the software of corresponding function is installed;

2) It shall check whether the upgrade and update of the anti-malicious code library is performed regularly.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.4.6 Trusted verification

7.1.4.6.1 Testing-evaluation unit (L2-CES1-17)

The testing-evaluation unit includes the following requirements:

established.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.4.10.2 Testing-evaluation Unit (L2-CES1-23)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: Unauthorized access and illegal use of user personal information shall be prohibited.

b) Testing-evaluation targets: Business application systems and database management systems.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether technical measures are taken to restrict access to and use of user personal information;

2) It shall check whether a management system and procedures concerning the protection of users' personal information have been established.

d) Unit judgment: If both 1) and 2) are positive, it meets the index requirements of this testing-evaluation unit; otherwise, it does not meet or partially meets the index requirements of this testing-evaluation unit.

7.1.5 Security management center

7.1.5.1 System management

7.1.5.1.1 Testing-evaluation unit (L2-SMC1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall authenticate the identity of the system administrator; it only allows to perform system management operations through specific commands or operation interfaces; audit these operations.

b) Testing-evaluation target: System that provides centralized system management functions.

c) The implementation of the testing-evaluation includes the following:

1) It shall check whether the system administrator is authenticated;

2) It shall check whether only system administrators are allowed to

1) It shall check whether the audit administrator's identity is authenticated;

2) It shall check whether only the audit administrator is allowed to perform security audit operations through specific commands or operation interfaces;

3) It shall check whether the operations of the audit administrator are audited.

d) Unit judgment: If 1) to 3) are all positive, then meet the index requirements of the testing-evaluation unit; otherwise, it does not meet or partially meet the index requirements of the testing-evaluation unit.

7.1.5.2.2 Testing-evaluation unit (L2-SMC1-04)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: The audit records shall be analyzed by the audit administrator and processed according to the analysis results, including storage, management, query of the audit records according to the security audit policy.

b) Testing-evaluation targets: Comprehensive security audit systems, database audit systems, other systems which provide centralized audit functions.

c) Testing-evaluation's implementation: It shall check whether the audit records are analyzed by the audit administrator and processed according to the analysis results, including storage, management, query of the audit records according to the security audit policy.

d) Unit judgment: If the content of the above testing-evaluation is positive, it meets the index requirements of the testing-evaluation unit; otherwise, it does not meet the index requirements of the testing-evaluation unit.

7.1.6 Security management system

7.1.6.1 Security policy (L2-PSS1-01)

The testing-evaluation unit includes the following requirements:

a) Testing-evaluation index: It shall establish the overall policy and security policies of cybersecurity work; clarify the overall target, scope, principles, security framework of the organization's security work.

b) Testing-evaluation target: General policy strategic documents.

c) Testing-evaluation's implementation: It shall check whether the general

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------