GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 25058-2019

Replacing GB/T 25058-2010

Information Security Technology - Implementation Guide for Classified Protection of Cybersecurity

信息安全技术 网络安全等级保护实施指南

Issued on: August 30, 2019 **Implemented on: March 1, 2020**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology - Implementation Guide for Classified Protection of Cybersecurity

1 Scope

This Standard stipulates the process that classified protection object implements cybersecurity protection work.

This Standard is applicable to the guidance of the implementation of cybersecurity classified protection work.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

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 22240 *Information Security Technology - Classification Guide for Classified Protection of Information System Security*

GB/T 25069 *Information Security Technology - Glossary*

GB/T 28448 *Information Security Technology - Evaluation Requirement for Classified Protection of Cybersecurity*

3 Terms and Definitions

Terms and definitions defined in GB 17859, GB/T 22239, GB/T 25069 and GB/T 28448 are applicable to this document.

4 Overview of Implementation of Classified Protection

4.1 Fundamental Principles

The core of classified security protection is to classify classified protection objects, and carry out construction, management and supervision in accordance with the standards.

protection, take charge of cybersecurity protection and supervision, management work within the scope of their respective duties.

b) Competent department

Competent department shall, in accordance with national management specifications and technological standards on classified cybersecurity protection, take charge of the supervision, inspection and guidance of classified cybersecurity protection work of the operating and using organizations of classified protection objects of the industry, the department or the locality.

c) Operating and using organization

Operating and using organization shall, in accordance with national management specifications and technological standards on classified cybersecurity protection, determine the security protection level of its classified protection objects. If there is a competent department, operating and using organization shall report to its competent department for review and approval. In accordance with the security protection level that is already determined, go through filing procedures at the public security. In accordance with national management specifications and technological standards on classified cybersecurity protection, conduct planning and design of security protection for the classified protection objects. Adopt information technology products and cybersecurity protects that comply with relevant national regulations and classified protection objects' demands for classified security protection. Carry out security construction or re-construction work; formulate and implement various security management systems. Conduct regular self-inspection of the security status, and the implementation of security protection systems and measures of classified protection objects. Select level evaluation institutions that comply with relevant national regulations to conduct level evaluation. Formulate response and disposal schemes for cybersecurity incidents at different levels. Conduct emergency response to cybersecurity incidents at different levels.

d) Cybersecurity service institution

Cybersecurity service institution shall, in accordance with national management specifications and technological standards on classified cybersecurity protection, under the entrustment of the operating and using organization, assist the operating and using organization to complete classified protection-related work, including determination of the security protection level of the classified protection objects, analysis of security demands, overall planning of security, implementation of security construction and transformation, and provision of service supporting platforms, etc.

5.2 Industry / Domain Rating Work

Activity objective:

If necessary, industry / domain competent department may organize the sorting of main social functions / functions and roles of industry / domain; analyze the main operations and service scope, on which, the main social functions / functions are performed; finally, in accordance with the analyzed and sorted content, form overall descriptive documents of operations in the industry / domain.

Participating roles: competent department; cybersecurity service institution.

Activity input: industry introduction documents, GB/T 22240.

Activity description:

This activity mainly includes the following sub-activity content:

a) Identify, analyze the importance of industry / domain

The competent department may organize the sorting of industrial characteristics, scope of operations, main social functions / functions and production output of the industry / domain; analyze the important role that the main social functions / functions play in guaranteeing national security, economic development, social order and public services, etc.

b) Identify main operations of industry / domain

The competent department may organize the sorting of operations that mainly depend on informatization processing in the industry / domain; in accordance with the importance of the social functions / functions undertaken by the operations, other industries' dependency level, determine the main operations in the industry / domain.

c) Rating guidance

The competent department may organize the analysis of the main operations in the industry / domain; in accordance with the importance of operational information and services, analyze the security protection requirements of various main operations; combine the condition of the industry / domain, form industry / domain rating instructions for the main operations. The security protection level of classified protection object of inter-provincial or nationally unified network operation may be uniformly determined by the competent department.

d) Deployment of rating work

The competent department may formulate rating instructions for the industry

object.

c) Identify the management framework of classified protection object

Understand the organizational management structure, management policy, department setting of classified protection object, and department's roles and position responsibilities in the operation; obtain information regarding management characteristics and management framework that support the operation of the classified protection object. Thus, the subject of security responsibility of the classified protection object can be clarified.

d) Identify the network and equipment deployment of classified protection object

Understand the physical environment, and the deployment of network topology and hardware equipment of classified protection object. On this basis, clarify the boundaries of classified protection object, which means the determination of the object and scope of classified protection.

e) Identify operational characteristics of classified protection object

Understand the various operations and operational processes that mainly depend on informatization processing in the organization, from which, clearly identify the operational characteristics of classified protection object that support the operation of the organization.

f) Identify information assets processed by classified protection object

Understand the type of information assets processed by classified protection object, and the importance of these information assets in confidentiality, integrity and availability, etc.

g) Identify the scope and type of users

In accordance with the distribution scope of users or user groups, understand the requirements of the service scope, roles and operational continuity of the classified protection object.

h) Describe classified protection object

Organize and analyze the collected information; form overall descriptive files of the classified protection object. The overall descriptive files of a typical classified protection object include the following content:

1) Overview of classified protection object;

2) Importance analysis of classified protection object;

3) Border description of classified protection object;

classified protection objects into relatively independent objects as the rating objects; ensure that each relatively independently object has the basic characteristics of rating object. During the classification of classified protection objects, firstly, consider elements of organizational management, then, consider factors like the type of operations and physical regions, etc. Objects that carry relatively single operational application or relatively independent operations shall be considered as independent rating objects.

In terms of communication network facilities, such as: telecommunication network, radio and television transmission network, respectively classify them into different rating objects in accordance with security responsibility body, service type or service area. Exclusive communication networks of industries or organizations across provinces may be rated as a whole, or, be classified into several rating objects in accordance with the regions.

In the environment of cloud computing, classified protection object on the cloud service customer side, and cloud computing platform / system on the cloud service provider side shall respectively be considered as independent rating objects. Furthermore, in accordance with different service modes, cloud computing platform / system shall be classified into different rating objects. In terms of large-scale cloud computing platform, cloud computing infrastructure and relevant auxiliary service system should be classified into different rating objects.

The Internet of Things mainly includes characteristic elements like perception, network transmission and processing application. The above elements shall be rated as a whole, and the various elements shall not be individually rated.

In terms of industrial control system, it generally includes characteristic elements like on-site acquisition / execution, on-site control, process control and production management. Specifically speaking, elements like on-site acquisition / execution, on-site control and process control shall be rated as a whole, and the various elements shall not be individually rated. The element of production management should be individually rated. In terms of large-scale industrial control system, multiple rating objects may be classified in accordance with system functions, responsibility body, control object and manufacturer, etc.

Classified protection objects that adopt mobile internet technology mainly include characteristic elements like mobile terminal, mobile application and wireless network, which may be rated as a whole, or, be rated together with associated operation systems, and the various elements shall not be individually rated.

c) Detailed description of rating objects

for industry / domain rating (if possible) and rating method, the operating and using organization shall determine the preliminary security protection level for each rating object.

b) Review of rating result

After preliminarily determining the security protection level, if necessary, the operating and using organization may organize cybersecurity experts and operation experts to review the reasonability of the preliminary rating result and issue experts' review comments.

c) Examination and approval of rating result

After preliminarily determining the security protection level, the operating and using organization shall (if there is an explicit competent department) report the preliminary rating result to the competent department or the higher competent department of the industry / domain for review and approval. The competent department or the higher competent department of the industry / domain shall reasonably review the preliminary rating result and issue review comments.

The operating and using organization shall regularly conduct self-inspection of changes in the level of the classified security objects and the rating of newly established systems; report to the competent department for review and approval in time.

Activity output: rating result; competent department's review comments.

5.4.2 Form rating report

Activity objective:

Organize documents generated during the rating process; form a report of rating result of classified protection object.

Participating roles: competent department; operating and using organization.

Activity input: detailed descriptive files of rating objects; rating result.

Activity description:

Organize the content: overall descriptive documents of classified protection objects, detailed descriptive files, rating result, etc.; form documented report of rating result.

The report of rating result may include the following content:

a) Overview of current situation of organization informatization;

Activity description:

This activity mainly includes the following sub-activity content:

a) Determine the scope and analysis object of classified protection objects

Clarify the scope and border of classified protection objects at different levels. Through the mode of survey or information consulting, understand the operational application and operational procedure of classified protection objects.

b) Form basic security demands

In accordance with the security protection level of classified protection objects of different levels, select requirements of corresponding levels from GB/T 22239 and basic industrial requirements; form basic security demands. In terms of protection objects with an already established level, in accordance with the level evaluation result, analyze the rectification demands; form basic security demands.

Activity output: basic security demands.

6.2.2 Determination of special security demands

Activity objective:

Through the analysis of special protection demands of important assets, adopt the method of demand analysis or risk analysis, determine possible security risks; judge the necessity of implementing special security measures; put forward special security protection demands for classified protection objects.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: detailed descriptive files of classified protection objects; security protection level rating report; other relevant documents of classified protection objects.

Activity description:

The determination of special security demands may adopt currently mature or prevailing demand analysis or risk analysis method, or, adopt the activities introduced below:

a) Analysis of important assets

Clarify important components in classified protection objects, such as: border equipment, gateway equipment, core network equipment, important server equipment and important application system, etc.

Activity output: security demand analysis report.

6.3 Overall Security Design

6.3.1 Overall security policy design

Activity objective:

Form institutional programmatic security policy files, including the determination of security guide and formulation of security policy, so as to combine the series standard of basic requirements for classified protection, basic industrial requirements and special security protection requirements, construct security technology architecture and security management architecture for institution's classified protection objects. In terms of newly established classified protection objects, the security protection level shall be clarified in the approval; in accordance with the requirements of corresponding protection level, conduct the overall security policy design.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: detailed descriptive files of classified protection objects; security protection level rating report; security demand analysis report.

Activity description:

This activity mainly includes the following sub-activity content:

a) Determine security guide

Form institution's highest level of security guide file; clarify the mission and aspiration of security work; define the overall objective of cybersecurity; stipulate responsible institution of cybersecurity and its responsibilities; establish security work operating mode, etc.

b) Formulate security policy

Form institution's highest level of security policy file; elaborate main policies of security work, including security organizational institution's division policy, operational system's classification policy, data information's classification policy and classified protection objects' interconnection policy and information flow control policy, etc.

Activity output: overall security policy file.

6.3.2 Security technology architecture design

Activity objective:

In accordance with GB/T 22239, basic industrial requirements, security demand

network lines and network equipment shall be considered. If rating objects at different levels transmit data through the same line and equipment of the communication network, the security protection policies and security technological measures of lines and equipment shall satisfy the basic requirements for classified protection of the highest level of rating objects.

d) Stipulate protection technological measures of borders of rating objects at different levels

In accordance with institution's overall security policy files, basic requirements for classified protection, and security demands, put forward security protection policies and security technological measures of the borders of rating objects at different levels. If rating objects at different levels share the same equipment for border protection, then, the security protection policies and security technological measures of the border equipment shall satisfy the basic requirements for classified protection of the highest level of rating objects.

e) Stipulate security technological measures of interconnection among rating objects

In accordance with institution's overall security policy files, basic requirements for classified protection, and security demands, put forward protection policy requirements and specific security technological measures of information transmission among rating objects in inter-LAN interconnection, including interconnection policy for the same level and different levels, etc. Put forward protection policy requirements and specific security technological protection measures of information transmission among rating objects in LAN interconnection, including interconnection policy for the same level and different levels, etc.

f) Stipulate security protection technological measures inside rating objects at different levels

In accordance with institution's overall security policy files, basic requirements for classified protection, and security demands, put forward security protection policies and security technological protection measures of internal network platform, system platform, operational application and data of rating objects at different levels. If low-level rating objects are deployed in the network area of high-level rating objects, then, the security protection policies and security technological measures of system platform, operation application and data of low-level rating objects shall satisfy the basic requirements for classified protection of high-level rating objects.

g) Stipulate security protection technological measures of new technologies, such as: cloud computing and mobile internet

and security demands, put forward institution's security organization management framework; allocate security management responsibilities towards rating objects at different levels; stipulate security management policies for rating objects at different levels.

c) Stipulate personnel security management policy of rating objects at different levels

In accordance with institution's overall security policy files, the series standard of basic requirements for classified protection, basic industrial requirements and security demands, put forward management personnel framework of rating objects at different levels; allocate management personnel responsibilities towards rating objects at different levels; stipulate personnel security management policies of rating objects at different levels.

d) Stipulate security management policy of physical environment (computer rooms and office areas) of rating objects at different levels

In accordance with institution's overall security policy files, the series standard of basic requirements for classified protection, basic industrial requirements and security demands, put forward security policy of computer rooms and office environment of rating objects at different levels.

e) Stipulate security management policy for medium and equipment of rating objects at different levels

In accordance with institution's overall security policy files, the series standard of basic requirements for classified protection, basic industrial requirements and security demands, put forward security policy of medium and equipment of rating objects at different levels.

f) Stipulate operational security management policy of rating objects at different levels

In accordance with institution's overall security policy files, the series standard of basic requirements for classified protection, basic industrial requirements and security demands, put forward security operation and maintenance framework, and operation and maintenance security policy of rating objects at different levels.

g) Stipulate security incident handling and emergency management policy of rating objects at different levels

In accordance with institution's overall security policy files, the series standard of basic requirements for classified protection, basic industrial requirements and security demands, put forward security incident handling and emergency management policy of rating objects at different levels.

determine security construction objectives of different stages.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: overall security scheme of classified protection objects; long and mid-term development planning of institution or organization's informatization construction.

Activity description:

This activity mainly includes the following sub-activity content:

a) Long and mid-term development planning and security demand survey of informatization construction

   Understand and survey the current situation of organization's informatization construction, the objectives of long and mid-term informatization construction, the competent department's investment in informatization; compare the gap between stage state and security policy planning during the informatization construction process; analyze urgent and critical security issues; consider the content of security construction that may be synchronously conducted.

b) Put forward staged objectives of security construction of classified protection objects

   Formulate overall security objectives that classified protection objects shall implement within the planned period (generally, security planning period is 3 years); formulate security objectives that classified protection objects shall implement in the short term (within 1 year); give priority to the settlement of existing urgent and critical security issues; strive for substantial improvement of security status within a short term.

Activity output: staged security construction objectives of classified protection objects.

6.4.2 Security construction content planning

Activity objective:

In accordance with security construction objectives, and the requirements of overall security scheme of classified protection objects, design construction content in stages and batches. Combine the construction content into different projects; clarify the dependency or promoting relationships among the projects.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: overall security scheme of classified protection objects; staged security construction objectives of classified protection objects.

Activity description:

Activity input: overall security scheme of classified protection objects; staged security construction objectives of classified protection objects; security construction content, etc.

Activity description:

Organize staged security construction objectives of classified protection objects, overall security scheme and security construction content; form security construction project planning of classified protection objects.

Security construction project planning may include the following content:

a) Basis and principle of planning and construction;

b) Objective and scope of planning and construction;

c) Current security status of classified protection objects;

d) Long and mid-term development planning of informatization;

e) Overall framework of security construction of classified protection objects;

f) Security technology architecture construction planning;

g) Security management and security assurance system construction planning;

h) Security construction investment estimation (including testing and operation and maintenance estimation);

i) Implementation guarantee of security construction of classified protection objects.

Activity output: security construction project planning of classified protection objects.

7 Security Design and Implementation

7.1 Workflow of Security Design and Implementation Stage

The objective of the security design and implementation stage is: in accordance with the requirements of the overall scheme of classified protection objects, combine security construction project planning of classified protection objects, implement security measures in stages and in steps.

The workflow of the security design and implementation stage is shown in Figure 6.

7.2 Detailed Design of Security Scheme

7.2.1 Design of technological measure implementation content

Activity objective:

In accordance with the objectives and the content of construction, implement security policy, security technology architecture, security measures and requirements that are required to be implemented in the overall security scheme of classified protection objects onto product functions or physical form; put forward products or components that can be implemented, and their specific specifications. In addition, organize product functional characteristics into documents, so that there can be basis for the procurement of cybersecurity products and the development of security control.

Participating roles: operating and using organization; cybersecurity service institution; cybersecurity product supplier.

Activity input: overall security scheme; security construction project planning; technological description of various information technology products and cybersecurity products; cybersecurity service institution evaluation materials.

Activity description:

This activity mainly includes the following sub-activity content:

a) Design of structural framework

In accordance with the construction content of the current implementation project and the practical situation of classified protection objects, provide security implementation technology framework that is consistent with the security architecture of the overall security planning stage. The content shall at least include the hierarchy of security protection, the application of cybersecurity products, the division of network sub-systems, IP address planning, the selection of cloud computing mode (if possible) and the access mode of mobile internet (if possible), etc.

b) Design of security function requirements

In terms of relevant cybersecurity products used in the security implementation technology framework, such as: firewall, VPN, gatekeeper, authentication gateway, proxy server, network anti-virus, PKI, cloud security protection products, mobile terminal application software and protection products, put forward requirements for security functional indicators. In terms of security control components that need to be developed, put forward requirements for security functional indicators.

c) Design of performance requirements

content of security management design shall mainly consider: the formulation of security policy and management system, security management institution and personnel supporting, security construction process management, etc.

Activity output: management measure implementation scheme.

7.2.3 Documentation of design result

Activity objective:

Summarize technological measure implementation scheme and management measure implementation scheme, meanwhile, consider labor-hour and cost. Finally, form guidance documents that guide security implementation.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: technological measure implementation scheme; management measure implementation scheme.

Activity description:

Organize documents of technological implementation content in technological measure implementation scheme and management implementation content in management measure implementation scheme; form detailed design scheme of security construction of classified protection objects.

Detailed security design scheme includes the following content:

a) Objective and content of construction;

b) Technological implementation scheme;

c) Security functions and performance requirements for cybersecurity products or components;

d) Deployment of cybersecurity products or components;

e) Security control policy and allocation;

f) Supporting security management construction content;

g) Construction implementation scheme;

h) Project investment estimation.

Activity output: detailed security design scheme.

shall guarantee the compliance with relevant national stipulations regarding the usage of cybersecurity products. In terms of the usage of password products, select and use them in accordance with relevant national stipulations regarding password management.

Activity output: performance, functions and security demands for cybersecurity products that need to be purchased, or service institution's competence requirements (checklist mode is allowed).

7.3.2 Development of security control

Activity objective:

In terms of some security measures and security functions that cannot be implemented through the procurement of existing cybersecurity products, they shall be implemented through exclusive design and development. The development of security control shall be synchronously designed and implemented with application development of the system. Once the development of application system is completed, there will be enormous cost investment if extra security measures are added. Hence, during the application system development, conduct development design of security control in accordance with the detailed security scheme, so as to guarantee synchronous construction of system application ad security control.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: detailed security design scheme.

Activity description:

This activity mainly includes the following sub-activity content:

a) Security measure demand analysis

In a standardized form, accurately express the indicator requirements in the design of security scheme. Under the circumstance when new technologies like cloud computing and mobile internet are adopted, analyze peculiar security threats; determine corresponding security measures and interface details related to other systems.

b) Outline design

Outline design shall consider the indictor requirements of identity authentication, access control, security auditing, software fault tolerance, resource control, data integrity, data confidentiality, data backup and recovery, residual information protection and personal information protection in security scheme; design the architecture of the security measure module; define the composition of the development of the security measure module; define the

7.3.3 Security control integration

Activity objective:

Integrate different software and hardware products. In accordance with detailed security design scheme, combine cybersecurity products, security control module of system software platform and development, various application systems, and merge them into a system. During the process of security control integration, the operating and using organization may work together with cybersecurity service institution, cooperate with each other, and organically combine security implementation, risk control and quality control, so as to implement security measures like security situation awareness, monitoring notification and early warning, emergency response tracking and tracing, and construct a uniform security management platform.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: detailed security design scheme.

Activity description:

This activity mainly includes the following sub-activity content:

a) Formulation of integration implementation scheme

The main work content is to formulate integration implementation scheme. The objective of integration implementation scheme is to specifically instruct the content, methods and specifications of the construction. A prominent characteristic that distinguishes implementation scheme from security design scheme is its extremely strong operability. It shall be specifically implemented in the installation, deployment and allocation of products. Implementation scheme is a specific guidance document for engineering construction.

b) Integration preparation

The main work content is to prepare for the implementation environment, including hardware equipment preparation, software system preparation and environment preparation. In order to guarantee the quality of system implementation, cybersecurity service institution shall, in accordance with the system design scheme, formulate a set of feasible system quality control scheme, so as to effectively guide the system implementation process. This quality control scheme shall determine the quality control goals, control measures, handling procedure for project quality issues, and responsibility requirement for system implementers of the various stages of system implementation; provide a detailed schedule of security control integration.

c) Integration implementation

This activity mainly includes the following sub-activity content:

a) System acceptance inspection preparation

After the development and integration of security control is completed, in accordance with the security goals that need to be attained in the security design scheme, prepare for acceptance inspection scheme. The acceptance inspection scheme shall be established on contract clauses, demand specifications and security design scheme, and thoroughly reflect users' security demands.

Establish acceptance inspection group to review the acceptance inspection scheme; organize the formulation of acceptance inspection scheme; define the method and the pass criteria of acceptance inspection.

b) Organization of acceptance inspection

The acceptance inspection group shall organize the implementation in accordance with the acceptance inspection scheme; organize inspection personnel to conduct acceptance inspection test of the classified protection objects of system acceptance inspection schemes that have already passed the review. Specifically speaking, functional test shall cover functionality, reliability, ease of use, maintainability and portability, etc.; performance test shall cover time characteristics and resource characteristics; security test shall cover security mechanism verification of computing environment, zone boundary and communication network.

c) Acceptance inspection report

After the test is completed, form acceptance inspection report. The acceptance inspection report needs to be confirmed by users and the construction party. The acceptance inspection will explicitly offer a conclusion of the acceptance inspection. Security service provider shall, in accordance with acceptance inspection comments, correct relevant problems as soon as possible; re-conduct acceptance inspection or transfer to contract dispute resolution procedure. In terms of Level-3 and above classified protection objects of cybersecurity protection, classified protection evaluation report shall be submitted as a necessary document for acceptance inspection.

d) System delivery

After classified protection objects pass the acceptance inspection, the delivery of classified protection objects shall be conducted. Security service institution shall submit documents of system construction process, documents guiding users in system operation and maintenance, and service commitment, etc.

specifications; management system review and revision records.

7.4.2 Security management institution and personnel setting

Activity objective:

Establish supporting security management functional department. Through management institution's post setting, personnel labor division and post training, and the allocation of various resources, ensure that personnel have the technical skills and management capabilities that are compatible with their job responsibilities, so as to provide organizational guarantee to the security management of classified protection objects.

Participating roles: operating and using organization; management personnel of classified protection objects; cybersecurity service institution.

Activity input: detailed security design scheme; instruction of security members and roles; various management systems and operational specifications.

Activity description:

This activity mainly includes the following sub-activity content:

a) Determine security organization

   Identify organization members and their roles that are related with cybersecurity management, such as: operators, document administrators, system administrators, security administrators, etc.; form a security organization structural table.

b) Role description

   In a written form, describe each role and its responsibilities in details; clarify the responsibilities and the scope of authority of relevant post personnel; seek the opinions of relevant personnel; ensure that the responsibilities are explicit and that all the risks are handled by somebody.

c) Personnel security management

   Carry out specific skill training and security awareness training for ordinary employees, administrators, developers, supervisors and security personnel. After the training, they shall be assessed, and qualified personnel will be issued employment qualification certificates.

Activity output: instruction of institution, roles and responsibilities; training records and employment qualification certificate, etc.

During the construction of classified protection objects, due to changes in various conditions, there will be alterations. The alterations occur in the scope, schedule, quality, cost, human resources, communication and contract of project, etc. The handling of each alteration shall comply with the same procedure, namely, the same written report, the same management method and the same monitoring process. The impact of each alteration on system cost, schedule, risks and technological requirements shall be determined. Once an alteration is approved, a procedure shall be set up to implement the alteration.

e) Schedule management

The implementation of the construction of classified protection objects must have a clear set of deliverables, and meanwhile, a date of termination. Hence, during the construction of classified protection objects, project schedule shall be formulated; schedule network diagram shall be drawn; the system shall be decomposed into different sub-tasks; time control shall be implemented to ensure that the project is completed as scheduled.

f) Document management

Document is written materials that record the entire process of the project. During the construction of classified protection objects, for each link, there shall be a great deal of document output. Document management involves the various links of the construction of classified protection objects, which mainly include: system rating, planning design, scheme design, security implementation, system acceptance inspection and personnel training, etc.

Activity output: documents and records of management processes of various stages.

8 Security Operation and Maintenance

8.1 Workflow of Security Operation and Maintenance Stage

Security operation and maintenance is a necessary link that ensures the normal operation of classified protection objects during the implementation of classified protection. It involves a lot of content, including the establishment of security operation and maintenance institution, and security operation and maintenance institution; the management of environment, assets, equipment and media; the management of networks and systems; the management of passwords and keys; the management of operation and alterations; security status monitoring and security incident handling; security auditing and security inspection, etc. This Standard will not describe all the above-mentioned management processes. Users of this Standard who hope to comprehensively understand and control the various processes of the security operation and maintenance stage may take other standards or guides as a reference.

8.2 Operation Management and Control

8.2.1 Determination of operation management responsibilities

Activity objective:

Through the role division of operation management activities or tasks, and the granting of corresponding management authority, determine the specific personnel and responsibilities of security operation management. Roles shall at least be divided into system administrators, security administrators and security auditors.

Participating role: operating and using organization.

Activity input: detailed security design scheme; a list of security institutional framework.

Activity description:

This activity mainly includes the following sub-activity content:

a) Divide operation management roles

In accordance with management system and the actual demands for operation management, divide roles and users needed for operation management. The roles and users shall be established by system administrators. The higher the security protection level is, the more detailed the role division of operation management shall be.

b) Grant management authority

In accordance with management system and the actual demands for operation management, security administrator shall grant different administrative rights to each operation management role and user. The higher the security protection level is, the more detailed the division of system management authority shall be.

c) Define personnel responsibilities

In accordance with the control granularity requested by different security protection levels, analyze the content that needs operation management and control. Through this, define the responsibilities of different operation management roles. Security auditors shall audit system administrators and security administrators' operation logs.

Activity output: a list of operation management personnel's roles and responsibilities.

8.2.2 Operation management process control

Activity objective:

Activity description:

This activity mainly includes the following sub-activity content:

a) Alteration demand analysis

Analyze alteration demands during the operation and maintenance process; determine the content, the resource demands and the scope of alteration; judge the necessity and feasibility of alteration.

b) Alteration influence analysis

Judge and analyze consequences that might be triggered by alterations during the operation and maintenance process; determine the extent of possible influence; determine the prerequisites and subsequent activities of alteration, etc.

c) Clarify the category of alteration

Determine whether partial adjustment or significant alteration shall be conducted to classified protection objects. If significant alteration is triggered to the security protection level of classified protection objects due to changes of the type of classified protection objects, the type of information assets being undertaken, the scope of services of classified protection objects and the automation degree of operational processing, then, the security protection level of classified protection objects needs to be re-determined; return to the classified protection object rating stage in the implementation of classified protection. If partial adjustment is needed, then, determine the other work content that needs to be supportively performed.

d) Formulate alteration scheme

In accordance with the result of a), b) and c), formulate alteration scheme.

Activity output: alteration scheme.

8.3.2 Alteration process control

Activity objective:

Ensure that the alteration implementation process is under control during the operation and maintenance. The various alteration content shall be recorded, so as to guarantee that the influence of the alterations on the operation is the minimum.

Participating role: operating and using organization.

Activity input: alteration scheme.

they might include external objects, for example, security standards, laws and regulations.

b) Form a list of monitoring objects

In accordance with the determined monitoring objects, analyze the necessity and feasibility of monitoring, and factors like the expenditure and the cost of monitoring; form a list of monitoring objects.

Activity output: a list of monitoring objects

8.4.2 Collection of monitoring object status information

Activity objective:

Select status monitoring tools; collect information of security status monitoring; identify and record intrusion behaviors. Monitor the security status of classified protection objects.

Participating role: operating and using organization.

Activity input: a list of monitoring objects.

Activity description:

This activity mainly includes the following sub-activity content:

a) Select monitoring tool

In accordance with the characteristics of monitoring objects, the specific requirements of monitoring management, and the functions and performance characteristics of monitoring tools, select a suitable monitoring tool. Monitoring tool may not be an automated tool, but an organization constituted of various personnel and complies with certain rules in operation, or, a combination of both.

b) Collect status information

Collect various status information coming from the monitoring object. It might include network flow, log information, security alarms and performance conditions, etc. Or, it might be alteration information of security standards, laws and regulations that come from the external environment.

Activity output: security status information.

8.4.3 Monitoring status analysis and report

Activity objective:

Activity description:

This activity mainly includes the following sub-activity content:

a) Determine the object and the method of self-inspection

Determine the object and the method of self-inspection; determine the scope and the tool of the current security self-inspection, and the survey form, etc.

b) Determine the plan and the scheme of self-inspection

Determine the roles and responsibilities of self-inspection work; determine the method of self-inspection work; establish security self-inspection work group. Formulate security self-inspection work plan and security self-inspection scheme. Explain the scope, object and method of security self-inspection. Prepare for various forms and tools needed for security self-inspection.

c) Implement security self-inspection

In accordance with the security self-inspection plan, through multiple means like inquiry, inspection and test, conduct self-inspection of security status. Record the result data of various self-inspection activities; analyze the effectiveness of security measures, the possibility of the occurrence of security incidents and the actual improvement demands of rating objects.

d) Security self-inspection result and report

Summarize the result of security self-inspection; propose suggestions of improvement; generate security self-inspection report. Archive and reserve various documents and materials of the security self-inspection process.

Activity output: security self-inspection report.

8.5.2 Formulation of improvement scheme

Activity objective:

In accordance with the result of security inspection, adjust the security status of classified protection objects, so as to ensure the effectiveness of security protection of classified protection objects.

Participating role: operating and using organization.

Activity input: security self-inspection report.

Activity description:

This activity mainly includes the following sub-activity content:

In accordance with the implementation of security improvement scheme and the various supplementary security measures, various relevant technological files and management systems shall be adjusted and revised, so as to ensure the integrity and consistency of the previous system.

Activity output: test or acceptance inspection report.

8.6 Management and Monitoring of Service Provider

8.6.1 Selection of service provider

Activity objective:

Determine service providers with nationally or industrially stipulated design, evaluation and construction qualifications; lay a foundation for the subsequent management and monitoring.

Participating roles: operating and using organization; cybersecurity service institution.

Activity input: detailed security design scheme; implementation scheme, etc.

Activity description:

This activity mainly includes the following sub-activity content:

a) Analysis of service capabilities

From the perspective of key factors that affect system and operational security, analyze service provider's service capabilities. In accordance with national requirements regarding bidding, select an optimal service provider. These factors might include: service provider's basic information, enterprise qualifications and personnel qualifications, credibility, technological strength and industrial experience, internal control and management capabilities, continuous operation status, service level and personnel allocation, etc.

b) Analysis of cybersecurity risks

When selecting service providers, service provider's cybersecurity risks need to be identified, so as to prevent high-risky and unqualified service providers from undertaking safe operation and maintenance projects. Cybersecurity risk points include, but are not limited to:

---Service provider's possible leaks.

---Service provider's service capabilities and industrial experience.

---Physical access, loss of information, unauthorized access to the system and mis-operation, etc.

---During the process of providing using organization with services, service provider's personnel shall rigorously comply with the using organization's various stipulations and management requirements and using organization's arrangements.

---If the service provider's personnel cause personal injury or property damage to the using organization or a third party, the service provider shall bear the liability for compensation.

---The using organization shall urge service provider to conduct training and security education work among the service personnel.

b) Service management

In order to ensure that the service work of service providers satisfies the agreed requirements, service provider shall satisfy (but not restricted to) the following requirements:

---Service provider shall provide complete entry-related materials (such as: enterprise qualifications, personnel qualifications, list of personnel, materials, etc.) and accept the using organization's review.

---When service provider's basic information changes, such as: legal person, name of organization and bank account, inform the using organization in advance.

---In accordance with the agreed requirements, service provider shall provide various services and complete service tasks with guaranteed quality and quantity. If the service provider fails to complete the service goals and causes loss to the using organization, compensations shall be made.

---Service provider ensures that the services provided do not infringe a third-party's copyright, trademark right, patent right and other legitimate interests; service provider shall properly protect the research achievements and intellectual property rights generated during the service process. Without permission from the using organization, service provider shall not transfer the rights and obligations to any third party in any form.

---Service provider shall provide relevant materials of acceptance inspection and assessment of projects; cooperate with the using organization to carry out final acceptance inspection and assessment.

---The using organization shall, in accordance with the agreed content and standards of after-sales services, conduct real-time tracking of service provider's after-sales service assessment; consider this as a

advance; properly handover the work; proceed with the agreement of the using organization.

Activity output: service provider analysis and evaluation report.

8.7 Level Evaluation

Activity objective:

Through cybersecurity level evaluation institution, conduct regular level evaluation of classified protection objects that have already completed classified protection construction, so as to ensure that the security protection measures of the classified protection objects comply with the security requirements of corresponding level.

Participating roles: competent department; operating and using organization; cybersecurity level evaluation institution.

Activity input: detailed descriptive files of classified protection objects; security protection level rating report of classified protection objects; system acceptance inspection report.

Activity description:

a) Cybersecurity level evaluation institution shall conduct level evaluation of classified protection objects in accordance with the relevant specifications or standards of security protection level evaluation of classified protection objects.

b) The operating and using organization shall take the security level evaluation report issued by level evaluation as a reference to analyze and determine the rectification demands.

Activity output: security level evaluation report; rectification demands.

8.8 Supervision and Inspection

Activity objective:

In accordance with classified protection management department's requirements for supervision and inspection of the rating, planning and design, construction implementation and operation management process of classified protection objects, classified protection management department shall, in accordance with relevant national and industrial requirements and standards of classified protection supervision and inspection, carry out supervision and inspection work.

The competent department, and the operating and using organization shall prepare corresponding supervision and inspection materials; cooperate with classified protection management department in the inspection, so as to ensure that classified

a) Establish emergency-handling organization

In accordance with the demands of emergency rescue, establish emergency-handling organization. Generally speaking, emergency-handling organization is divided into five core emergency-handling functional institutions, namely: command, operation, planning, logistics and finance.

b) Clarify emergency-handling responsibilities

Clarify the composition or personnel, responsibilities and authority of leading institution, administrative body, special emergency command institution, grass-root emergency-handling institution and emergency-handling expert group for emergency management.

c) Classification and rating of security incidents

Take *Emergency Plan of National Network Security Incident* and GB/Z 20986-2007 as a reference; in accordance with the type of security incidents, the scope and extent of influence of security incidents on operations, and the sensitivity level of security incidents, classify and rate possible security incidents of classified protection objects. In accordance with different categories and levels, formulate corresponding security incident reporting procedure.

d) Determine the objects of emergency plan

In accordance with different categories and levels of security incidents, consider the possibility of the occurrence and the impact on the system and the operations; determine the objects of emergency plan that needs to be formulated.

e) Determine the responsibilities and emergency coordination mode

Under a uniform framework of emergency plan, clarify the responsibilities of different departments in the emergency plan, and the cooperation and labor division mode among the departments.

f) Formulate emergency plan procedure and its execution conditions

In accordance with different categories and levels of security incidents, formulate corresponding procedure of emergency plan; determine the scope and extent of response and disposal of different categories and levels of security incidents; explain the conditions of initiating the emergency plan, and procedures and measures to be taken after a security incident occurs.

g) Publicizing and implementation of training

In accordance with departments and personnel involved in emergency plan,

incidents; analyze their development trends, and the impact of these changes on the security status. By judging their impact, determine whether it is necessary to respond.

c) Report and share security incidents

In accordance with the result of security status analysis and impact analysis, analyze possible security incidents; clarify the level, extent of impact and priority of the security incidents; form a security status analysis report and cybersecurity incident report form. In accordance with the level of security incidents and security incident report procedure, report the security incidents. Share security incidents that need to be shared to specific objects in accordance with the stipulations.

d) Dispose security incidents

In terms of security incidents that need to initiate emergency plan, in accordance with the emergency plan response mechanism, dispose the security incidents. The disposal of unknown security incidents shall formulate security incident disposal scheme in accordance with the level of security incidents. The disposal scheme includes security incident disposal methods and measures that shall be adopted. In accordance with the security incident disposal procedure and scheme, dispose the security incidents.

e) Summarize and report security incidents

Once security incidents are resolved, if the security incidents are unknown, record them; analyze the recorded information and supplement necessary information, so that the security incidents could become known and be documented. Summarize the security incident disposal process; formulate security incident disposal report and reserve it.

Activity output: cybersecurity incident report form; security status analysis report; security incident disposal report.

8.9.3 Post-mortem evaluation and improvement

Activity objective:

Investigate and analyze the causes and disposal process of security incidents. Moreover, in accordance with the analysis result, determine the responsibilities and formulate improvement and precautionary measures.

Participating role: operating and using organization.

Activity input: security incident report procedure; various special emergency plans; security incident disposal report.

Meanwhile, adopt secured methods to eliminate information in rating objects to be terminated.

Participating role: operating and using organization.

Activity input: a checklist of rating object information assets.

Activity description:

This activity mainly includes the following sub-activity content:

a) Identify information assets to be transferred, temporarily stored and removed

In accordance with the checklist of information assets of rating objects to be terminated, identify important information assets, location and current status, etc.; make a checklist of information assets that need to be transferred, temporarily stored and removed.

b) Transfer, temporarily store and remove information assets

In accordance with the importance of information assets, formulate methods and processes for the transfer, temporary storage and removal of information assets. If it is confidential information, conduct the transfer, temporary storage and removal in accordance with the stipulations of relevant national departments.

c) Record the processing process

Record the process of information transfer, temporary storage and removal, including participating personnel, the mode of transfer, temporary storage and removal, and the current location of the information.

Activity output: information transfer, temporary storage and removal disposal record documents.

9.3 Equipment Migration or Abolishment

Activity objective:

Ensure that after the termination of rating objects, the migrated or abolished equipment does not include sensitive information. The mode of equipment disposal shall comply with the requirements of relevant national departments.

Participating role: operating and using organization.

Activity input: a checklist of equipment transfers or abandonment.

Activity description:

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

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