GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 28449-2018

Replacing GB/T 28449-2012

Information security technology - Testing and evaluation process guide for classified protection of cyber security

信息安全技术

网络安全等级保护测评过程指南

Issued on: December 28, 2018 **Implemented on: July 01, 2019**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Testing and evaluation process guide for classified protection of cyber security

1 Scope

This Standard standardizes testing and evaluation process for classified protection of cyber security (hereinafter referred to as “classified testing and evaluation”). It also specifies testing and evaluation as well as work tasks.

This Standard is applicable for testing and evaluation organization, supervision department of classified target as well as operation user to carry out testing and evaluation for classified protection of cyber security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB 17859, *Classified criteria for security protection of computer information system*

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

GB/T 25069, *Information security technology - Glossary*

GB/T 28448, *Information security technology - Evaluation requirement for classified protection of cybersecurity*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB 17859, GB/T 22239 and GB/T 28448 apply.

This Standard gives corresponding working procedure, main task, output file as well as duties of relevant parties of each activity. Each work task has corresponding input, task description and output product.

4.2 Classified testing and evaluation risks

4.2.1 Risk that affects system's normal operation

During on-site testing and evaluation, it needs to conduct a certain verification testing to equipment and system. Some testing contents need on-board verification and need checking some information, which might cause a certain impact on system's operation even cause possible mis-operation.

In addition, when it uses testing tool to conduct vulnerability scanning test, performance test and penetration test, it might cause a certain impact on network and system's load. Penetration attack test might also affect normal operation of server and system, for example, it might cause reboot, service interruption, and code implanted during penetration process is not completely cleaned up.

4.2.2 Risk of sensitive information disclosure

Testing and evaluation personnel intentionally or unintentionally discloses information of system status under test, such as network topology, IP address, business process, business data, security mechanism, security risk, and related file information.

4.2.3 Risk of Trojan implant

After testing and evaluation personnel completes penetration test, he or she may intentionally or unintentionally not clean or not clean thoroughly testing tool that is used during penetration test process, or because testing computer has Trojan program. All may bring Trojan implant risk in system under test.

4.3 Classified testing and evaluation risk avoidance

During classified testing and evaluation, it shall take the following measures to avoid risks:

a) Signing of a commissioned testing and evaluation agreement

Before testing and evaluation are officially started, testing and evaluation party and party under test and evaluated need to, in a mode of commissioned agreement, SPECIFY goal, scope, personnel composition, planning, implementation steps and requirements of testing and evaluation as well as responsibilities and obligations of both parties, so as to make both parties of testing and evaluation reach a consensus on basic problems in testing and evaluation process.

Output/product: project planning proposal.

5.2.2 Information collection and analysis

Through checking material that has been obtained by classified target under test or using system survey form, testing and evaluation organization knows composition of entire system and protection situation as well as relevant situation of responsible department, so as to lay a foundation for on-site testing and evaluation as well as security evaluation.

Input: project planning proposal, system survey form, relevant information of classified target under test.

Task description:

a) Testing and evaluation organization collects relevant information required for classified testing and evaluation, including management structure, technical system, operation, construction plan, and related test files during construction of testing and evaluation trusted organization. See Annex C for supplementary collection information of cloud computing platform, Internet of Things, mobile internet, industrial control system.

b) Testing and evaluation organization submits system survey form to testing and evaluation entrusted organization, supervises and urges relevant personnel of classified target under test to correctly fill in survey form.

c) Testing and evaluation organization takes back survey form that has been filled, analyzes survey results so as to understand and be familiar with actual situation of classified target under test.

   When analyzing collected information, it may use the following methods:

   1) Use system analysis method to analyze entire network structure and system composition, including network structure, external boundary, number and level of classified target, distribution of classified target at different security protection levels, and load application.

   2) Use decomposition and comprehensive analysis method to analyze classified target boundary and system composition component, including physical and logical boundaries, hardware resources, software resources, information resources.

   3) Use comparison and analogy analysis method to analyze interrelation of classified target, including application architecture, application processing flow, processing information type, business data processing flow, service target, number of users.

d) If information in survey form is inaccurate, imperfect or contradictory,

According to results of system survey, analyze entire business flow of classified target under test, data flow, scope, characteristics as well as main functions of each device and components so as to confirm target of testing and evaluation of this testing and evaluation.

Input: completed survey form, various technical information related to classified target under test.

Task description:

a) Identify and describe overall structure of classified target under test

According to basic situation of classified target under test obtained from survey form, identify overall structure of classified target under test and describe it.

b) Identify and describe boundaries of classified target under test

According to completed survey form, identify boundaries of classified target under test as well as boundary device and describe.

c) Identify and describe network area of classified target under test

In general, classified target shall, according to business type as well as its degree of importance, divide classified target into different areas. According to area division, describe main business application, business flow, area boundaries as well as connection between them in every area.

d) Identify and describe main devices of classified target under test

When describing devices in system, taking area as clue, specifically describe devices deployed in each area. Describe major business born by each device, situation of software installation as well as main connection between each device.

e) Confirm target of testing and evaluation

Combining security level and degree of importance of classified target under test, comprehensively analyze functions and characteristics of each device and component in system. Confirm target of testing and evaluation of technical level from attributes such as importance, security, sharing, comprehensiveness and appropriateness of components of classified target under test. Confirm personnel and management file related to classified target under test as target of testing and evaluation. See Annex D for confirmation rules and examples for target of testing and evaluation.

f) Describe target of testing and evaluation

scheme.

6.2.3 Confirmation of testing and evaluation contents

This sub-clause confirms specific implementation contents of on-site testing and evaluation, i.e., testing and evaluation content of individual item.

Input: completed system survey form, target of testing and evaluation part in testing and evaluation scheme, testing and evaluation indicators part in testing and evaluation scheme.

Task description:

According to GB/T 22239, combine testing and evaluation indicators obtained above and target of testing and evaluation together. Make testing and evaluation indicators mapped on each target of testing and evaluation. By combining with characteristics of target of testing and evaluation, explain testing and evaluation method that is adopted by each target of testing and evaluation. This constitutes contents of individual testing and evaluation that can be specifically tested and evaluated. Testing and evaluation contents are foundation for testing and evaluation personnel to develop testing and evaluation guide.

Output/product: implementation part of testing and evaluation in testing and evaluation scheme.

6.2.4 Confirmation of tool testing method

In classified testing and evaluation, use testing tools for testing. Testing tools could be vulnerability scanner, penetration test tool set, protocol analyzer. See Annex C for supplementary test contents of Internet of Things, mobile internet, industrial control system.

Input: implementation part of testing and evaluation in testing and evaluation scheme, GB/T 22239, list of selected testing and evaluation tools.

Task description:

a) Confirm tool testing environment. According to real-time requirements for system under test, it may select production environment or backup environment that is same with production environment in each security configuration, production verification environment or testing environment as tool testing environment.

b) Confirm target of testing and evaluation under test.

c) Select testing path. Access of testing tool uses step-to-step and point-to-point access from outside to inside, from other network to local network,

Input: implementation part of individual testing and evaluation of testing and evaluation scheme, tool testing content and method part.

Task description:

a) Describe target of individual testing and evaluation, including name, position information, usage, management personnel.

b) According to implementation of individual testing and evaluation in GB/T 28448, confirm testing and evaluation activities, including testing and evaluation items, testing and evaluation method, operation steps and expected results.

   Testing and evaluation items refer to requirements in this usage example to this target of testing and evaluation in GB/T 22239. In GB/T 28448, it corresponds to “testing and evaluation indicators” in each individual testing and evaluation. Testing and evaluation methods refer to three methods: interview, verification and testing; see Annex E for details. Specific to target of testing and evaluation, verification can be refined to file review, field inspection and configuration verification. Each testing and evaluation item might correspond to multiple testing and evaluation methods. Operation steps refer to commands or steps that shall be executed in on-site testing and evaluation. When involving in testing, it shall describe tool testing path and access point. Expected results refer to results that shall be obtained and data obtained according to operation steps under normal situation.

c) Individual testing and evaluation, usually in form, designs and describes testing and evaluation items, testing and evaluation methods, operation steps and expected results. Overall testing and evaluation usually expresses in text description, organizes in a mode of testing and evaluation example.

d) According to testing and evaluation guide, form a record form of testing and evaluation results.

Output/product: testing and evaluation guide, record form of testing and evaluation results.

6.2.6 Formation of testing and evaluation scheme

Testing and evaluation scheme is foundation of implementation of classified testing and evaluation to guide on-site implementation of classified testing and evaluation. Testing and evaluation scheme shall include but not limited to the following items: project overview, target of testing and evaluation, testing and evaluation indicators, testing and evaluation contents, testing and evaluation methods.

evaluation coordinators and testing and evaluation environment required.

Output/product: meeting minutes, testing and evaluation scheme, work plan of on-site testing and evaluation and risk notification, letter of authorization of on-site testing and evaluation.

7.2.2 On-site testing and evaluation and results record

This task is mainly for testing and evaluation personnel to implement testing and evaluation according to testing and evaluation guide and accurately record evidence source obtained during testing and evaluation process in details.

Input: work plan of on-site testing and evaluation, letter of authorization of on-site testing and evaluation, on-site testing and evaluation guide, on-site testing and evaluation record form.

Task description:

a) Testing and evaluation personnel and testing and evaluation coordinators confirm that key data in target of testing and evaluation has been backed up.

b) Testing and evaluation personnel confirms that conditions for testing and evaluation have been well prepared, target of testing and evaluation works normal and system is in a relatively good condition.

c) Testing and evaluation personnel, according to testing and evaluation guide, implements on-site testing and evaluation to obtain relevant evidence and information. On-site testing and evaluation usually includes three testing and evaluation modes: interview, verification and testing. See Annex E for details.

d) After testing and evaluation end, testing and evaluation personnel and testing and evaluation coordinators timely confirm that whether testing and evaluation has make bad impact on target of testing and evaluation, whether target of testing and evaluation as well as system work as normal.

Output/product: various testing and evaluation result records.

7.2.3 Result confirmation and material return

This task is mainly to confirm evidence source record obtained during testing and evaluation process and return files borrowed during testing and evaluation process.

Input: various testing and evaluation result records, electronic output record after tool testing is completed.

Task description:

a) For each testing and evaluation item, analyze whether threat with which this testing and evaluation item is against exists in classified target under test. If it doesn't exist, this testing and evaluation item shall be marked as inapplicable item.

b) Analyze testing and evaluation evidence of individual testing and evaluation item. Compare with expected testing and evaluation results of required contents to give individual testing and evaluation result and compliance score.

c) If testing and evaluation evidence shows that all required contents are consistent with expected testing and evaluation results, individual testing and evaluation result of this testing and evaluation item shall be determined as compatible. If testing and evaluation evidence shows that all required contents are not consistent with expected testing and evaluation results, individual testing and evaluation result of this testing and evaluation item shall be determined as incompatible; otherwise it shall determine that individual testing and evaluation result of this testing and evaluation item is partially compatible.

Output/product: record part of classified testing and evaluation result in testing and evaluation report.

8.2.2 Determination of unit testing and evaluation result

This task is mainly to gather individual testing and evaluation result, to separately conduct statistics on individual testing and evaluation result of different target of testing and evaluation, so as to determine unit testing and evaluation result.

Input: record part of classified testing and evaluation result in testing and evaluation report.

Task description:

a) According to level, respectively gather individual testing and evaluation result of testing and evaluation indicator that different target of testing and evaluation corresponds, including number of testing and evaluation items, number of compatible items.

b) Analyze compliance of all testing and evaluation items under each control point and give unit testing and evaluation result. Rules for determination of unit testing and evaluation result:

- when individual testing and evaluation results of all applicable testing

item can have correlation with it, what kind of correlation it is, whether effect that is produced by such correlation can “compensate” insufficiency of this testing and evaluation item or “weaken” protection of this testing and evaluation item, as well as that whether testing and evaluation result of this testing and evaluation item shall affect testing and evaluation result of other testing and evaluation items that have correlation with it.

c) According to overall testing and evaluation, correct compliance score of individual testing and evaluation item and problem severity value.

Output/product: overall testing and evaluation part in testing and evaluation report.

8.2.4 Evaluation of system security assurance

Combining results of individual testing and evaluation and overall testing and evaluation, calculate corrected security control point score and level score. According to scores, conduct overall evaluation on security assurance of classified target under test.

Input: record part of classified testing and evaluation result in testing and evaluation report and overall testing and evaluation part.

Task description:

a) According to overall testing and evaluation results, calculate corrected individual testing and evaluation result of each target of testing and evaluation and compliance score.

b) According to individual item’s compliance score of each target, calculate score of security control point.

c) According to score of security control point, calculate score of security level.

d) According to score of security control point and score of security level, conduct overall evaluation on effective protection measures that have been adopted by classified target under test and existing major security problems.

Output: evaluation part of system security assurance in testing and evaluation report.

8.2.5 Analysis of security problem risk

Testing and evaluation personnel, according to specifications and standards related to classified protection, use risk analysis method to analyze possible impact of existing security problems in classified testing and evaluation results

b) Basic compliance: There are security problems in classified target. Not all statistical results of some compatible items and incompatible items are 0 but existing security problems shall not cause classified target to face high-level security risk and comprehensive score is not less than threshold value.

c) Incompliance: There are security problems in classified target. Not all statistical results of some compatible items and incompatible items are 0 and existing security problems shall cause classified target to face high-level security risk or comprehensive score is less than threshold value.

Output/product: conclusion part of classified testing and evaluation in testing and evaluation report.

8.2.7 Preparation of testing and evaluation report

According to each analysis process of report preparation, form classified testing and evaluation report. Format of classified testing and evaluation report shall comply with “Template of testing and evaluation report of information security classified protection” (see Annex F for template example).

Input: testing and evaluation scheme, “Template of testing and evaluation report of information security classified protection”, analysis content of testing and evaluation result.

Task description:

a) Testing and evaluation personnel organize outputs/products of tasks above. According to “Template of testing and evaluation report of information security classified protection”, prepare corresponding parts of testing and evaluation report. It shall problem testing and evaluation report separately for each classified target under test.

b) For existing security risks of classified target under test, from perspective of system security, propose corresponding suggestions on improvement and prepare suggestions on problem handling of testing and evaluation report.

c) After report is prepared, testing and evaluation organization shall, according to testing and evaluation agreement, relevant files submitted by testing and evaluation entrusted organization, original testing and evaluation record and other supplementary information, review testing and evaluation report.

d) After review is passed, person in charge of project shall sign and confirm to testing and evaluation entrusted organization.

Annex A

(Normative)

Workflow of classified testing and evaluation

Classified testing and evaluation as well flow that are implemented by entrusted testing and evaluation organization shall be different from self-check and flow of operator, user. Initial classified testing and evaluation AND second classified testing and evaluation as well as their flows are not exactly same. Classified testing and evaluation as well as flow for classified target at different level are not same either.

Initial classified testing and evaluation of entrusted testing and evaluation organization on classified target are divided into four activities: preparation of testing and evaluation, scheme preparation, on-site testing and evaluation, report preparation. See Figure A.1 for details.

If classified target under test has been implemented classified testing and evaluation once (or several times), four activities in Figure A.1 shall remain unchanged but specific task contents shall change. Testing and evaluation organization and personnel shall, according to existing problems in previous classified testing and evaluation as well as actual situation of classified target under test, adjust contents of partial work tasks. For example, in information collection and analysis task, especially collect changed information since previous classified testing and evaluation; other information may refer to result of previous classified testing and evaluation. It shall try to select failed item or item with problem in previous classified testing and evaluation as target of testing and evaluation. Testing and evaluation contents shall also focus on problems found in previous classified testing and evaluation as well as changed content of classified target, record of operation-maintenance process since previous classified testing and evaluation.

Basic work activities of classified testing and evaluation of different level classified target shall be completely consistent with classified testing and evaluation of classified target in Figure A.1, that is, preparation of testing and evaluation, scheme preparation, on-site testing and evaluation and report preparation. Figure A.1 gives a more comprehensive workflow and tasks. Some contents of specific work task of each activity of classified testing and evaluation of lower-level classified target shall be deleted or simplified based on Figure A.1. Some contents of work task of classified testing and evaluation of higher-level classified target shall be added or refined. For example, for classified testing and evaluation of level-four classified target, during task confirmation of target of testing and evaluation, it does not only require to confirm target of

Annex B

(Normative)

Requirements for classified testing and evaluation

B.1 Standards and principles that shall be followed

Classified testing and evaluation shall be performed according to relevant technical standards of classified protection. Relevant technical standards mainly include GB/T 22239, GB/T 28448. Goal and contents of classified testing and evaluation shall be according to GB/T 22239. Testing and evaluation implementation method for specific testing and evaluation item shall be in accordance with GB/T 28448.

In implementation of classified testing and evaluation, it shall follow principles of objectivity and impartiality, economy and reusability, repeatability and reproducibility, and completeness of results, so as to ensure testing and evaluation fair, scientific, reasonable and perfect.

B.2 Proper selection and strength assurance

Proper selection means that selection of specific target of testing and evaluation shall be appropriate. It shall avoid important target, target that might have security risk not selected. It shall also avoid too many selections to make workload increased.

Strength assurance means that it shall implement testing and evaluation strength that matches its classification to classified target under test.

B.3 Behavior standardization and risk avoidance

Implementation of classified testing and evaluation by testing and evaluation organization shall be standardized, including: to form internal security system, to form process control system, to stipulate review procedures for relevant files, to designate a person responsible to save archive of classified testing and evaluation.

Behavior of testing and evaluation personnel shall be standardized, including: testing and evaluation personnel shall wear work card when entering scene; to use computer and tool specially for testing and evaluation; perform testing and evaluation strictly according to use specification of testing and evaluation guide; to accurately record testing and evaluation evidence; not to evaluate testing and evaluation results without authorization; not to copy testing and evaluation results to non-testing and evaluation personnel; only check relevant information

Annex C

(Normative)

Supplement for classified testing and evaluation of new technology and new application

C.1 Supplement for classified testing and evaluation of could computing

C.1.1 Preparation of testing and evaluation

C.1.1.1 Information collection and analysis

For classified testing and evaluation to cloud computing platform, relevant information collected by testing and evaluation organization shall also include management structure of cloud computing platform operator, technology implementation mechanism and structure, operation situation, classification of cloud computing platform, classified testing and evaluation result of cloud computing platform.

For classified testing and evaluation for cloud tenant system, relevant information collected by testing and evaluation organization shall also include relation between operator of cloud computing platform and tenant, relevant information of classified target.

In classified testing and evaluation of cloud tenant system, testing and evaluation entrusted organization is cloud tenant. Could tenant shall supervise and urge relevant personnel of classified target under test as well as relevant personnel of cloud computing platform operator to accurately fill survey form.

C.1.1.2 Duties of both parties in preparation of testing and evaluation

Duties of testing and evaluation entrusted organization of cloud tenant shall also include: responsible for communication and coordination with cloud service provider so as to provide assistance to information collection of testing and evaluation personnel.

C.1.2 Duties of both parties in on-site testing and evaluation

Duties of testing and evaluation entrusted organization of cloud tenant shall also include: assist testing and evaluation organization to obtain on-site testing and evaluation authorization of cloud computing platform, responsible for coordinating could service provider to cooperate testing and evaluation or provide classified testing and evaluation report of cloud computing platform.

C.1.3 Example of determination of target of testing and evaluation

testing and evaluation organization shall also include deploying situation of various wireless access equipment, using situation of mobile terminal, mobile application program, mobile communication protocol.

C.3.2 Confirmation of tool testing method

Tool testing shall also add mobile terminal security testing, i.e., it shall include reverse analysis test of mobile application program.

C.3.3 Example for confirmation of target of testing and evaluation

Based on D.3, confirmation of target of testing and evaluation of four levels shall also consider the following aspects:

- working environment of wireless access equipment;
- mobile terminal, mobile application software, mobile terminal management system;
- network interconnection equipment that determines security of entire classified target, wireless access device;
- wireless access gateway.

C.4 Supplement to classified testing and evaluation of industrial control system

C.4.1 Overall requirements for classified testing and evaluation of industrial control system

C.4.1.1 Principle of completeness

Modern industrial control system is a complex information physics fusion system. In addition to traditional IT system target, its unique control equipment (such as PLC, operator workstation, DCS controller) needs to be protected carefully because they are directly responsible for process control. Therefore, it needs to focus on completeness of selected target of testing and evaluation during testing and evaluation.

C.4.1.2 Principle of minimum impact

Industrial control system requires real-time response. Longer delay or large fluctuation in response are not allowed. And since industrial control system has strict requirements for availability, responses such as restart are not allowed. It needs to consider possible negative effects of testing and evaluation on normal operation of target system from perspective of project management and technology application, so as to minimize risk and ensure target system business to operation as normal.

Annex D

(Normative)

Principle and example for confirmation of target of testing and evaluation

D.1 Principle for confirmation of target of testing and evaluation

Target of testing and evaluation is direct work target of classified testing and evaluation. It is also specific system component of corresponding security function to realize specific testing and evaluation indicator in classified target under test. Therefore, selection of target of classified testing and evaluation is a necessary step to prepare testing and evaluation scheme. It is also an important link of entire testing and evaluation. Appropriate selection of type and number of target of testing and evaluation is an important assurance to make entire classified testing and evaluation able to obtain sufficient evidence, to understand real security protection situation of classified target under test.

Confirmation of target of testing and evaluation usually uses random inspection method. That is, conduct random inspection of representative component in classified target as target of testing and evaluation. Moreover, in confirmation of target of testing and evaluation, it shall balance work input and outcome output.

When confirming target of testing and evaluation, it shall follow the following principles:

- Importance. Randomly inspect server, database and network device that are important to classified target under test;

- Security. Randomly inspect network boundary exposed outside;

- Sharing. Randomly inspect shared device and data exchange platform/device;

- Comprehensiveness. Random inspection shall try to cover various device type, operating system type, database system type and application system type of system;

- Compliance. Selected device, software system shall be able to meet requirements for testing and evaluation strength at corresponding level.

D.2 Steps for confirmation of targeting of testing and evaluation

When confirming target of testing and evaluation, it can classify system

host operating system types, database system types, and application system types in system.

d) According to testing and evaluation strength that security protection level corresponds of classified target of testing and evaluation, perform suitability analysis. Comprehensively measure testing and evaluation input and outcome output to have a suitable confirmation of type and number of target of testing and evaluation.

D.3 Example for confirmation of target of testing and evaluation

D.3.1 Level-1 classified target

In classified testing and evaluation of level-1 classified target, type and number of target of testing and evaluation are few. Focus on inspection of key equipment, facilities, personnel and files. Type of randomly-inspected target of testing and evaluation mainly considers the following aspects:

- main computer room (including its environment, equipment and facilities). If in some auxiliary computer room, equipment, facilities that serve entire classified target or determine security of classified target are placed, they shall be target of testing and evaluation;

- network topology of entire system;

- security devices, including firewall, intrusion detection device, antivirus gateway;

- boundary network devices (which may include security devices), including router, firewall, and authentication gateway;

- network interconnection equipment that determines security of entire classified target, such as core switch, router;

- core server that bears business or data that best represents mission of classified target under test (including its operating system and database);

- important business application system that best represents mission of classified target under test;

- information security officer;

- main management systems and records involving in security of classified target, including registration records for entry-exit of computer room, relevant design acceptance files for classified target.

In testing and evaluation of this level classified target, it shall at least randomly inspect one security device, boundary network device, network interconnection

D.3.3 Level-3 classified target

In classified testing and evaluation of level-3 classified target, type of target of testing and evaluation basically cover all, randomly sample the number. Focus on inspection of key equipment, facilities, personnel and files. Type of randomly-inspected target of testing and evaluation mainly considers the following aspects:

- main computer room (including its environment, equipment and facilities) and some auxiliary computer rooms. Auxiliary computer room that places equipment and facilities that serve part of classified target (including whole) or determine security of part (including whole) of security of classified target as target of testing and evaluation;

- storage environment that stores medium of important data of classified target under test;

- work place;

- network topology of entire system;

- security devices, including firewall, intrusion detection device, antivirus gateway;

- boundary network devices (which may include security devices), including router, firewall, authentication gateway, and boundary access device (such as floor switch);

- network interconnection equipment that determines security of entire classified target or partial security, such as core switch, aggregation layer switch, core router;

- server that bears main business or data of classified target under test (including its operating system and database);

- management terminal and main business application system terminal;

- business application system capable of fulfilling different business missions of classified target under test;

- business backup system;

- information security supervisors, responsible personnel in all aspects, parties responsible for security management, and business leaders;

- all management systems and records related to security of classified target.

In testing and evaluation of this level classified target, it shall at least randomly

Annex E

(Informative)

Modes and work tasks for on-site testing and evaluation of classified testing and evaluation

E.1 General

When testing and evaluation personnel is conducting on-site testing and evaluation according testing and evaluation guide, it usually has three testing and evaluation modes: interview, inspection and testing.

E.2 Interview

Input: on-site testing and evaluation plan, testing and evaluation guide, record form for testing and evaluation result of technology and management security testing and evaluation.

Task description:

Testing and evaluation personnel communicate, discuss with relevant personnel (individual/group) of classified target under test so as to obtain relevant evidence to know relevant information. About interview scope, classified target at different level has different requirements in testing and evaluation. Usually, it shall basically cover all types of relevant security personnel, sampling on quantity. Refer to requirements of each level in each part of “Information security technology - Testing and evaluation of classified protection of cyber security”.

Output/product: testing and evaluation result record of technology and management security testing and evaluation.

E.3 Inspection

E.3.1 General

Inspection can be refined into three specific methods: file review, field review and configuration inspection.

E.3.2 File review

Input: on-site testing and evaluation plan, security strategy, security policy file, security management system, implementation process file of security management, system design scheme, technical information of network device, instructions on actual configuration of system and product, various operating

management security testing and evaluation.

E.3.3 Field inspection

Input: testing and evaluation guide, record form of technology security and management security testing and evaluation results.

Task description:

According to actual situation of classified target under test, testing and evaluation personnel go to system operating field, through field observation of personnel behavior, technical facilities and physical environment conditions, to judge security situations of personnel's security awareness, business operation, management procedures and system's physical environment, so as to test and evaluate whether they meet security requirements of corresponding level.

Different strength requirements for different level classified target during testing and evaluation are listed as below.

Level 1: meet level-1 requirements in GB/T 22239.

Level 2: meet level-2 requirements in GB/T 22239.

Level 3: meet level-3 requirements in GB/T 22239. Judge whether field observation is consistent with instructions in system and file. Verify validity and position of relevant equipment and facilities, and consistency with system design.

Level 4: meet level-4 requirements in GB/T 22239. Judge whether field observation is consistent with instructions in system and file. Verify validity of relevant equipment and facilities and correctness of position, consistency with system design.

Output/product: record of technology security and management security testing and evaluation results.

E.3.4 Configuration inspection

Input: testing and evaluation guide, record form of technical security testing and evaluation result.

Task description:

a) According to record form content of testing and evaluation result, use on-board verification mode to verify whether application system, host system, database system as well as configuration of each device are correct, whether they are consistent with file, relevant devices and parts. Verify contents of file review (including log audit).

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

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