GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 20269-2006

Information security technology - Information system security management requirements

信息安全技术　信息系统安全管理要求

Issued on May 31, 2006 **Implemented on December 01, 2006**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology –

Information System Security Management Requirements

1 Scope

This Standard specifies management requirements of security levels required for information system security based on the division of security levels required by information system security.

This Standard applies to information system security management based on graded requirements.

2 Normative references

The articles contained in the following documents have become part of this document when they are quoted herein. For the dated documents so quoted, all subsequent modifications (excluding corrigendum) or revisions made thereafter do not apply to this Standard. However, the parties who reach an agreement according to this Standard are encouraged to study whether the latest versions of these documents may be used. For the undated documents so quoted, the latest versions (including all modification sheets) apply to this document.

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

GB/T 20271-2006 Information security technology - Common security techniques requirement for information system

3 Terms and definitions

The following terms AND the definitions defined in GB 17859-1999 apply to this Standard.

3.1

Integrity

It includes data security and system security. Data security represents all the characteristics of data, i.e. accuracy and consistency of data remain unchanged regardless of any changes of data; system integrity represents the quality that system can fulfill the operation purposes under the circumstance of preventing unauthorized users from modifying or using resources and prevention authorized users from incorrectly modifying or using resources.

3.2

shall universally participate in information system security management and cooperate with and coordinate relevant parties to jointly ensure the security of information system.

d) The responsible-person of system approach: Identify and understand correlative levels and processes of information security assurance based on the requirements of information security assurance and adopt management and technology combination method to improve the effectiveness and efficiency of achieving security assurance objectives.

e) Principle of continuous improvement: Security management is a dynamic feedback process throughout the life cycle of whole security management. With the changing of spatial and temporal distribution of security requirements and system vulnerability, increasing of extent of threat, changing of system environment and the deepening of system security awareness, etc., there is a need to timely review, modify and adjust existing security policy, risk acceptance level and protective measures or even improve security management level to maintain and improve the effectiveness of information security management system.

f) Principle of management by law: Information security management work is mainly reflected in management behaviors. It shall be ensured legal information system security management main body, legal management behaviors, legal management contents and legal management procedures. For security even handling, authorizer shall timely issue accurate and consistent relevant information to avoid adverse impact on society.

g) Principle of decentralization and authority: Separate specific functions or management functions in responsibility fields and decentralize independent audit, etc. to avoid hidden dangers caused by excessive concentration of power and reduce unauthorized changes or the changes of misusing system resources. Any entity (e.g. users, administrators, applications, processes, application or system) is only entitled to required permissions to fulfill the tasks and shall not be entitled to any extra permission.

h) Principle of using mature technology: Mature technology has good reliability and stability; attention shall be paid to the maturity of new technology to be adopted, and there shall be local pilot before gradual popularization in order to reduce or avoid faults that may arise.

i) Responsible-person of graded protection: Determine security protection level of information system based on classification standard and perform graded protection; for large-scale information system that is composed of several subsystems, determine basic security protection levels of system and respectively determine security protection level of subsystems based on actual security requirements to implement multi-level security protection.

b) Complete security management policy: On the basis of a), information security management policy also include: autonomously protect in accordance with national policy and regulations and technical and management standards under the guidance of information system security monitoring department; clearly define the security protection level (graded protection based on region) of information system (subsystem/domain); develop complete information security policy including risk management policy, business continuity policy, security training and education policy, audit policy, etc.

c) Systematic security management policy: On the base of b), security management policy also include: autonomously protect in accordance with national policy and regulations and technical and management standards under the premise of receiving supervision and inspection from information system security monitoring department; developing objective policy, planning policy, organization policy, personnel policy, management policy, security technology policy, control policy, life cycle policy, investment policy, quality policy, etc., forming a systematic information system security policy;

d) Mandatory protection security management policy: On the basis of c), information security management policy also includes: autonomously protect in accordance with national policy and regulations and technical and management standards under the premise of receiving supervision and inspection from information system security monitoring department; developing complete information system security management policy.

e) Exclusive security control security management policy: On the basis of d), autonomously protect in accordance with national policy and regulations and technical and management standards under the premise of receiving special supervision from designated special national department or special agency; developing information system that may be sustainably improved.

5.1.1.3 Development of security management policy

For development of information system security management policy, different security levels shall selectively meet one of following requirements:

a) Development of basic security management policy: Developed by security management personnel, convened by the responsible-person in charge of information security work, based on security management personnel who develop information system security management policy together with relevant personnel, including overall policy and specific policy, which is presented in document.

b) Development of complete security management policy: Developed information security functional department, organized by responsible-person who is in charge of information security work. Information security functional department is responsible for developing complete information system security management policy, including

approval management, third-party access control and relevant operation specification, etc.

d) Mandatory protection security management system: On the basis of c), increase information privacy identification management regulations, password use management regulations, regulations on security event routine assessment and report, regulations on regular assessment of key control measures, etc.;

e) Exclusive control security management system: On the basis of d), increase security management audit supervision regulation, etc.

5.1.2.2 Development of security management rules and regulations

Development and release of security management system shall have clearly defined procedures; different security levels shall selectively meet one of following requirements:

a) Development of basic security management system: Security management personnel shall be responsible for developing information system security management system, whish is stated in the form of document and approved to release by responsible-person in charge of information security work;

b) Development of complete security management system: Information security functional department is responsible for developing information system security management system, which is stated in the form of document and approved to release by responsible-person in charge of information security work and released in accordance with document management procedures;

c) Development of systematic security management system: Information security functional department is responsible for developing information system security management system, which is stated in the form of document and approved to release by responsible-person in charge of information security work and released in accordance with document management procedures; release scope shall be indicated and there shall be receiving and dispatching registration;

d) Development of mandatory protection security management system: Information security functional department specially assigns a person who is responsible for developing information system security management system, which is stated in the form of document and discussed by information security leading group and approved to release by the responsible-person of information security leading group; information system security management system document released shall give clear indication of security classification; development of secret-associated information system security management system shall be in an corresponding range;

e) Development of exclusive control security management system: On the basis of d), seek the opinions of confidentiality department management of organization or

c) Establishing security leading group: On the basis of b), establish information system security management committee or information system security leading group (hereinafter referred to as information security leading group) in the management; for organizations that cover the whole country or are trans-regional, establish various levels of information security leading group in headquarters and subordinate units; one or more full-time security managers at basic level shall be responsible for information system security work;

d) Main responsible-persons to serve as leaders: On the basis of c), main responsible-person of organization shall take the post of information system security leading group responsible-person;

e) Establishing information security confidentiality management department: On the basis of d), establish functional department of information system security confidentiality supervision management or define information security confidentiality management responsibility of original confidentiality department; strengthen confidentiality supervision management for important process of information system security management.

5.2.1.2 Information security leading group

Information system security leading group is responsible for information system security work of the organization; exercise at least one of following management functions:

a) Security management leading function: Based on national and industry policy, laws and regulations on information security, approve the security policy and development planning of information system of organization; determine the duties of relevant department in information system security work and lead the implementation of security work; supervise the implementation of security measures and make decisions on treatment of important security event; supervise and inspect the work of information system security functional department and emergency treatment group; establish and improve secure organization system of information system under centralized control and management and management mechanism.

b) Management functions of confidentiality supervision: On the basis of a), provide confidentiality management department guidance and inspection on relevant information system security and confidentiality supervision management.

5.2.1.3 Information security functional department

Information security functional department is responsible for specific work of information system security of the organization under the guidance of information system security leading group and shall exercise at least one of following management functions:

a) Basic security management functions: In accordance with national and industry laws and regulations on information security, draft security policy and development

shall be aware of the sensitivity of information and the importance of information security, get to know the own responsibilities and that security violations will be subject to disciplinary punishment as well as information security basic knowledge and skills that shall be mastered, etc.;

b) Planned training: On the basis of a), develop and implement security education and training plan; cultivate the security awareness of various personnel of information system and provide cognition awareness and training on security policy and operation specification, etc.;

c) Training for different posts: On the basis of b), develop different professional training plans for different posts, including security knowledge, security technology, security standard, security requirements, legal responsibilities and business control measures, etc.;

d) Training based on personnel qualification requirements: On the basis of c), carry out regular inspection and assessment for the security qualifications of all staffs so that corresponding security education becomes one part of work plan of organization;

e) Cultivating security consciousness: On the basis of d), carry out corresponding security qualification management for all staffs and make security awareness become the self-awareness of all staffs.

5.2.4.2 Information security experts

Information security experts may be invited or employed; different levels of security shall selectively meet one of following requirements:

a) Listen to the suggestions of information security expert: Listen to the suggestions of information security experts on information system security of organization; organize experts to participate in assessment of security threats; provide suggestions on security control measures; judge the effectiveness of information security effectiveness and provide professional guidance and causal investigation on security event, etc.

b) Management for information security experts: On the basis of a), necessary internal information of organization may be provided to invited or employed information security expert; notify these experts of sensibility and confidentiality of such information and take necessary security measures to ensure that the information provided is in a secure and controllable range.

5.3 Risk management

5.3.1 Risk management requirements and policy

5.3.1.1 Risk management requirements

a) Vulnerability scanning tool: Gain awareness of system vulnerability through scanner and other tools, including scanning vulnerability of network equipment, host equipment and security equipment and preparing list of vulnerabilities as the basis of system strengthening and improvement and security project construction; list of vulnerabilities and check list of vulnerabilities may be prepared against asset portfolio and asset classification.

b) Vulnerability analysis and penetration: On the basis of a), manual analysis of vulnerability shall at least involve network equipment, security equipment and host system configuration inspection, user management inspection, system log and audit inspection, etc.; penetration test shall be carried out through respectively selecting different access points from inside or outside network of organization as needed; understand potential consequences of test and make full preparation; for different assets and asset portfolio, comprehensively apply manual assessment, tool scanning, penetration test and other methods to analyze and assess system vulnerability; comprehensively analyze the results obtained through different methods and tools to obtain the vulnerability level.

c) Institutionalized vulnerability assessment: On the basis of b), adhere to institutionalized vulnerability assessment; clearly define vulnerability assessment time and system scope, personnel and responsibilities, assessment results analysis and reporting procedures as well as reported newly discovered loopholes, patched loopholes, loophole trend analysis, etc.

5.3.2.4 Risk analysis and assessment requirements

For risk analysis and assessment, different levels of security shall selectively meet one of following requirements:

a) Risk assessment based on experience: Users and some experts judge risks by experience and assess the risks to form a risk assessment report, which must include risk level, risk points, etc. and determine security risk status of information system.

b) Comprehensive risk assessment: On the basis of a), users and experts carry out qualitative comprehensive assessment for asset, threat, vulnerability, etc. through multi-level multi-angle systematic analysis method to propose risk treatment and mitigation measures and form a risk assessment report. Besides risk status, procedures of risk assessment shall generate information system characteristics report, threat assessment report, vulnerability assessment report, security measures analysis report, etc.; assessor shall offer suggestions on security measures based on these reports.

c) Establishing and maintaining risk information database: On the basis of b), integrate information assets, threats, vulnerabilities, protective measures and other assessment information into a database for management; organization shall

policy of “necessary for knowing, necessary for use, necessary for share, necessary for disclosure, necessary for interconnection communication”.

c) Asset system architecture: On the basis of b), center on business application and describe information asset through the method of system structure; asset system architecture is not simply a list of assets but a structural description on organic connection and relations between various assets.

5.4.2.3 Media management

For media management, different security levels shall selectively meet one of following requirements:

a) Basic requirements of media management: Control and protect various media (including the media of information asset and software asset) in offline storage to prevent theft, destruction, revision or illegal leakage of information; there shall be records on media filling and inquiry; make periodic inventory of catalogue list of filed media; media shall be stored in a secure environment to avoid damage; avoid illegal leakage of information for the media required to be repaired or destructed by others; refer to relevant requirements in 5.1.3.2 for the storage of various media.

b) Requirements for off-sire storage of media: On the basis of a), carry out media identification and classification in accordance with the importance degree of carried data and software and store in media storehouse managed by specially-assigned person to prevent theft, destruction or illegal leakage of information; for the media of information that have high storage confidentiality requirements, the borrowing, approval and transmission shall be approved by leaders of corresponding level and registered; destruction of storage media must be approved and follow a specified mode; arbitrary destruction is not allowed; at least 2 copies of media shall be kept and media shall be stored offsite; environment requirements and management method in storage place is the same with local storage.

c) Integrity inspection requirements: On the basis of b), media and software of important data may be encrypted for storage; the borrowing, copy, distribution and transmission of important information media shall be approved by leaders of corresponding level beforehand; various disposal processes shall be registered; media distribution and transmission shall have protective measures; for media required to be repaired or destructed by others, first delete the information, and then repeat the write operation to cover to prevent data recovery and information leakage; for media to be taken away from working environment, the information shall be protected; media in media storehouse shall regularly receive integrity and availability inspection to make ensure that the data or software is not damaged or lost.

d) Encryption storage requirements: On the basis of c), for important data in media, it is necessary to use encryption technique or data hiding technique for storage; media

d) Security audit of change control: on the basis of c), the security audit of change control shall also include: the approval procedure and operation procedure for the change of system shall be established to prevent the casual change or opening of dangerous port or service; for the important change control, the independent security audit shall be implemented; an overall inspection and assessment for the consistency of security matters shall be conducted; the log records and important equipment records shall be properly stored.

e) Security assessment of change: on the basis of d), the security audit of change control shall also include: the security assessment targeted to all the changes and reuse of equipment; measures taken to ensure the change scheme and effect are perfected continuously.

5.5.2.7 Information exchange management

For the management of information exchange, one of the following items shall be satisfied according to the security level.

a) Basic management of information exchange: the information published in the information system shall conform to the relevant national regulations. The security measures shall be taken to protect the completeness of the published information. The exchange security of information in business application shall be protected to prevent fraud, contract dispute, disclosure or modification of information.

b) Standardized management of information exchange: on the basis of a), the security agreement on the information exchange between organizational institutions shall be established. The management responsibilities and the minimum security requirements on data transmission shall be clarified according to the sensitivity of business information.

c) Management of information transmission between different security regions: on the basis of b), the information transmission between different security regions within the information system shall be included. The security requirements shall be clarified.

d) Management of security information transmission from higher leveled to lower leveled security region: on the basis of c), the approval of the leader of organizational institution shall be obtained to transmit the security information from higher leveled to lower leveled security region. The responsibilities of the relevant department and staff shall be clarified. The special security control measures shall be taken.

5.5.3 Operation maintenance management

5.5.3.1 Daily operation security management

c) Risk assessment for the visit of external service provider: on the basis of b), risk analysis and assessment shall be conducted for the visit of external service provider; the visit of external service provider shall be strictly controlled; the visit of external service provider shall be monitored.

d) Enhanced management to the visit of external service provider: on the basis of c), risk control shall be conducted to each visit of external service provider to the important security area. The visit of external service provider shall be restricted if necessary.

5.5.4 Outsourced service management

5.5.4.1 Outsourced service contract

a) Basic requirements of outsourced service contract: for the outsourced service which is undertaken by the external service provider not belonging to the financial institution, the official written contract shall be signed, which shall at least indicate the following contents:

— Description on the conformity with legal requirements, e.g. regulations on data protection;

— Description on the risks of outsourced service, including the source of risks, specific description on the risks and their impacts and description about how to maintain and detect the completeness and confidentiality of the organized business assets;

— Description on the security responsibilities that each party in the outsourced service contract shall fulfill; ensure each participator in the outsourced contract understands their own security responsibilities;

— Description on the control measures that shall be taken to control security risks from physical and logical perspectives; what physical or logical measures to be taken shall be specified, e.g. restriction of authorized user to access sensitive business information and what physical security protection level that shall be provided for the outsourced equipment;

— Description on the measures that shall be taken in case of outsourced service risks, e.g. how to maintain service in case of fire accident;

— Description on the time limit and termination conditions of outsourced service and post-handling matters and the responsibilities aroused thereof;

— Description on the access right of audit staff

5.5.4.2 Outsourced service provider

system, including:

- Designate security information management personnel, to take charge of classification management and release of information according to operating rules of information security.

- Any practical procedures and system software that may surpass the system or application program control shall have formal authorization and permission and their usage shall be registered. Assure the access to the application system information or software does not affect the security of sharing information of other information systems.

- The internal users of the application system, including supporting personnel, shall handle authorization permission according to regulated procedures and sign the security agreement according to sensitivity degree of information, to assure confidentiality, integrity and availability of data in the application system.

- Designate special personnel to take charge of audit of the application system, to assure precision, integrity and availability of audit.

- Organize related personnel to inspect security of the application system regularly or irregularly and submit a formal report according to change or risk change of the application system, to propose security suggestions.

- Implement qualification management for the personnel in the key post of the application system, to assure reliability and availability of personnel.

- Formulate a backup plan and emergency plan available of the application system and data, which shall be implemented and managed by special personnel.

- Formulate corresponding rules and regulations of software security management, including management such as development and use of application software. (See 5.8)

c) System security management based on label: on the basis of b), it shall adopt authorization and label management system of use of application software. Unauthorized users are not allowed to install, debug, operate and uninstall application software. Use of the application software shall be audited. Evaluate security of application software regularly or irregularly and submit a formal evaluation report according to change or risk change of the system, to propose security suggestions, and revise and perfect related management systems and rules. The developers of the application system shall not work on daily operation and audit of the application system. The management personnel of the operating system shall not participate security configuration management and application management of the application system.

- Plan maintenance, regular update it to adapt to system development;

- Establish disaster backup plan and its starting mode.

5.6.3.3 Emergency plan implementing assurance

For emergency plan implementing assurance, different security level shall selectively meet one of the following requirements:

a) Emergency plan responsibility requirements: organizing and implementing personnel who know clearly the emergency plan shall be made to know their own responsibilities in the implementation process;

b) Emergency plan capability requirements: on the basis of a), train system-related personnel to know how and when to use controlling method and recovery policy in the emergency plan so as to ensure the capability needed for implementing emergency plan;

c) Emergency plan systemized management: on the basis of b), systemized management shall be conducted to implement and maintain the emergency plan system of whole organization with the plan-implementing process recorded; ensure there is enough resource assurance for implementing emergency plan;

d) Emergency plan supervising measures: on the basis of c) and starting from risk assessment, take all operation management process into consideration and recognize possible incidents causing business process interruption, also there shall be participation and supervision from managers of business resources and processes;

e) Emergency plan continuous improvement: on the basis of d), regular check shall be taken to the correctness and integrity of the plan, and shall be taken immediately when there is significant change in plan; based on importance difference of business application, continuous assessment and improvement shall be taken to plan contents and regulations.

5.7 Supervision and inspection management

5.7.1 Conforming with legal requirements

5.7.1.1 Understanding applicable laws

For understanding applicable laws, different security level shall selectively meet one of the following requirements:

a) Understanding applicable laws and preventing illegal activities: organizations shall know all laws and regulations applicable to information system application scope; as to the design, operation, use, management of information system and

5.7.2.1 Inspection and improvement

For inspection and improvement, different level shall selectively meet one of the following requirements:

a) Basic requirements for inspection and improvement: require organizations to regularly inspect and assess every aspects of security management activities; achieve self-management, self-inspection, self-assessment by referring to security policy and management system of organizations, and implement responsibility system.

b) Systemized inspection and improvement: on the basis of a), establish inspection and improvement system, regularly inspecting whether all implemented security processes abide by security principle and policy established by organizations, whether information system is technologically in compliance with security standard; based on the deficiencies discovered in inspection, make improvement in security management system; achieve state supervision combining with self-management.

5.7.2.2 Compliance inspection of security policy

For compliance inspection of security policy, different security level shall selectively meet one of the following requirements:

a) Inspection to system manager: regular inspect obedience to security policy with focus on manager of information system network, operation system, database system, etc., ensuring they can correctly execute all security processes within their responsibility scope and correctly abide by security policy established by organizations.

b) Complete and systemized inspection: on the basis of a), regular inspect execution of operation regulations and management processes against every position in information system, ensuring the obedience to security policy of organizations; inspection scope shall include information system itself, system manufacturer, owner of information and information asset, user and the management, ensuring their compliance with security policy and standard.

c) Operation process monitor and continuous improvement: on the basis of b), inspect relevant system using condition and operating and other monitoring process; based on inspection results, continuous improvement shall be made to problems in information system security management system and security management execution process.

5.7.2.3 Technology compliance inspection

For technology compliance inspection, different security level shall selectively meet one of the following requirements:

c) Further acceptance requirements: on the basis of c), the followings shall be at least considered in the acceptance of information system construction and revamp:

- Performance and computer capacity requirements;

- Error recovery and reboot process and emergency plan;

- Establishing and testing daily operating process to reach specified standards;

- Implementing security control measures already agreed;

- Effective guiding process;

- Having considered the evidence that new system would have impact on the overall security of organizations;

- Training on operating and using new system.

5.8.3 System startup and stop management

5.8.3.1 Startup management of new system

For the startup management of new information system or subsystem and information system equipment, different security levels shall meet at least one or more of the following requirements:

a) Application and approval for the startup of new system: before startup, new information system or subsystem and information system equipment shall undergo formal tests and acceptance, and after the user or administrator submits an application and the corresponding leaders grant an approval, they can be formally put into use, with specific procedures executed in accordance with the provisions of relevant competent agencies;

b) Test run before the startup of new system: on the basis of a), a test run shall be conducted and continued for a certain period, and after being accepted by corresponding leaders and technical directors, the new system can be formally put into use, with documents formed for filing;

c) Security assessment of new system: on the basis of b), organize relevant administrator, technical director, user and security expert to conduct a special security assessment for the test run of new information system or subsystem and information system equipment, which can be formally put into use after being accepted with documents formed for filing;

d) Audit and follow-up of new system operation: on the basis of c), audit and follow-up shall be conducted and continued for a certain period after any new information system or subsystem and information system equipment being formally put into use,

system security work of each department and subordinate units. (See 5.2.1.1b), 5.2.1.3a))

b) Personnel management requirements: propose the multiple job-holding limitation requirements for security administrators and personnel at other key posts; personnel at key posts shall conduct job rotation periodically; necessary examination and assessment shall be conducted during the recruitment; personnel at key posts shall fulfill the confidentiality obligation before leaving; periodically conduct examination for personnel at key posts. (See 5.2.3.1b), 5.2.3.2b), 5.2.3.3b), 5.2.3.4b), 5.2.3.5b) and 5.2.3.6b))

c) Education and training requirements: cultivate the staff's security awareness and carry out trainings for security policy and operating procedures in a planned way. (See 5.2.4.1b) and 5.2.4.2a))

6.2.4 Risk management requirements

Based on meeting the requirements of Level-one management requirements, requirements of this level are as follows:

a) Risk management requirements and policy: conduct periodic risk analysis and assessment for key system resources; formulate basic risk management policy and provide necessary organization and resource assurance. (See 5.3.1.1b), 5.3.1.2a))

b) Risk analysis and assessment requirements: add the threats list for each asset or each kind of assets; make vulnerability manual analysis and penetration test for the information system, and make comprehensive analysis for each index to get the vulnerability level; conduct overall risk assessment to judge the priority levels of risks, provide suggested risk processing measures, and finally form risk assessment report and relevant intermediate results. (See 5.3.2.1a), 5.3.2.2b), 5.3.2.3b), 5.3.2.4b))

c) Risk treatment and slowdown requirements: determine the information security control measures based on the risk assessment results; (See 5.3.3.1b))

d) Risk-based decision-making requirements: form the residual risk analysis report, and pay close attention to the changes of residual risks and make timely treatment; the top management of the organizations shall decide the acceptance of risks; take corresponding risk avoidance measures to control the operation of the information system. (See 5.3.4.1b), 5.3.4.2b))

e) Risk assessment management requirements: choose the assessment agencies having security service qualifications accepted by national competent agency within the scope accepted by the industry executives or approved by the superior administrative leading departments; supervise and inspect the implementation of confidentiality agreement by the assessment agencies; hide or replace sensitive

b) Security event processing requirements: have perfect security event processing system; for security event reporting and processing, security vulnerabilities and suspicious event as well as those that cannot be determined to be incidents or intrusion events shall be reported. (See 5.6.2.1b), 5.6.2.2b))

c) Emergency processing requirements: conduct institutional management for emergency processing and disaster recovery, which shall be implemented by the emergency processing group; conduct systematic management for developing and maintaining the emergency plan system of the whole organization; conduct training for personnel related to the system to ensure the implementation of the emergency plan. (See 5.6.3.1b), 5.6.3.2a), 5.6.3.3b))

6.2.8 Supervision and inspection management requirements

Based on meeting the requirements of Level-one management requirements, requirements of this level are as follows:

a) Requirement of complying with laws: the organization shall have measures to prevent abuse of information processing equipment; for important application system software, prevent infringement of software copyright due to software upgrading or adapting. (See 5.7.1.1b), 5.7.1.2b), 5.7.1.3a))

b) Requirements of compliance inspection: periodically inspect and assess the security management; for the security policy compliance, the information system administrator shall inspect the compliance condition of the security policy; for technology compliance, periodically inspect the compliance of system security safeguard measures and security implementation standard. (See 5.7.2.1a), 5.7.2.2a), 5.7.2.3a))

c) Audit and supervision requirements: have independent audit institutions to conduct audit for the security management responsible system of the organization, the security risk control of the information system, etc.; conduct discretionary protection under the guidance of the information security supervision functional department and in accordance with the national policy and regulations as well as technology and management standards. (See 5.7.3.1a), 5.7.3.2b))

d) Responsibility determination requirements: solve the problems found during the supervision and inspection within a limited time, and determine the technical responsibilities and management responsibilities as well as the responsible person, and relevant department shall propose the solutions and responsibility treatment opinions; the supervisor shall bear corresponding responsibilities for the information system losses due to failing to timely solve the problems which should have been avoided. (See 5.7.4.1a), 5.7.4.2a))

6.2.9 Life cycle management requirements

c) System startup and stop management: before being formally put into use, the startup of new information system or subsystem and information system equipment shall conduct a test run and obtain the acceptance of special security assessment; before formally stopping running, the existing information system or subsystem and information system equipment needing to stop running shall take necessary security measures, back up data and software, conduct irreversible data cleaning for the equipment to stop running, conduct destruction measures in case of any damages of the storage equipment, and obtain the acceptance of corresponding leaders and technical directors. (See 5.8.3.1c), 5.8.3.2c))

6.4 Level-four: Structured protection level

6.4.1 Management objectives and scope

This level is structured protection level, implementing standardized management and carrying out mandatory protection, which is suitable for important information related to national security, social order, economic construction and public interests and information system. Its damage will cause serious damage to national security, social order, economic construction and public interests. On the basis of achieving the level-three management objectives, the management of this level is required to have security management measures with quantization control and to establish perfect information security management system; to develop strict test plans according to the risk for key control measures; to organize risk assessment immediately for risks with obvious internal and external changes; to have local computing environment that can protect the core and to have reliable network infrastructures and borders; to have strict user rights and access control measures; to have various measures to prevent information from being leaked and theft in various ways to ensure the accuracy and integrity of information and processing methods; to ensure that the authorized users can access the information at any time and to ensure there are perfect control measures(strong audit and anomaly detection) and basic response and recovery measures for responsibilities (Non-repudiation and they take responsible for their own actions). Remind the working personnel to pay attention to their relevant security responsibilities through regular assessment; implement decentralized enforcement mechanism compulsorily; provide reliable facilities management; enhance the configuration management control. Ensure that the system has a strong anti-penetration ability. Ensure that the information system reaches the requirements of this level in GB 17859-1999 through management activities. (See 5.1.1.1 d))

6.4.2 Policy and system requirements

The requirements of this level are as follows based on that the management requirements of level-three are met:

a) Overall security management policy: shall include mandatorily protected information security management policy. The information security leadership team organizes and proposes the guiding ideology and information security departments designate

availability, controllability and so on. The possible indirect consequences of the accidents include endangering national security and social stability, causing economic losses, destroying social images of organizations or institutions and so on.

B.1.5 Risks

The risk means the possible losses caused by some threats to the assets of organizations or institutions by using the vulnerabilities of the system. The risk is assessed through the probability of occurrence of accidents and the possible influences after occurrence.

Given the limitations of protective measures, the information system will face more or less residual risks, so organizations or institutions shall consider the acceptance of residual risks.

B.1.6 Protective measures

Protective measures are the general term of various practices, procedures and mechanisms implemented to handle threats, to reduce vulnerabilities, to limit the effects of accidents, to detect accidents and to promote the recovery of disasters. One function or more functions of the following functions shall be considered to achieve through using protective measures: prevention, delay, stopping, detection, limitation, correction, restoration, monitoring and hint or strengthening of sub-consciousness. The effective areas of protective measures can include physical environment, technical environment (such as hardware, software, and communications), personnel and administration. Protective measures can be access control mechanisms, anti-virus software, encryption, digital signature, firewalls, monitoring and analysis tools, backup power and information backup and so on.

Factors affecting security decided by the operation of organizations or institutions shall be considered in selecting protective measures, such as boundary conditions of organization, business, finance, environment, personnel, time, law, technology and cultural or social factors and so on.

B.2 Security management process

B.2.1 Security management process model

Security management is a process with continuous development and continuous correction, which runs through the information system life cycle, involving the management of security risks, security measures, security running, security configurations and others of information system management level, physical level, network level, operation system level and application system level. security management is the basis of ensuring the correct, security and effectiveness of security technology, security projects, security running of the information system.

The emphasizes and requirements of each stage of management work are different in the

- The entirety and details shall be considered meantime when the implementation plan is reviewed and the inspection shall be done by contrasting the security policy, security requirements of organizations or institutions and the actual situation of it strictly and all backup plans shall be analyzed and contrasted earnestly to ensure that the select plan meets the pretended requirements and standards;

- The selected technology and products shall pass strict selection tests in the implementation process of security measures, which shall comply with regulations and laws in respect of national information security, especially products with password technology shall be selected and purchased according to relevant regulations of national and competent agencies;

- The implementation shall be conducted according to relevant project requirements;

- If the unit has no implementation conditions, the unit shall select another appropriate and reliable implementation unit with corresponding qualification to implement information systems security measures.

B.2.8 Supervision of security implementation process

B.2.8.1 Purposes

To establish a security supervisions system to inspect the quality and sense of responsibility of the construction unit and to ensure the quality of each stage of the project in security implementation process.

B.2.8.2 Principles

It includes:

- Supervise and inspect the implementation from the specification, procedure, process and other aspects to ensure the quality of each stage;

- The security supervise unit or personnel shall be a third party neutral institute obtaining the approval of relevant departments or a personnel with corresponding qualification, which ensures that the implementation of security measures are conducted according to reasonable procedures and technical standards and to ensure the effectiveness of the implementation process.

- Supervisions before the implementation: inspect the authenticity, quality and time of delivery of selected security products; review the identity and qualification of project implementation personnel; review the specific implementation procedures of the implementation unit and the specific implementation plan documents of each procedure; record the time when the implementation unit starts the implementation and the completion time in advance;

- Supervisions in the implementation: plan for and urge the project implementation

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

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