GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 36959-2018

Information security technology - Capability requirements and evaluation specification for assessment organization of classified protection of cybersecurity

信息安全技术 网络安全等级保护

测评机构能力要求和评估规范

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

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

Table of Contents

Foreword 3

Introduction 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 5

4 Capability requirements of assessment organizations 6

4.1 Classification of assessment organizations 7

4.2 Classification of level evaluation personnel 7

4.3 Capability requirements for level I assessment organizations 7

4.4 Capability requirements for level II assessment organizations 16

4.5 Capability requirements for Level III assessment organizations 27

4.6 Normative requirements for activities of assessment organization 38

5 Evaluation of the capability of assessment organization 39

5.1 Evaluation process 39

5.2 First-time evaluation 41

5.3 Continuous evaluation 43

5.4 Capability review 43

Appendix A (Normative) Summary form of requirements for capability enhancement of assessment organizations of classified protection of cybersecurity at all levels 44

Appendix B (Normative) Capability requirements for classified protection evaluator of cybersecurity 52

Information security technology - Capability requirements and evaluation specification for assessment organization of classified protection of cybersecurity

1 Scope

This standard specifies the capability requirements and evaluation specifications of assessment organizations of classified protection of cybersecurity.

This standard is applicable to activities such as capability building, operation management, qualification evaluation that intend to become or upgrade to a higher level of assessment organization of cybersecurity protection.

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

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

3 Terms and definitions

The terms and definitions as defined in GB/T 28448 as well as the following terms and definitions apply to this document.

3.1

Capability evaluation

According to standards and/or other normative documents, the process of

e) There are no less than 15 technical and managerial personnel with cybersecurity related work experience; no less than 2 full-time penetration testers, with clear job responsibilities and relatively stable personnel;

f) Have a fixed office space, equipped with testing and evaluation tools and experimental environments that meet the needs of the evaluation business;

g) It has complete rules and regulations for security and confidentiality management, project management, quality management, personnel management, file management, training and education;

h) Does not involve business that may affect the fairness of the evaluation results (except for personal use) such as cybersecurity product development, sales, or information system security integration;

i) Other conditions that shall be met.

4.3.2 Organizational management capabilities

4.3.2.1 The manager of the assessment organization shall master the classified protection policy documents and be familiar with relevant standards and specifications.

4.3.2.2 The assessment organization shall organize and set up relevant departments in a certain way; clarify their responsibilities, authorities and mutual relations; ensure the orderly development of various tasks.

4.3.2.3 The assessment organization shall have professional and technical personnel and management personnel competent for the level evaluation work; the proportion of bachelor's degree (including) or above shall not be less than 70%.

4.3.2.4 The assessment organization shall set up positions that meet the needs of the level evaluation work, such as evaluation technicians, evaluation project team leaders, technical supervisors, quality supervisors, security officers, equipment managers, file managers, etc., with clear job responsibilities and stable personnel.

4.3.2.5 The assessment organization shall formulate complete rules and regulations, including but not limited to the following:

a) Project management system

The assessment organization shall formulate a comprehensive evaluation project management system in line with its own characteristics in accordance with GB/T 28449, which shall mainly include the organization

examinations organized by the designated assessment organization and obtain the certificate of level evaluator. Level evaluation personnel need to hold a permit to work.

4.3.3.1.3 Evaluation technicians, evaluation project team leaders, technical supervisors shall obtain primary, intermediate, advanced level evaluator certificates respectively; the number of evaluators shall not be less than 15.

4.3.3.1.4 In addition to the qualifications of level evaluators, evaluators shall participate in various forms of evaluation business and technical training each year. The total training time of evaluators shall not be less than 40 hours per year.

4.3.3.1.5 The assessment organization shall appoint a technical supervisor who is fully responsible for the technical work of level evaluation.

4.3.3.2 Evaluation capability

4.3.3.2.1 The assessment organization shall prove that it has more than 2 years of work experience in cybersecurity-related work by providing case, process records and other materials.

4.3.3.2.2 The assessment organization shall ensure that it is engaged in evaluation work within its capabilities and has sufficient resources to meet the requirements of the evaluation work, which is specifically reflected in the following aspects:

a) Security technology evaluation and implementation capabilities, including the development, use, maintenance and professional judgment of obtaining relevant results in terms of physical and environmental security, network and communication security, equipment and computing security, application and data security, etc.;

b) Security management evaluation and implementation capabilities, including security strategy and management system, security management organization and personnel, security construction management, security operation and maintenance management, development, use, maintenance and professional judgment of obtaining relevant results;

c) Security testing and analysis capabilities, which refer to the capability to develop test-related work instructions based on actual evaluation requirements, use special evaluation equipment and tools to realize vulnerability discovery and problem analysis;

d) The overall evaluation implementation capability, which refers to the capability to give specific results of the overall evaluation based on the

form the evaluation report. The evaluation report shall be compiled according to the format and content requirements of the evaluation report template of classified protection of cybersecurity as uniformly formulated by the public security administrative department. The evaluation report shall pass the review and have relevant records.

4.3.4 Security and assurance capabilities of facilities and equipment

4.3.4.1 The assessment organization shall have the necessary office environment, equipment, facilities and management system. The technical equipment and facilities used shall in principle meet the following conditions:

a) The product development and production organization is invested by a Chinese citizen, legal person, or invested or controlled by the state, has an independent legal personality within the territory of the People's Republic of China;

b) The core technology and key components of the product have our country's independent intellectual property rights;

c) The product development and production organizations and their main businesses and technical personnel have no criminal records;

d) The product development and production organizations declare that they have not intentionally left or set loopholes, backdoors, Trojan horses and other programs and functions;

e) No harm to national security, social order, or public interest;

f) It shall be equipped with critical network equipment and special cybersecurity products that have passed security certification or meet the requirements of security testing.

4.3.4.2 The assessment organization shall be equipped with evaluation equipment and tools that meet the requirements of the level evaluation work, such as WEB security detection tools, malicious behavior detection tools, etc., to assist in the discovery of security issues during the testing process. Testing equipment and tools shall pass the testing of authoritative organizations and provide testing reports.

4.3.4.3 The assessment organization shall have a computer room that meets the relevant requirements and the necessary software and hardware equipment to meet the needs of cybersecurity simulation, technical training and simulation testing.

4.3.4.4 The assessment organization shall ensure that the evaluation equipment and tools are in good operating condition; ensure that it provides

4.3.6.2.2 The assessment organization shall prove that its organization is in compliance, the property rights relationship is clear, the capital registration meets the requirements (5 million yuan), by providing documents such as the nature of the organization, shareholding structure, capital contribution, legal person and shareholder identity.

4.3.6.2.3 The assessment organization shall establish and maintain personnel files of staff, including basic personnel information, social background, work experience, training records, professional qualifications, rewards and punishments, etc., to ensure the stability and reliability of personnel.

4.3.6.2.4 The test equipment and tools used by the assessment organization shall have a comprehensive function list; there shall be no hidden functions outside the function list.

4.3.6.2.5 The assessment organization shall attach importance to security and confidentiality work; designate persons responsible for security and confidentiality work.

4.3.6.2.6 The assessment organization shall regularly educate its staff on confidentiality in accordance with the confidentiality management system. The assessment organization and evaluation personnel shall keep the state secrets, work secrets, business secrets, personal privacy, etc., that they learn during the evaluation activities.

4.3.6.2.7 The assessment organization shall clarify the requirements of job confidentiality; sign a "Confidentiality Responsibility Letter" with all personnel; stipulate the security and confidentiality obligations and legal responsibilities it shall perform; be responsible for inspection and implementation.

4.3.6.2.8 The assessment organization shall take technical and management measures to ensure the security, confidentiality and control of information related to the level evaluation, including but not limited to:

a) Information provided by the organization under evaluation;

b) Data and records generated by the level evaluation activities;

c) Analysis and professional judgment based on the above information.

4.3.6.2.9 The assessment organization shall use effective technical means to ensure the security and confidentiality of the level evaluation related information during the entire data life cycle.

4.3.6.3 Standardization of evaluation methods and procedures

The assessment organization shall ensure that all working procedures,

or insufficient resources;

b) The risk that test verification activities may affect the normal operation of the system under test;

c) The risk that the access of test equipment and tools may affect the normal operation of the system under test;

d) The risk of leakage of important information of the system under test (such as network topology, IP address, business process, security mechanism, security risks and related documents, etc.) that may occur during the evaluation process.

4.3.7.2 The assessment organization shall adopt a variety of measures to avoid and control the risks that the aforementioned system under test may face.

4.3.8 Sustainability

4.3.8.1 The assessment organization shall formulate a strategic plan according to its own situation; ensure the continuous construction and development of the assessment organization through continuous investment.

4.3.8.2 The assessment organization shall periodically review and continuously improve the management system; continuously improve management requirements. Set mid-term and long-term goals; gradually improve quality management capabilities through the realization of goals.

4.3.8.3 The assessment organization shall do a good job of training in accordance with the training system and keep training and evaluation records.

4.3.8.4 The assessment organization shall devote special forces to the summary of evaluation practice and the research of evaluation technology. The assessment organizations shall conduct experience exchanges and technical discussions, to keep pace with the development of evaluation technology.

4.4 Capability requirements for level II assessment organizations

4.4.1 Basic conditions

The assessment organization shall have the following basic conditions:

a) Enterprises and organizations registered and established within the territory of the People's Republic of China, invested by Chinese citizens, legal persons, or invested by the state;

equipment administrators, file administrators, etc., with clear job responsibilities and stable personnel. Among them, technical supervisors and quality supervisors shall be full-time personnel, not concurrently.

4.4.2.5 The assessment organization shall formulate complete rules and regulations, including but not limited to the following:

a) Confidentiality management system

The confidentiality management system shall be formulated in accordance with the relevant national confidentiality regulations. The system shall specify the scope of confidentiality objects, personnel confidentiality responsibilities, various measures and requirements for confidentiality management during the evaluation process, penalties for violations of the confidentiality system.

b) Project management system

The assessment organization shall formulate a comprehensive evaluation project management system in line with its own characteristics in accordance with GB/T 28449, which shall mainly include the organization of the evaluation work, job responsibilities, the work content and management requirements of each stage of the evaluation.

c) Equipment management system

It shall include the relevant responsibilities of organizational personnel in the management of equipment, various regulations on the purchase, use, operation and maintenance of instrument and equipment.

d) Document management system

It shall include the relevant responsibilities of the staff of the organization in the management of the evaluation documents, the provisions on the borrowing and reading of files, the storage and the destruction, etc.

e) Personnel management system

It shall include the content and requirements of personnel recruitment, evaluation, daily management, resignation.

f) Training and education system

It shall include the content and requirements of the formulation of training plans, the implementation of training, the evaluation and induction of training, the establishment of personnel training files.

g) Appeal, complaint and dispute handling system

following aspects:

a) Security technology evaluation implementation capabilities, including the development, use, maintenance and professional judgment of obtaining relevant results in terms of physical and environmental security, network and communication security, equipment and computing security, application and data security, etc. The evaluation guide shall cover the current mainstream products and related technologies;

b) Security management evaluation and implementation capabilities, including security strategy and management system, security management organization and personnel, security construction management, security operation and maintenance management and other aspects of the development, use, maintenance and professional judgment of obtaining relevant results;

c) Security testing and analysis capabilities, which refer to the development of test-related work instructions based on actual evaluation requirements; the capability to realize vulnerability discovery and problem analysis with the help of special evaluation equipment and tools; having the cryptanalysis evaluation capabilities;

d) The overall evaluation implementation capability, which refers to the capability to give specific results of the overall evaluation based on the result recording part, the result summary part and the problem analysis part of the evaluation report's unit evaluation, from the perspective of security control points and between levels and regions;

e) Risk analysis capability, which refers to the capability to establish a set of unified risk analysis methods based on the relevant norms and standards of classified protection, analyze the impact of the security issues in the level evaluation results that may have on the security of the system under evaluation in a scientific and reasonable manner.

4.4.3.2.3 The assessment organization shall strengthen the application of information technology in the implementation of evaluation; with the help of automated means, standardize the evaluation process; optimize the allocation of resources; reduce errors that may be caused by human factors; improve the efficiency of evaluation work.

4.4.3.2.4 The assessment organization shall establish a complete mechanism for the development, maintenance and update of evaluation methods to continuously improve its own evaluation technical capabilities.

4.4.3.2.5 The assessment organization shall combine the industry characteristics and business types of the system under test; analyze the

4.4.4.1 The assessment organization shall have the necessary office environment, equipment, facilities and management system; the technical equipment and facilities used shall in principle meet the following conditions:

a) The product development and production organization is invested by a Chinese citizen, legal person, or invested or controlled by the state, meanwhile has an independent legal personality within the territory of the People's Republic of China;

b) The core technology and key components of the product have our country's independent intellectual property rights;

c) The product development and production organization and their main businesses and technical personnel have no criminal records;

d) The product development and production organizations declare that they have not intentionally left or set loopholes, backdoors, Trojan horses and other programs and functions;

e) No harm to national security, social order, or public interest;

f) It shall be equipped with critical network equipment and special cybersecurity products that have passed security certification or meet the requirements of security testing.

4.4.4.2 The assessment organization shall be equipped with evaluation equipment and tools that meet the requirements of the level evaluation work, such as WEB security detection tools, malicious behavior detection tools, network protocol analysis tools, source code security audit tools, etc., to assist in analyzing and positioning security problem during the testing process. Testing equipment and tools shall pass the testing of authoritative organizations and provide testing reports.

4.4.4.3 The assessment organization shall have a computer room that meets the relevant requirements and the necessary software and hardware equipment; it shall establish a basic environment composed of mainstream network equipment, security equipment, operating systems and database systems, to meet the needs of network simulation, technical training and simulation testing.

4.4.4.4 The assessment organization shall ensure that the evaluation equipment and tools are in good operating condition; ensure that they provide accurate evaluation data through continuous updating and upgrading.

4.4.4.5 The testing equipment and tools shall be properly marked.

4.4.4.6 The assessment organization shall establish a special system, to effectively operate and maintain the computer used for evaluation data

strictly implement relevant management norms and technical standards; develop objective, fair and safe evaluation services.

4.4.6.1.2 The personnel of the assessment organization shall be free from commercial, financial and other pressures that may affect the evaluation results.

4.4.6.1.3 The assessment organization shall publicly announce to the public the policies, regulations, standards and norms on which it conducts the evaluation of cybersecurity's classified protection.

4.4.6.2 Reliability and confidentiality assurance capability

4.4.6.2.1 The legal persons and main staff of the assessment organization are limited to Chinese citizens within the territory of the People's Republic of China; they have no criminal record.

4.4.6.2.2 The assessment organization shall prove that its organization is compliant, the property rights relationship is clear, the capital registration meets the requirements, by providing documents such as the nature of the organization, shareholding structure, capital contribution, legal person, shareholder identity.

4.4.6.2.3 The assessment organization shall establish and maintain personnel files of staff, including basic personnel information, social background, work experience, training records, professional qualifications, rewards and punishments, etc., to ensure the stability and reliability of personnel.

4.4.6.2.4 The test equipment and tools used by the assessment organization shall have a comprehensive function list; there shall be no hidden functions outside the function list.

4.4.6.2.5 The assessment organization shall attach importance to security and confidentiality work; assign persons responsible for security and confidentiality work.

4.4.6.2.6 The assessment organization shall regularly educate the staff on confidentiality in accordance with the confidentiality management system; the assessment organization and evaluation personnel shall keep the state secrets, work secrets, business secrets, personal privacy that they know about in the evaluation activities.

4.4.6.2.7 The assessment organization shall clarify the requirements for job confidentiality; sign a "Confidentiality Responsibility Letter" with all personnel; stipulate its security and confidentiality obligations and legal responsibilities; be responsible for inspection and implementation.

4.4.6.2.8 The assessment organization shall adopt technical and management

a) The assessment organization shall issue an evaluation report in accordance with the template format of evaluation report of classified protection of cybersecurity as uniformly formulated by the public security administrative department.

b) The evaluation report shall include all evaluation results, professional judgments based on these results, all information needed to understand and interpret these results. The above information shall be correctly, accurately and clearly stated.

c) The evaluation report shall be reviewed by the evaluation project team leader as the first editor; the technical director (or quality director) shall be responsible for review; the organization manager or its authorized personnel shall issue or approve it.

d) The assessment organization that has passed the capability evaluation shall uniformly stamp the special identification on qualified capability of the assessment organization, register, archive the level evaluation report issued by it.

4.4.6.6 Security management capabilities

Assessment organizations shall pay attention to their own security and improve security management capabilities by deploying security measures.

4.4.7 Risk control capability

4.4.7.1 The assessment organization shall fully estimate the risks that the evaluation may bring to the system under test. The risks include but are not limited to the following:

a) The risk caused by the assessment organization due to its own capability or insufficient resources;

b) The risk that test verification activities may affect the normal operation of the system under test;

c) The risk that the access of test equipment and tools may affect the normal operation of the system under test;

d) The risk of leakage of important information of the system under test (such as network topology, IP address, business process, security mechanism, security risks and related documents, etc.) that may occur during the evaluation process.

4.4.7.2 The assessment organization shall adopt a variety of measures to avoid and control the risks that the aforementioned system under test may face.

China and have no criminal record;

e) There are no less than 50 technical and managerial personnel with cybersecurity related work experience; no less than 5 full-time penetration testers, with clear job responsibilities and relatively stable personnel;

f) Have a fixed office space, equipped with testing and evaluation tools and experimental environments that meet the needs of the evaluation business;

g) It has complete rules and regulations for security and confidentiality management, project management, quality management, personnel management, file management, training and education;

h) Does not involve business that may affect the fairness of the evaluation results (except for personal use) such as cybersecurity product development, sales, or information system security integration;

i) Other conditions that shall be met.

4.5.2 Organizational management capabilities

4.5.2.1 The manager of the assessment organization shall master the classified protection policy documents and be familiar with relevant standards and specifications.

4.5.2.2 The assessment organization shall clearly establish the department to carry out the level evaluation business, to ensure the independence of the evaluation activity.

4.5.2.3 The assessment organization shall have professional and technical personnel and management personnel competent for the level evaluation work; the proportion of bachelor's degree (including) or above shall not be less than 90%.

4.5.2.4 The assessment organization shall set up positions that meet the needs of the level evaluation work, such as evaluation technicians, evaluation project team leaders, technical supervisors, quality supervisors, confidential security officers, equipment administrators, file administrators. The above-mentioned positions shall be full-time personnel, which cannot be served concurrently.

4.5.2.5 The assessment organization shall formulate complete rules and regulations, including but not limited to the following:

a) Confidentiality management system

The confidentiality management system shall be formulated in

4.5.3.1 Personnel capability

4.5.3.1.1 The professional and technical personnel (hereinafter referred to as the evaluation personnel) of the assessment organization engaged in the level evaluation work shall have the knowledge and capability to grasp the national policies; understand and master the relevant technical standards; be familiar with the level evaluation methods, procedures and work specifications; have the capability to make professional judgments based on the evaluation results and issue level evaluation reports.

4.5.3.1.2 The evaluation personnel shall participate in the special training and examinations organized by the designated assessment organization and obtain the certificate of the level evaluator. Level evaluation personnel need to hold a permit to work.

4.5.3.1.3 Evaluation technicians, evaluation project team leaders, technical supervisors shall obtain primary, intermediate, advanced level evaluation certificates respectively; the number of evaluation engineers shall not be less than 50.

4.5.3.1.4 In addition to having the qualifications of level evaluators, evaluators shall participate in various forms of evaluation business and technical training each year. The total training time of evaluators shall not be less than 60 hours per year.

4.5.3.1.5 The assessment organization shall appoint a technical supervisor who is fully responsible for the technical work of level evaluation. The technical director of the assessment organization shall have a bachelor's degree or above; shall publish 5 or more papers (or apply for 1 patent copyright) in the information security professional journals in the past 3 years; preside over 1 national (or ministerial) level scientific research projects.

4.5.3.2 Evaluation capability

4.5.3.2.1 The assessment organization shall have the capability to implement not less than 80 third level (inclusive) classified protection objects which are subject to level evaluation every year.

4.5.3.2.2 The assessment organization shall ensure that it is engaged in evaluation work within its capability and has sufficient resources to meet the requirements of the evaluation work, which is specifically reflected in the following aspects:

a) Security technology evaluation implementation capabilities, including the development, use, maintenance and professional judgment of obtaining relevant results in terms of physical and environmental security, network and communication security, equipment and computing security,

specific requirements are as follows:

a) In the evaluation preparation stage, collect relevant information about the system under test; fill in a standardized system questionnaire; fully grasp the details of the system under evaluation; lay a foundation for the development of the evaluation work;

b) At the stage of plan preparation, correctly and reasonably determine the evaluation object, evaluation index and evaluation content, etc.; develop the evaluation plan, evaluation guide, evaluation result record form, etc. in accordance with the current effective technical standards and norms. The evaluation plan shall pass the technical review and have relevant records. The evaluation guide shall be maintained for the validity of the version and meet the following requirements:

1) Conform to relevant level evaluation standards;

2) Provide sufficient detailed information to ensure the standardization and operability of the evaluation data acquisition process.

c) During the on-site evaluation stage, strictly implement the content and requirements in the evaluation plan and evaluation guide; use the evaluation equipment and tools proficiently in accordance with the operating procedures; fill in the evaluation result records in a standardized, accurate and complete manner; obtain sufficient evidence; objectively, true, scientifically reflect the security protection status of the system. The evaluation process shall be monitored and recorded;

d) During the preparation of the report, objectively describe the effective protection measures taken by the classified protection object and the main security problems that exist; point out the gap between the current security protection of the classified protection object and the protection requirements of the corresponding level; analyze the risk that the evaluated system may face due to the gap; give the level evaluation conclusion and form the evaluation report. The evaluation report shall be compiled according to the format and content requirements of the template of evaluation report of classified protection of cybersecurity as uniformly formulated by the public security administrative department. The evaluation report shall pass the review and have relevant records.

4.5.4 Facilities and equipment security and assurance capabilities

4.5.4.1 The assessment organization shall have a complete office environment, equipment, facilities and management system; the technical equipment and facilities used shall in principle meet the following conditions:

a) The product development and production organization is invested by a

4.5.5.1 Management system construction

4.5.5.1.1 The assessment organization shall establish, implement and maintain a documented management system that meets the requirements of the level evaluation work; ensure that the personnel at all levels of the assessment organization can understand and implement it. If necessary, it can apply for the qualification of management system certification in related fields.

4.5.5.1.2 The assessment organization shall formulate corresponding quality objectives and continuously improve its evaluation quality and management level.

4.5.5.1.3 The assessment organization shall appoint a quality supervisor, to clarify the responsibilities of quality assurance. The quality supervisor shall not be affected by the influence that may damage the quality of the work; has the right to communicate directly with the top management of the assessment organization.

4.5.5.2 Management system maintenance

4.5.5.2.1 The assessment organization shall ensure the effective operation of the management system; promptly respond to problems found and take corrective measures to ensure its effectiveness.

4.5.5.2.2 The assessment organization shall strictly abide by the appeal, complaint and dispute handling system; record the measures taken.

4.5.5.2.3 The assessment organization shall establish and implement a review and feedback processing mechanism of the internal management system, to verify the compliance and effectiveness of the management system; ensure that the problems found during the operation of the management system are resolved in a timely manner. The person performing the audit shall be independent of the department being audited.

4.5.5.3 Quality supervision capability

The assessment organization shall appoint a supervisor to supervise all evaluation technicians. The supervision content includes on-site evaluation activities, the standardization of the evaluation process, the accuracy of evaluation conclusions.

4.5.6 Normative assurance capability

4.5.6.1 Capability to ensure fairness

4.5.6.1.1 The assessment organization and its evaluation personnel shall strictly implement relevant management norms and technical standards;

related to the level evaluation, including but not limited to:

a) Information provided by the tested organization;

b) Data and records generated by the level evaluation activities;

c) Analysis and professional judgment based on the above information.

4.5.6.2.9 The assessment organization shall use effective technical means to ensure the security and confidentiality of the entire data life cycle of the level evaluation related information.

4.5.6.2.10 The assessment organization shall establish a special document storage place and data encryption environment; strictly manage the data information related to the evaluation.

4.5.6.3 Standardization of evaluation methods and procedures

4.5.6.3.1 The assessment organization shall formulate procedures, to ensure that all working procedures, instructions, standards, work forms, verification records related to the level evaluation work are currently valid and easy to obtain by the evaluation personnel.

4.5.6.3.2 The release and implementation of the above-mentioned documents shall be subject to a unified approval procedure; the changes and revisions of the documents shall be authorized, and the versions shall be maintained in a timely manner.

4.5.6.4 Standardization of evaluation records

The assessment organization shall ensure the standardization of the content and management of evaluation records:

a) The evaluation record shall be clear and standardized; obtain written confirmation from the evaluated party.

b) The transfer, reproduction, transmission of all data recorded or generated by computers shall be checked, to ensure its accuracy and completeness.

c) The assessment organization shall have the capability to securely keep records; all evaluation records shall be kept for more than 3 years.

4.5.6.5 Standardization of evaluation report

The assessment organization shall ensure the standardization of the content of the evaluation report and the issuance process management:

a) The assessment organization shall issue an evaluation report in

and control the risks that the aforementioned system under test may face.

4.5.8 Sustainability

4.5.8.1 The assessment organization shall formulate a strategic plan according to its own situation; ensure the continuous construction and development of the assessment organization through continuous investment.

4.5.8.2 The assessment organization shall periodically review and continuously improve the management system, to continuously improve management requirements. Set mid-term and long-term goals (such as obtaining the certification qualification of corresponding management system); gradually improve the quality management capability through the realization of the goals.

4.5.8.3 The assessment organization shall implement a complete training system, to ensure that its personnel continue to meet the needs of the level evaluation work in terms of professional technology and management. In addition to regular training, a detailed and targeted training plan shall be formulated according to the job requirements of the personnel; it shall carry out job training, appraisal and evaluation.

4.5.8.4 The assessment organization shall track the development of new technologies and new applications at home and abroad; ensure that technical capabilities are synchronized with current technological development through special subject research and practice.

4.6 Normative requirements for activities of assessment organization

The assessment organization shall not engage in the following activities:

a) Affect the normal operation of the classified protection objects under the evaluation; endanger the security of the classified protection objects under the evaluation;

b) Divulge the state secrets and work secrets of the evaluated organization and the evaluated classified protection object;

c) Deliberately conceal the security issues discovered during the evaluation process; or resort to fraud during the evaluation process; fail to truthfully issue a level evaluation report;

d) Failure to issue a level evaluation report in the prescribed format;

e) Unauthorized possession and use of level evaluation related materials and

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

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