JR

ICS 03.060

A 11

INDUSTRY STANDARDS OF

THE PEOPLE'S REPUBLIC OF CHINA

JR/T 0072-2012

Testing and Evaluation Guide for Classified Protection of Information System of Financial Industry

金融行业信息系统信息安全等级保护测评指南

Issued on: July 06, 2012 **Implemented on: July 06, 2012**

Issued by: THE PEOPLE'S BANK OF CHINA

Table of Contents

Foreword

This is the second-item standard of series standard “Classified protection of information system of financial industry”. Structure and name of the series standards are as follows:

Implementation guide for classified protection of information system security of financial industry

Testing and evaluation guide for classified protection of information system security of financial industry

Testing and evaluation service security guide for classified protection of information security of financial industry

This Standard is drafted in accordance with the rules specified in GB/T 1.1-2009.

This Standard was proposed by the People's Bank of China.

This Standard shall be under the jurisdiction of China Financial Standardization Technical Committee.

Responsible drafting organization of this Standard: The Department of Science-technology of the People's Bank of China.

Participation drafting organizations of this Standard: China Financial Computerization Corp.

Main drafters of this Standard: Wang Yonghong, Wang Xiaoqing, Zhang Yongfu, Wang Xiaoyan, Wang Haitao, Yang Jian, Bai Zhiyong, Shen Like, Xu Ming, Xu Ziqiang, Qiu Ningning, Li Fan, Zheng Kaiyi, Chen Guanghui, Zhao Yibin, Yang Ying and Zhou Qingbin.

This Standard is issued for the first time.

Introduction

Important information system of financial industry is related to national economy and the people's livelihood; it is a key protected object of national information security; national information security regulatory functional department shall guide and supervise the information security protection work of important information and information system.

Classified protection of information security is a basic national system on information security assurance; financial industry, as one of the important information system industrial sectors, shall follow to implement this system. Centering on the launching of classified protection of information security, a series of appropriate classified protection standard systems are required as a support to regulate and guide implementation of classified protection work of finance. Therefore, Science-technology Division of the People's Bank organizes experts and related technical personnel in classified protection field to develop industrial standard and implementation guide in classified protection of information that comply with the characteristics of financial industry and practical, in accordance with relevant national standard and system of classified protection of information.

In the text of this Standard, the black-bold-letters marked as class F refer to security requirements that are newly added based on business characteristics of financial industry; the black-bold-letters not marked as class F refer to the enhanced requirements of required-items in GB/T 22239-2008 "Baseline for Classified Protection of Information System Security".

Testing and Evaluation Guide for Classified Protection of Information System of Financial Industry

1 Scope

This Standard specifies the requirements for classified protection of information system of financial industry, including unit-evaluation requirements for security evaluation of second-level information system, third-level information system and fourth-level information system and overall evaluation system of information system, etc. Based on the classification of information system of financial industry, fifth-level system does not exist, while first-level system is not required to file at public security agency, and it is not the key point of evaluation. This Standard omits specific content requirements for unit-evaluation of first-level information system and fifth-level information system.

This Standard applies to the industry to perform self-evaluation (e.g. second-level information system), security evaluation of classified protection of information system security that is performed by information security evaluation service agency (e.g. third-level and fourth-level information systems).

2 Normative references

The following documents are indispensable for the application of this document. For the dated documents so quoted, only the dated versions apply to this document. For the undated documents so quoted, the latest versions (including all modification sheets) apply to this document.

GB/T 22239-2008 Information security technology - Baseline for classified protection of information system security

JR/T 0003-2001 Security specification for the interoperable services of bank card

JR/T 0013-2004 The security specification for star topology inter-networking of financial industry

JR/T 0011-2004 Systematic specification of centralized bank data center

JR/T 0023-2004 The criterion of IT management for securities companies

JR/T 0026-2006 Specification for protection against lightning of banking computer information system

JR/T 0044-2008 Management specification of information system disaster recovery for banks

JR/T 0055.4-2009 Technical specifications on bankcard interoperability - Part 4: Data

secure transmission control

Yin-Fa (2002) No.260 Guiding opinions of the People's Bank of China on Strengthening Bank Data Concentration Security Work

Yin-Ke-Ji (2006) No.73 Guidelines on Information System Security Configuration of the People's Bank of China

Yin-Ban-Fa (2006) No.154 IT Contingency Plan Guidelines of the People's Bank of China

Yin-Ban-Fa (2006) No.9 Guidelines on Computer Room Standardization of the People's Bank of China

Yin-Fa (2010) No.276 Provisions on Computer System Information Security Management of the People's Bank of China

Yin-Jian-Fa (2008) No.50 Measures for the Commissioning and Change of Important Information Systems of Banking Institutions

Yin-Jian-Hui (2009) No.19 Guidelines on the Information Technology Risk Management of Commercial Banks

Yin-Jian-Ban-Fa (2009) No.437 Working Guidelines for the Response Handling in Banking and Securities Cross-industry Information System Emergencies

Yin-Jian-Ban-Fa (2010) No.112 Guides on the Regulation of Data Centers of Commercial Banks

Zhong-Zheng-Xie-Fa (2006) Technical Guidelines for Centralized Transaction Security Management of Security Companies

Zhong-Qi-Xie-Fa (2009) Technical Guidelines for Online Futures Information System of Futures Companies

Zhong-Zheng-Xie-Fa (2009) No.154 Guidelines for Information Technology of Security Exchange

Bao-Jian-Hui-Ling (2003) No.3 Provisions on Preparedness and Response for Emergencies in Insurance Industry

3 Overview

3.1 Evaluation contents

Evaluation for classified protection of information system shall include two aspects: the first is security control evaluation, mainly for the implementation configuration of basic security control in information system as required classified protection of information security; the second is overall evaluation of system, mainly for the overall security of

analysis information system. Security control evaluation is the basis of overall security evaluation of information system.

Description of security control evaluation is organized by the mode of work-unit. Work-unit is divided into two categories - security technology evaluation and security management evaluation. Security technology evaluation includes security control evaluation on five levels of physical security, network security, host system security, application security and data security; security management evaluation includes security control evaluation in five aspects of security management organization, security management system, personnel security management, system construction management and system operation-maintenance management.

Overall evaluation of system involves both overall topology and local structure of information system, and implementation of specific security functions of information system and security control configuration, which is closely associated with the actual situation of a particular information system, with complex content and full of personality. Therefore, it is very difficult to comprehensively provide complete content of overall evaluation requirements of system, specific implementation method and clear determination method of results. Evaluation personnel shall determine the specific contents of overall evaluation of system, in combination with requirements of this Standard based on specific circumstances of information system; give key consideration to incidence relation between security controls, layers and regions based on security control evaluation; evaluate whether there are enhancing, supplementing or weakening roles on security functions between security controls, layers and regions as well as overall structural security of information system, overall security between different information systems, etc. based on security control evaluation.

3.2 Evaluation object

Evaluation object is a constituent of information system involved in implementation process of evaluation, objectively existing personnel, documentation, mechanism or equipment, etc. Evaluation object may be a single person, document, mechanical, equipment, etc. or a collection of several persons, documents, mechanisms, equipment, etc., which shall respectively use some specific security control function.

3.3 Evaluation index

GB/T 22239-2008 proposes specific requirements for security functions and measures of information systems of different levels; class-evaluation shall take corresponding security evaluation indexes of general index class (G), business information security index class (S) and business service assurance class (A) in accordance with classification situation of information system; security evaluation for information system shall be carried out based on “Information Security Technology - Evaluation Requirement for Classified Protection of Information System” and “Information Security Technology - Process Guidelines for Security Level of Information System”.

3.4 Evaluation method

3.4.1 Field evaluation method

Field evaluation generally adopts three methods - interview, inspection and evaluation.

1) Interview is a method that evaluation personnel obtain the evidence through communication, discussion and other activities with personnel of information system; main tool used for interview is interview list. Evaluation personnel communicate and discuss with relevant personnel of information system item by item on the problems in interview list, and get to know and confirm the security protection of information system based on the answers of interviewed personnel;

2) Inspection is a method that evaluation personnel obtain the evidence through evaluation object, examination, analysis and other activities; main tool used for inspection is verification list. Evaluation personnel verify the issues in verification list item by item through observation, examination, analysis and other activities. Based on inspection objects, inspection may be further divided into document review, field observation, configuration verification, etc.;

3) Evaluation is a method that evaluation personnel make the evaluation object to generate specific response and other activities according to a predetermined method/tool, and obtain evidence through examining and analyzing response output results.

In accordance with tools and implementation processes, evaluation may be further divided into information access, vulnerability scanning, penetration scanning, cryptanalysis and other modes.

1) Information access means obtaining host/equipment name, IP address, operating system, open service ports, specific data packet and other information contents;

2) Vulnerability scanning means using vulnerability scanning equipment to automatically detect target equipment and finding misconfiguration and known security vulnerabilities at network open ports of hosts/equipment;

3) Penetration test is one of means of simulating attack technology to intrude into information system and obtain information resource that hackers may use, through which security situation of information system is more intuitively and efficiently evaluated.

Vulnerability scanning and penetration evaluation for information system from different access-points may reflect the security status of information system from different angles and different visions.

3.4.2 Risk analysis method

Risk analysis method includes:

1) Determining the possibility that lacking of information system security protection

machine room and office space;

c) Inspect whether machine room and office space are in buildings that have basic quakeproof, windproof and rainproof capacities.

Result judgment

a) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Physical access control (G2)

Evaluation items

a) Machine room entrance and exit shall be able to control, identify and record the incoming personnel;

b) Visiting personnel who enter into machine room shall apply for and get approval; the range of activity shall also be restricted and monitored;

c) Machine room shall be zoned for management, e.g. machine room is divided into production area and auxiliary area. Production area refers to the operating area for general business system server, client (workstation) and other equipment; auxiliary area refers to the area for power supply, fire fighting, air conditions, etc. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room duty personnel, machine room, machine room security management system, duty record, machine room entry registration record, machine room entry approval records of visiting personnel.

Implementation of evaluation

a) Interview physical security responsible-person to get to know the capacities to control machine room entry and exit;

b) Interview machine room duty personnel and inquire whether the management system on machine room entry and exit is faithfully implemented and whether the personnel who enter machine room are put on record;

c) Inspect security management system of machine room and check whether there are provisions on machine room entry and exit;

d) Inspect whether machine room entrance and exit are guarded by specially-assigned person, whether there are duty records and registration records of personnel who

enter or exit machine room; inspect whether machine room has entrances or exits that are not guarded by specially-assigned persons;

e) Inspect machine room, whether there are identification measures for personnel who enter machine room, e.g. wearing visible identify recognition logo;

f) Inspect whether there are machine room entrance approval records of visiting personnel.

Result judgment

a) In evaluation implementation, if a) at least involves machine room exit and entrance management system developed, guard of specially-assigned person at machine room exit and entrance, registration of incoming personnel and identify recognition, approval for incoming personnel and range of activity restriction and monitoring, then this item is positive;

b) In evaluation implementation, if c) at least involves machine room exit and entrance management system developed, guard of specially-assigned person at machine room exit and entrance, registration of incoming personnel and identify recognition, approval for incoming personnel and range of activity restriction and monitoring, then this item is positive;

c) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Anti-theft and anti-damage (G2)

Evaluation items

a) Main equipment shall be placed in machine room;

b) Equipment or main parts shall be fixed and there shall be clear marker difficult to be removed;

c) Communication wires and cables shall be laid in shelter, e.g. underground or in pipeline;

d) Medium shall be classified for identification and stored in medium library or archives;

e) Primary machine room shall be installed with necessary burglar alarm facilities;

f) There shall be machine room and space environment monitoring system for comprehensive monitoring over machine room air conditioning, fire fighting, uninterruptible power supply (UPS), power supply and distribution, access control system and other important facilities. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, asset administrators, machine room facilities, equipment management system documents, communication line wiring document, alarm facilities installation evaluation/inspection report.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring which protective measures are taken to prevent the loss of equipment, medium, etc.;

b) Interview machine room maintenance personnel, inquiring whether placement position of main equipment is secure and controllable, whether equipment and main parts are fixed and marked, whether communication wires and cables are laid in the shelter, whether burglar alarm facilities installed in machine room are regularly inspected;;

c) Interview asset administrator, inquiring whether medium management involves classified identification and whether it is stored in medium library or archives;

d) Check whether main equipment are placed in machine room or other controllable range that cannot be easily stolen or damaged; check the fixation of main equipment or main parts of equipment, whether they cannot be easily moved or removed, whether there are clear marks that cannot be removed;

e) Check whether communication cables are laid in the shelter (e.g. laid underground or in pipeline);

f) Check whether machine room burglar alarm facilities are operating normally and check operation and alarm records;

g) Check the management of medium, whether the medium have correct classification identification, whether the medium are stored in medium library or archives;

h) Check whether there are equipment management system documents, communication line wiring documents, medium management system documents, medium list and usage records, machine room burglar alarm facilities installation evaluation/inspection report.

Result judgment

a) In evaluation implementation, if a) at least involves equipment management system, secure and controllable placement position of main equipment, fastening and marking of equipment or main parts, laying of communication wires and cables in the shelter, classification identification of medium in medium library or archives, burglar alarm facilities installed in machine room to prevent burglar and damage,

then this item is positive;

b) If a) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Lightning protection (G2)

Evaluation items

a) Machine room building shall be installed with lightning protection device;

b) Machine room shall be installed with ground wire for alternating current power supply.

Evaluation methods

Interview and inspection.

Evaluation object physical security responsible-person, machine room maintenance personnel, machine room facilities (lightning protection device, ground wire for AC power supply), building lightning protection design/acceptance document.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring w protective measures taken to prevent damage of important devices due to lightning strike, whether machine room building is installed with lightning protection device and whether it passes the inspection or technical detection by relevant national departments, inquiring whether computer power supply system of machine room is equipped with ground wire for AC power supply;

b) Interview machine room maintenance personnel, inquiring whether lightning protection device of machine room building is regularly inspected and maintained, inquiring whether computer system grounding (AC work grounding, safety protection grounding, lightning protection grounding) meets the requirements of GB50174-2008 “Design Code for Electronic Computer Room”;

c) Check whether machine room has building lightning protection design/inspection document and whether there is description on ground wire connection requirements.

Results determination

a) In evaluation implementation, a) shall at least meet lightning protection requirements of computer room in GB 50057-1994 “Design Code for Protection of Structures Against Lightning” (GB157 “Design Code for Protection of Structures Against Lightning”). In the area where there is frequent lightning is installed with surge voltage absorbing device, then this item is positive;

b) In evaluation implementation, b) requires that leading ground wire shall be insulated from steel mesh of building and various metal pipe, AC grounding resistance shall not be greater than 4Ω, grounding resistance in protected area is no greater than 4Ω; grounding resistance in lightning protection area (such area may not be provided in buildings with lightning protection facilities) is no greater than 10Ω, then this item is positive;

c) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Fire prevention (G2)

Evaluation items

a) Machine room shall be equipped with gas fire extinguishing equipment and automatic fire alarm system that have little effect on computer equipment;

b) Internal passage setting of machine room, decorative materials, equipment cables shall meet fire fighting requirements and pass fire fighting inspection. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Automatic fire alarm system design/inspection documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether there are fire fighting equipment in machine room, whether there is automatic fire alarm system, whether someone is responsible for maintaining operation of this system, whether there are management system and fire fighting plan on machine room fire fighting, whether there is fire training;

b) Interview machine room duty personnel, inquiring whether potential fire safety hazard in machine room can be timely reported and eliminated, whether there is training on use of fire extinguishing equipment in machine room and whether fire extinguishing equipment and automatic fire alarm are correctly used;

c) Check whether machine room is equipped with fire extinguishing equipment, whether placement is reasonable and whether validity period is qualified, whether automatic fire alarm system of machine room is operating normally, whether there operating records, alarm records, regular inspection records and maintenance records;

d) Check whether there are management system document on machine room fire fighting, machine room fire protection design/acceptance document, automatic fire

alarm system design/acceptance document.

Result judgment:

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Waterproof and moisture-proof (G2)

Evaluation items

a) Water pipe better does not pass through roof of machine room; preventive measures shall be taken if water pipe passes through floor;

b) Take measures to prevent rainwater penetration through machine room window, roof and wall;

c) Take measures to prevent condensation of water vapor in machine room and transfer and penetration of underground water.

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities (plumbing devices, dehumidification devices), building waterproof and moisture-proof design/acceptance documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether machine room construction takes waterproof and moisture-proof measures, whether plumbing passes through roof and moving floors and whether water pipes that pass through wall and floor are reliably protected if machine room is equipped with plumbing, whether someone is responsible for waterproof and moisture-proof matters in high-humidity areas or seasons and whether there are dehumidification devices;

b) Interview machine room maintenance personnel, inquiring whether there was water leakage or damping event, whether it is regularly checked for leakage if machine room has plumbing installation, whether there is specially-assigned person who is responsible for machine room waterproof and moisture-proof matters and dehumidification devices are used in high-humidity areas and seasons, whether preventive measures are taken timely if condensation of water vapor in machine room and underground water transfer and penetration phenomena occur;

c) Check whether machine room has building waterproof and moisture-proof design/inspection records and whether they can meet waterproof and

moisture-proof demands of machine room;

d) If there are pipes of passing through primary machine room wall and floor, check whether there are casing pipes and whether measures of sealing between pipe and casing pipe may be taken;

e) Check whether machine room roof and wall have leakage, infiltration or damp phenomena, whether machine room and the environment have obvious leakage and damping threats and whether leakage, infiltration and damp can be promptly repaired and resolved in case it occurs;

f) In high-humidity areas or seasons, check whether machine room has humidity records, whether there are humidification devices that can be operating normally, whether there are measures to prevent transfer and infiltration of machine room underground water and whether there are waterproof and moisture-proof processing records.

Result judgment

a) In implementation of evaluation, the content is not applicable if “if” conditions in d) and f) are false, then this item is not applicable;

b) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Anti-static (G2)

Evaluation items

a) Key equipment shall have necessary grounding anti-static measures.

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, anti-static design/inspection documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether machine room adopts necessary grounding anti-static measures and whether there are measures to control machine room humidity;

b) Interview machine room maintenance personnel, inquiring whether machine room humidity is regularly checked and controlled within the scope prescribed in GB2887, inquiring whether machine room has electrostatic problem or failure event caused

by static electricity;

c) Check whether machine room has anti-static design/inspection documents;

d) Check whether machine room has safe grounding, relative humidity of machine room conforms to the provisions of GB2887 and whether machine room has significant electrostatic phenomenon.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) Temperature-humidity control (G2)

Evaluation items

a) Set temperature and humidity automatic adjustment facilities, so that changes of machine room temperature and humidity are within the range allowable for equipment operating.

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, temperature and humidity control design/inspection documents, temperature and humidity records, operation records and maintenance records.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether machine room is equipped with temperature and humidity automatic adjustment facilities to ensure that temperature and humidity can meet operation requirements of computer equipment, whether machine room management system includes temperature and humidity control requirements and whether someone is responsible for this job;

b) Interview machine room maintenance personnel, inquiring whether temperature and humidity automatic adjustment facilities are regularly inspected and maintained and whether there were events that temperature and humidity impact operation;

c) Check whether machine room has temperature and humidity control design/inspection documents;

d) Check whether temperature and humidity adjustment facilities can normally operate; check temperature and humidity records, operation records and maintenance records; check whether machine room temperature and humidity meet the

requirements in GB 2887-89 “Specification for Computation Center Field”.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) Power supply (A2)

Evaluation items

a) Configure voltage stabilizer and over-voltage protection device on power supply line of machine room

b) Provide short-term backup power supply; backup power supply measures (e.g. batteries, generators, etc.) can provide power-on time of over 1 hour;

c) Important areas and important equipment of machine room provide UPS separate power supply. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

chine room facilities (power lines, voltage stabilizer, overvoltage protection equipment, short-term backup power supply), power supply security design/inspection documents, inspection and maintenance records.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether power supply lines of computer system are separated from other power supply, whether power supply lines of computer system are installed with voltage stabilizer and over-voltage protection device, whether power supply lines of computer system are installed with short-term backup power equipment (e.g. UPS) and whether power supply time meets minimum power supply demand of system;

b) Interview machine room maintenance personnel, inquiring whether voltage stabilizer, over-voltage protection device, short-term backup power equipment, etc. on power supply lines of computer system are regularly inspected and maintained, whether power supply voltage stabilization range can be controlled sot that computer system is normally operating;

c) Check whether machine room has power supply security design/inspection documents; check whether document indicates separate power supply of computer system is separate as well as the requirements of equipping voltage stabilizer, over-voltage protection device, short-term backup electrical power equipment, etc.;

d) Check power supply lines of computer and check whether power supply of computer system is separated from other power supply;

e) Inspect machine room and check whether voltage stabilizer, over-voltage protection device and short-term backup power supply on power supply line of computer system are operating normally;

f) Inspect whether there are inspection and maintenance records of stabilizer, over-voltage protection device, short-term backup power source and other electrical power equipment.

Result judgment

a) If a) ~f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

10) Electromagnetic protection (S2)

Evaluation items

a) Power lines and communication cables shall be separately laid to prevent mutual interference.

Evaluation methods

Interview and inspection.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, electromagnetic protection design/inspection documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether there are measures to prevent external electromagnetic interference and equipment parasitic coupling interference (equipment housing has good grounding, power line, communication wires and cables isolation, etc.);

b) Interview machine room maintenance personnel, inquiring whether equipment housing has good grounding, whether power lines and communication cables are isolated, whether there are any failures due to external electromagnetic interference and other problems;

c) Inspect whether there are electromagnetic protection design/inspection documents;

d) Inspect whether machine room equipment housing has safe grounding;

e) Inspect machine room wiring and check whether power lines and communication

j) Inspect software version information of network equipment regularly; (F2)

k) Establish clock synchronization mechanism of network equipment; (F2)

l) Regularly inspect and lock or revoke unnecessary user account in network equipment. (F2)

Evaluation methods

Interview, inspection and assessment.

Evaluation objects

Network administrators, boundary and important network equipment (including security equipment).

Implementation of evaluation

a) Interview network administrators and check whether there is AAA certification or other certification mode for network equipment. In case AAA server is logged in, check whether user matches administrator identity and permissions;

b) Interview network administrator, inquiring password policy of network equipment;

c) Inspect security settings of boundary and important network equipment; check whether there are settings to take appropriate measures for identification failure and there is a function to limit illegal login frequency.

d) Inspect security settings of boundary and important equipment; check whether there are restrictions on administrator login address of main network equipment; check whether there is automatic exit in case of network login connection timeout; check whether permission separation of equipment privileged users is achieved; check whether peer entities on the network are authenticated on identity;

e) Evaluate security settings of boundary and important network equipment; verify identification failure processing measures and the times that wrong passwords are used to log in network equipment; observe whether dialogue is ended; restrict illegal login times; check whether administrator login address of network equipment (e.g. using random address to log in, observing) and other functions are effective;

f) Evaluate security settings of boundary and critical network devices; verity whether the setting of automatic exit in case of network login connection timeout is effective (if there is no operation under long-time connection, observe the action of network devices);

g) Make remote login of network devices and check whether 22 ports SSH modes or other encryption modes are adopted;

h) Make penetration evaluation for boundary and important network devices; use a

variety of penetration techniques (e.g. password guessing solution, etc.) for penetration evaluation for network devices; verifying whether protective capacity of network equipment meets requirements.

i) Check inspection records and verity whether network equipment running state is inspected regularly;

j) Evaluate network devices, inquiring whether unnecessary network equipment services are closed;

k) Interview network equipment administrator, inquiring whether software version information of network equipment is regularly inspected and there are written records;

l) Interview network equipment administrator, inquiring whether there is regular inspection and lock or revocation of redundant user account in network equipment.

Result judgment

a) If password policy of network devices involves password length of more than 6 digits and password complexity (e.g. stipulating that characters shall be a mix of upper and lower case letters, digits and special characters), password life cycle, new password and old password replacement requirements (stipulating number of replaced characters) or use of token in order to facilitate memory, then b) meets evaluation requirements;

b) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

Main evaluation objects of network security evaluation are three categories of network interconnecting device, network security device and network topology results, specifically as follows:

1) Core switches, access switches, access routers, dial-up access routers and other network interconnecting devices;

2) Intrusion inspection system, firewalls and other network security devices;

3) Overall network topology results of information system.

In terms of content, implementation process of evaluation in network security level involves 6 work-units; see annex A.1.1.2 for specific contents.

7.1.1.1.3 Host security

1) Identity authentication (S2)

Evaluation items

a) Label and identify the identify of users who log in operation system and database system;

b) Identification label of operating system and database system management users shall have the feature that illegal use is not easy; static password of key system shall have more than 6 digits and are a mix of letters, number, symbols and other components and changed regularly;

c) Start login failure processing function; measures of terminating dialogues, restricting illegal logins, automatic exit, etc. may be adopted;

d) For remote management of servers through internet, necessary measures shall be taken to prevent bugging of information during network transmission process;

e) Allocate different user names to different users of operating system and database system to ensure that user name is unique.

Evaluation methods

Interview, inspection and assessment.

Evaluation objects

System administrators, database administers, important server operating system, important database management system, server operating system documents, database management system documents.

Implementation of evaluation

a) Check whether identity authentication function of server operating system and database management system have evaluation reports of second-level above or TCSEC C2 level above in “Security Technical Requirements of Classified Protection Operating System Of Information Security” and “Security Technical Requirements Of Classified Protection Database Management System Of Information Security”.

b) Interview system administrator, inquiring the measures taken to achieve identity label and authentication system of operating system;

c) Interview database administrator, inquiring the measures taken to achieve identity label and authentication system of database;

d) Inspect server operating system and database management system documents; check the attributes of guaranteeing the uniqueness of user identity authentication (e.g. user name, UID, etc.);

e) Inspect server operating system or database user and affiliated group, or whether UID is unique.

f) Inspect important server operating system and critical database management

system; check whether there are identity authentication measures (e.g. user name, password, etc.) and whether identify authentication information has the feature that illegal use is not easy; check account password policy setting, e.g. efficient password length, password complexity (e.g. stipulating a mix of upper and lower case letters, figures and special characters), short update cycle, or token is used to facilitate memory;

g) Inspect important server operating system and important database management system; check whether the function of identify failure processing is configured and whether limit value of illegal logins are set; check whether login connection timeout processing function is set, e.g. automatic exit;

h) Evaluate important server operating system and critical database management system; wrong user name and password may be used as an attempt to log in the system and verify whether identification failure processing function is effective;

i) Evaluate important server operating system and critical database management system, whether identification (e.g. setting up an account) is required first when it enters the system, while users who are not identified cannot enter system;

j) Evaluate important server operating system and critical database management system; first add anew user that is identified the same with original user (e.g. user name or UID) and check whether it exceeds.

Result judgment

a) In implementation of evaluation, if a) is positive, then evaluation implementation h) and i) are positive;

b) If e) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Access control (S2)

Evaluation items

a) Enable access control function; control access of users to resources based on security policies;

b) Achieve permissions separation of operating system and database system users;

c) Restrict access permission of default accounts; rename system default account and modify default password of these accounts;

d) Delete redundant and expired accounts in a timely manner to avoid the presence of shared accounts.

Evaluation methods

Inspection and assessment.

Evaluation objects

Important server operating system, important database management system, security policy.

Implementation of evaluation

a) Check whether discretionary access control function of server operating system and database management system have evaluation reports of second-level above or TCSEC C2 level above in “Security Technical Requirements for Classified Protection Operating System of Information Security” and “Security Technical Requirements for Classified Protection Database Management System Of Information Security”.

b) Inspect the security policies of server operating system and database management system; check whether access control of subject (e.g. user) over object (e.g. document or system device, directory list and access control table access control, etc.) in the identity of user and/or user group is defined, whether coverage includes subject (e.g. user) and object (e.g. document, database table) directly associated with information security as well as the operation between them (e.g. reading, writing or execution);

c) Inspect security policies of server operating system and database management system; checking whether it is defined that subject (e.g. user) has non-sensitive label (e.g. role) and object may be accessed based on non-sensitive labels;

d) Check the access control list of important server operation system and database management system to see whether the overdue account or useless account is included among the authorized users; whether the users in the access control list and their access rights are consistent with these in the security strategy;

e) Check the important server operation system and database management system to see whether the proprietor of subject (e.g. documents, database chart, view, storage process and trigger, etc.) or the authorized user can change the property of the corresponding access control list;

f) Check the important server operation system and database management system to see whether the access right of anonymous/default user is forbidden or strictly restricted (e.g. within the restricted scope);

g) Evaluate the important server operation system and database management system to see whether the access to subject as the unauthorized user/character is successful or not based on the security access control strategy.

Result judgment

a) If a) under the implementation of evaluation is positive, e) and g) under the implementation of evaluation are positive;

b) If b) ~g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Security audit (G2)

Evaluation items

a) The scope of audit shall cover each operational system user and database user of server;

b) The contents of audit shall include the behaviors of important users, the abnormal application of system resources and the use of important system commands;

c) The audit record shall include the date, time and category of event and the identifications of object and subject;

d) Protect the audit record to prevent it from being deleted, modified or covered unexpectedly; the duration of storage shall not be less than one month.

Evaluation methods

Interview, inspection and assessment.

Evaluation objects

Security auditor, operational system of important server, important database management system.

Implementation of evaluation

a) Interview the security auditor to ask him/her whether the security audit is set within the host system and what the requirements and strategy of the host system's selection of events which shall be audited are and what the methods to handle the audit log are;

b) Check the important server operation systems and database management systems to see whether the current scope of audit covers each user;

c) Check the important server operation system and database management system to see whether the current scope of audit covers each user, e.g. the identification of user, all the operation records of discretionary access control, the important user behaviors (e.g. the change of identification and the deletion of system table upon the commands of super-user), the abnormal use of system resources, and the use of important system commands (e.g. deletion of subject), etc.

d) Check the important server operation system and database management system to

see whether the audit record includes the date and time of event, the object and subject triggering event, the category of event, the success or failure of event, the source of the request of identification (e.g. terminal identifier) and the result of event, etc.

e) Check the important server operation system and database management system to see whether the threshold value limits of audit tracking is defined in the setting of audit tracking and whether the necessary protective measures can be adopted when the storage space is depleted, e.g. alarm and derivation, the discard of unrecorded audit information, auditing pause or the coverage of previous audit record, etc.

f) Evaluate the main server operation system and database management system to see whether the coverage of security audit is consistent with the recorded scope and conforms to the relevant requirements when some user tries to generate some significant security events in the system (e.g. failure of identification);

g) Evaluate the main server operation system and database management system to see whether the protection of security audit is consistent with the relevant requirements when some user tries to delete, modify, or cover the audit record.

Result judgment

a) If b) ~g) under the implementation of evaluation are positive during evaluation, this information system fulfills the requirements of evaluation.

4) Invasion prevention (G2)

Evaluation items

a) The operation system shall follow the minimum installation principle. Only the necessary assemblies and application programs shall be installed. The patch of system shall be repaired and updated in time through the upgrading of server and preventive maintenance of system software.

Evaluation methods

Interview, inspection and evaluation.

Evaluation objects

System administrator, main server system.

Implementation of evaluation

b) [Translator note: item a) is not existed in original text] Interview the system administrator to ask him/her whether the invasion protection measures are taken for the host system, including host operation monitoring, alarm of resources exceeding the use limits, progress monitoring, invasion detection, and integrity detection, etc.

c) Interview the system administrator to ask him/her the producer, installation, configuration and edition of invasion prevention products; ask him/her whether the configuration of products is improved or changed or updated as required (periodically or real time);

d) Check the host server system to see whether host operation monitoring is conducted, including host CPU, disk, RAM, network, and the history record of used resources shall be provided;

e) Check the host server system to see whether the alarm threshold value of resource is set (e.g. the alarm threshold value of CPU, disk, RAM or network, etc.) and whether it will trigger alarm when the used resource exceeds the regulated value and what alarm methods are;

f) Check the main server system to see whether it monitors the specific progress (including the progress of main system such as the progress of the Explorer of WINDOWS) and whether the illegal progress list can be set;

g) Check the main server system to see whether it controls the host account (e.g. system administrator) and restrict the addition and modification of important account;

h) Check the main server system to see whether it can record the IP of source of attacker, and the category, target and time of attack, etc. and whether it can alarm in case of severe invasion events (e.g. sound, message, E-mail, etc.)

i) Evaluate the main server system to see whether it can restrict the running of illegal progress if the illegal progress tries to run and whether the host can restrict the addition or modification of important account when trying to add or modify the important account;

j) Evaluate the main server system to see whether the integrity of important program under attack can be detected when trying to destroying the integrity of important program (the important program to execute the tasks of system)

Result judgment

a) If the factory is authorized (e.g. sales license) in b) under the implementation of evaluation, and the edition is new, the improvement is reasonable and the software is updated periodically, this item is positive.

b) If a) ~f) in evaluation implementation are positive, this information system fulfills the requirements of evaluation.

5) Malicious code prevention (G2)

Evaluation items

a) Install the malicious code prevention software which shall be updated in time as well

as malicious code database;

b) Support the unified management of malicious code software

Evaluation methods

Interview and inspection.

Evaluation objects

System security guard, important server system, important terminal system, network malicious code prevention products, host security design/acceptance documents

Implementation of evaluation

a) Interview the system security administrator to ask him/her whether the host system takes the real time detection and killing measures and how the detection and killing measures are configured when malicious codes attack;

b) Check the design/acceptance documents about malicious code prevention to see whether the prescribed scope of installation covers server and terminal equipment (including mobile equipment);

c) Check the important server system and terminal system to see whether the real-time malicious code detection and killing software products are installed and check the producers and edition numbers of malicious code software products and the names of malicious code databases;

d) Check the network malicious code products and their producers and edition numbers and the names of malicious code databases.

Result judgment

a) If the real-time malicious code detection and killing measures are configured in the server and important terminals in a) under the implementation of evaluation, this item is positive;

b) If a) ~c) under the implementation of evaluation are positive and it is discovered that different malicious code databases are used by the host system and network malicious code prevention products (e.g. different producers, edition numbers and the names of malicious code databases), then this information system satisfies the requirements of evaluation items of this unit.

6) Resource control (A2)

Evaluation items

a) Restrict the login of terminal through the setting of the terminal connection methods and the scope of network address, etc. to;

b) Set the login terminal overtime operation locking based on the security strategy;

c) Restrict the maximum or minimum limit of single user to use the system resources.

Evaluation methods

Inspection, evaluation.

Evaluation objects

Operational system of important server.

Implementation of evaluation

a) Check the important server operation system to see whether it restricts the number of multiple concurrent dialogues of single user and whether the terminal login is restricted through the setting of the terminal connection mode and the scope of network address;

b) Evaluate the important server operation system to verify whether the number of dialogues of single user is restricted through randomly selecting a user to log in the server and try to send out concurrent dialogues;

c) Evaluate the important server operation system to verify whether the operation system of server restricts the terminal login through the restriction of terminal connection methods or the scope of network address when a randomly selected user account logs in the server through different terminal connection methods and network address;

d) On-line inspection: whether host operation system, database and important application system set the overtime terminal login locking according to the security strategy.

Result judgment

a) If a) ~d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The key host security evaluation system includes the operation systems of network server, application server and database server and from the aspect of contents, the security of system is involved with 6 work-units. Please refer to Annex A.1.1.3 for details.

7.1.1.1.4 Application security

1) ID Identification (S2)

Evaluation items

a) Provide the login control module to identify the ID of logging user.

b) Provide the functions of user ID uniqueness inspection and identification information complexity inspection to ensure there are no repeated user identifications in the application system and the user identification information cannot be used illegally;

c) Provide the function to handle the failure of login, measures such as end of dialogue, restriction of illegal login times and automatic exit can be adopted;

d) Enable the functions of user identification, user ID uniqueness inspection, user identification information complexity inspection and login failure handing and set the relevant parameters according to the security strategy.

Evaluation methods

Interview, inspection and evaluation.

Evaluation objects

System administrator, important application system, overall planning/design documents.

Implementation of evaluation

a) Interview the system administrator to ask him/her whether the user identification measures are taken and what the specific measures are; what measures that system adopts to prevent user identification information being used illegally (e.g. the mixture of capital or small letters, number and special characters or the setting of command cycle, etc.)

b) Check whether the application system has user management module and whether the system has compulsory requirements on the intensity of user account and password;

c) Interview the system administrator to ask him/her whether the application system is equipped with function to handle the login failure and how it is handled;

d) Interview the system administrator to ask him/her whether the user identification of application system is unique (e.g. the ID, user name or other information is unique in the system and this identification can only identify this user)

e) Check the overall planning/design documents to see whether the system adopts a unique identification (e.g. user name, ID or other properties)

f) Check the important application system to see whether it has the function of user identification (e.g. establish account) and distinguish (e.g. password); check whether the identification information may be used illegally, e.g. complexity (e.g. capital or small letters, number and special characters shall be mixed as required) or token used to make it easy for memory;

g) Check the important application system to see whether it is equipped with and uses the function to handle the failure of login (e.g. if the times of login exceed the set

limit, system will exit automatically, etc.)

h) Evaluate the important application systems to verify whether the handling of login failure, the time limit of illegal login and the automatic exit due to overtime login connection are effective;

i) Evaluate the application system to see whether the login password is set as the unified original password and whether it has the function of suggesting the modification of original password.

Result judgment

a) If the relevant documents in c) under the implementation of evaluation specify the unique identification of user, this item is positive.

b) If d) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Access control (S2)

Evaluation items

a) Provide the access control function and control the user access to documents or database based on the security strategy.

b) The coverage scope of access control shall include the subject and object related to resource access and the operation between subject and object;

c) Authorize the subject to configure the access control strategy and strictly restrict the access right of default user;

d) For different accounts, authorize them the minimum right enough to finish the tasks it bears and create the interaction between them;

e) The production system shall establish the relation chart between account and right limit. (F2)

Evaluation methods

Interview, inspection and evaluation.

Evaluation objects

System administrator, important application system.

Implementation of evaluation

a) Interview the system administrator to ask him/her whether the business system can provide access control measures and what the specific measures are and how the discretionary access control granularity is;

b) Check the important application system to see whether it provides access control mechanism and whether the user access to the subject is controlled according to the security strategy (e.g. data of documents or database)

c) Check the important application system to see whether the coverage scope of its discretionary access control includes the subject or object directly related to information security and the operation between them; whether the discretionary access control granularity reaches the subject as subscriber stage and the object as document and database stage (e.g. database chart, view, storage process, etc.);

d) Check the important application system to see whether it conducts the systematic functional operation to the authorized subject and has the function to set the data access right.

e) Check the important application system to see the right limit of its privileged user is separated (e.g. the separation of right limits of system administrator, security supervisor and auditor) and whether the right limits are interacted;

f) Check the important application system to see whether it has the function to restrict the access of default user and whether it allocated for application;

g) Evaluate the important application system to see whether the right limits are restricted by the application system through the login of users with different right limits and verify whether the function of system right separation is valid;

h) Evaluate the important application system to verify whether the user right management function is effective through the systematic functional operation and data access of the specific user set by the authorized user and then the login of this user;

i) Evaluate the important application system to verify whether the restriction to the access rights of default user is effective through the login and operation (including legal and illegal operations) of the default user (default password).

Result judgment

a) If b) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Security audit (G2)

Evaluation items

a) Provide the security audit function covering each user and audit the significant security events which have great impact on the application system;

b) Do not provide the function to delete, modify or cover the audit record;

c) The contents of audit record shall at least include the date and time of event,

information of initiator, category, description and result, etc. which shall be stored for at least one month.

Evaluation methods

Interview, inspection and evaluation.

Evaluation objects

Auditor, important application system.

Implementation of evaluation

a) Interview the security auditor to ask him/her whether the application systems are set with security audit; ask him/her what requirements and strategies that the application systems have for the audit of events and what methods are used to handle the audit log;

b) Check the important application systems to see whether the current scope of audit covers each user;

c) Check the important application system to see whether the audit strategy covers the significant security events within the system, e.g. user identification, all the operational records of discretionary access control, important user behaviors (if super-user command to change the identification of user, delete system table), the application of important system orders (e.g. delete object), etc.

d) Check the important application systems to see whether the audit record includes the data and time of event, the subject and object which trigger the occurrence of events, the category of event, the failure or success of event, the source of request for ID identification (e.g. tag of terminal), the result of event, etc.;

e) Check the important application systems to see whether the limit of audit tracking threshold value is defined, and whether necessary protective measures can be taken in case of the depletion of storage space, e.g. alarm and derivation, the discard of unrecorded audit information, audit pause or the coverage of previous audit record, etc.

f) Evaluate the important application system to verify whether the audit function is under protection through the illegal termination of audit function or the modification of its configuration;

g) Evaluate the important application system to see whether the coverage and record of security audit fulfills the requirements when some users try to create some important events related to system security (e.g. failure of identification);

h) Evaluate the important application systems to see whether the protection of security audit fulfills the requirements when some system users try to delete, modify or cover the audit records.

Result judgment

a) If b) ~h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Integrity of communication (S2)

Evaluation items

a) Apply the check code technology to ensure the integrity of data during communication.

Evaluation methods

Interview, inspection and evaluation.

Evaluation objects

Security guard, design/acceptance documents, important application system.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether the operation to ensure the integrity of data during transmission is provided and what the specific measures are;

b) Check the design/acceptance documents to see whether the instructions on the integrity of communication are specified; if specified, check whether the system judges the validity of data pack sent from the other side through the check code;

c) Evaluate the important application system to see whether there is the check code through obtaining the data packs of both sides.

Result judgment

a) If b) ~c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Communication confidentiality (S2)

Evaluation items

a) Before the establishment of mutual communication, the application system shall use the cryptology to conduct the initialization verification to the dialogue.

b) Encrypt the sensitive information during communication.

Evaluation methods

Interview, inspection and evaluation.

administrator, system administrator and database administrator.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, documents on staff configuration, name list of management staff

a) Interview the security supervisor to ask him/her the configuration of security management posts (consult him/her based the post duty documents, including machine room administrator, system administrator, database administrator, network administrator, security guard, etc.) including quantity, full-time or part-time, etc.

b) Check the relevant documents on the configuration of staff to see the post division and work shifting conditions (including work shift cycle, work shift procedure) and check whether the security management staffs shall be configured including machine room administrator, system administrator, database administrator, network administrator, and security guard, etc.

c) Check the post division list and whether machine room administrator, system administrator, database administrator, network administrator, and security administrator are clarified and confirm whether security administrator takes the additional duties of network administrator, system administrator, or database administrator.

Result judgment

a) If there is no security administrator who takes the additional duties of network administrator, system administrator, or database administrator in a) under the implementation of evaluation, this item is positive;

b) If a) ~c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Authorization and approval (G2)

Evaluation items

a) Authorize the right of approval to the department or staff based on the duties of each department or post to review and approve the key activities, such as, system operation, network system connection and the access of important resources;

b) Establish the approval procedure targeted to the key activities which shall be confirmed through the signature of approver.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, approver of key activities, approval item list, approval documents

Implementation of evaluation

a) Check whether the key activities of information system are approved or not;

b) Check the approval of key activities (e.g. the access of important resources such as network system, application system, database management system and important server and equipment, and the formulation and issuance of important management systems, the configuration and training of staff and the procurement of products, etc.)

c) Check the approval list to see whether the approval items, approval departments, approver and approval procedure are specified clearly;

d) Check the approved documents to see whether the approver or the approval department is granted with the right of approval.

Result judgment

a) If a) ~d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Communication and cooperation (G2)

Evaluation items

a) Reinforce the cooperation and communication between administrators and organizational structures and internal functional departments on information security.

b) Reinforce the cooperation and communication with relevant organizations, public security institutions and telecom companies.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, security management staffs, meeting records, description documents of outsource organizations.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether he/she often contacts with

relevant organizations, public security institutions and telecom companies and what the contact information is and what the contents of cooperation with these institutions or departments are, and how to communicate and cooperate with them;

b) Interview the security supervisor to ask him/her whether he/she convenes meetings to coordinate different departments or organizes the relevant staff to assist in the handling of security problems and whether the security management institution convenes the internal security meetings on the configuration of security works and which department and who are participated and how the meetings come out;

c) Interview the security administrator (selected from system administrators and security guards) to ask him/her how or what he/she communicates with the staff of other departments or within the organizational structure or the administrators within each internal department;

d) Check the security meeting documents or records on the coordination of different departments and check whether the contents, time, participated staff and conclusion of meeting are specified;

e) Check the security meeting documents or records to see whether the contents, time, participated staff and conclusion of meeting are specified;

f) Check the description documents of outsource-organizations to see whether public security institutions, telecom companies and relevant companies are included and whether the contactors and contact information of outsource organizations are specified.

Result judgment

a) If a) ~f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Audit and inspection (G2)

Evaluation items

a) Security administrator shall conduct periodic security inspection including the inspection of system's routine operation, system loopholes and data back-ups, etc.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, security guard, security inspection records.

Implementation of evaluation

a) Check whether he/she organizes the staff to conduct periodic security inspection to information system and how long the inspection cycle is and whether the contents of inspection are clarified;

b) Check the inspectors and whether the inspection procedure conforms to the relevant strategy and requirements and how the inspection comes out;

c) Check the security inspection records to see whether the record time is consistent with the inspection cycle and whether there are descriptions on the inspection, inspectors and conclusion in the documents.

Result judgment

a) If a) ~c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The evaluation objects of security management institution are the documents or records related to the setting of post, configuration of staff, authorization and approval, communication and cooperation and investigation and inspection. Please refer to Annex A.1.2.2 for details.

7.1.1.2.3 Personnel security management

1) Personnel Employment (G2)

Evaluation items

a) Appoint or authorize the special department or person in charge of staff employment;

b) Regulate the employment procedure and conduct an investigation to the ID, background and qualification of the employed staff and conduct an assessment to his/her technical skills;

c) Sign the confidentiality agreement with the staff who works in the important post;

d) Conduct the recording management to information security administrator. The configuration or replacement of information security administrator shall be reported to the superior department for filing; for the information administrator working in the headquarters of financial institution, the configuration or replacement shall be filed in the technical department of headquarters. (F2)

e) Anyone who has been penalized or punished due to the violation of the relevant national laws and regulations or the regulations of financial institution shall not be engaged in the information security management work. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Responsible-person for human resource, human resource staff, employment management documents, employer investigation documents or records, assessment documents or records, confidentiality agreement.

a) Interview the responsible-person for human resource to ask him/her what the specific requirements on the employment of staff are and whether the employed security management and technical staff are capable to complete the tasks under the scope of duties;

b) Interview the human resource staff to ask him/her whether the ID, background, qualification of the employed staff are investigated before official employment and whether the confidentiality agreement is signed with him/her and whether the duties of work is informed to him/her;

c) Check the employment management documents to see whether the employed staff is qualified to the job, e.g. education background, academic degree; for technical staff, the relevant level of technical skills shall be acquired and for the management staff, the security management knowledge shall be acquired;

d) Check whether there are the documents or records on the investigation to the ID, background, qualification of the employed staff and check whether the contents and conclusion of investigation are recorded;

e) Check the documents or records on the technical skill assessment to see whether the contents and conclusion of assessment are recorded;

f) Check the confidential agreement to see whether the scope and responsibilities of confidentiality, and the responsibilities for breach of agreement and the valid period are specified and the signature of responsible-person is attached.

Result judgment

a) If a) ~f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Staff leave-post (G2)

Evaluation items

a) The leave-post procedure shall be regulated and all the access rights of the staff who leaves the job shall be terminated in time;

b) Various ID cards, keys and emblems and hardware and software provided by the institution shall be taken back;

c) Handle the leave- or transfer-post procedure strictly in accordance with the regulations and ensure the password of the information technical system under the

charge of the staff who leaves the job shall be changed immediately.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, human resource staff, security handling records, confidentiality commitment documents.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether the access right of the staff who leave the job is terminated and whether various ID cards, keys, emblems and hardware and software provided by the institution are taken back;

b) Interview the human resource staff to ask him/her what the leave- or transfer-job procedure is and whether the leave- or transfer-staff is required to sign the confidentiality agreement before departure;

c) Check whether there are security disposition records about the staff who leaves the job, e.g. the registration record about ID cards and of equipment that he/she submits;

d) Check whether there is the signature of the leave- or transfer-job staff in the confidentiality commitment documents.

Result judgment

a) If a) ~d) are positive in the implementation of evaluation, then this information system satisfies the requirements of evaluation items of this unit.

3) Staff assessment (G2)

Evaluation items

a) Conduct the periodic assessment on the security skills and conscientiousness of the staff of each post.

Evaluation methods

Interview.

Evaluation objects

Security supervisor, human resource staffs.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether the periodic assessment on the security skills and knowledge of staff of each post is conducted;

b) Interview the human resource staff to ask him/her the conditions of assessment, how long the assessment cycle is and what the contents of assessment are; ask him/her the conditions of security inspection of the staff and what the contents of inspection are (e.g. operational behavior, social relation, and social activities, etc.) and whether the contents are complete;

c) Interview the human resource staff to ask him/her what disciplinary measures are taken to the staff who violates the security strategy and regulations.

Result judgment

a) If the interviewed staff says about social relation, social activities and operational behaviors in b) under the implementation of evaluation, this item is positive;

b) If what the interviewed staff describes in c) under the implementation of evaluation is consistent with what the documents say, this item is positive;

c) If a) ~c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Security consciousness education and training (G2)

Evaluation items

a) Formulate the security and training program;

b) Conduct the security, technical and other relevant trainings to all the staff;

c) Conduct the information security training to information security administrators for at least one time per year; (F2)

d) Inform all the staff of the security responsibilities and punishments; for the person who violates the security strategy and regulations, disciplinary action will be taken.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, security guard, system administrator, network administrator, training plan, training records.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether the security education and training are conducted to each staff according to the education and training program

and how the education and training are conducted and what the effects are;

b) Check the systems and records related to the security responsibilities and disciplinary actions;

c) Check the security education and training program documents to see whether the purpose, mode, object, contents and time and place of training are specified and whether the contents of training include the basic knowledge about information security and post operation procedure, etc.

d) Check whether there are the records on the security education and training and whether there is description on the trained staff and the contents and conclusion of training in the record; check whether the record is consistent with the training program.

Result judgment

a) If the interviewed staff can describe clearly about the asked problems and the security responsibilities, disciplinary actions and post operation procedure he/she says are consistent with the descriptions in the documents, this item is positive;

b) If a) ~d) in evaluation implementation are positive, this information system satisfies the evaluation requirements of this organization.

5) Outsider access management (G2)

Evaluation items

a) Each institution shall appoint the responsible department to take the charge of the approval of outsiders who do not work in the fields of computer system and network. The outsider shall be accompanied by the designated staff during the whole visit. The visit shall be registered for filing;

b) All the institutions or persons who obtain the access authorization shall sign the security confidentiality agreement with the financial institution and shall not add, delete, modify or check data without authorization or copy or disclose any information about the financial institution; (F2)

c) Outsider shall submit the contents of planned operations before entering in the financial institution to conduct on-site operation; the staff of financial institution shall be accompanied with the outsider and verify the contents of operation. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, security administrator, security responsibility or confidentiality agreement, third party access management documents, registration records.

Implementation of evaluation

a) Check what management measures are taken to the third party visit (e.g. system software or hardware maintainer who provides service for system, business partner, evaluator, etc.) and whether the third party is required to sign the security responsibility or confidential agreement before visiting;

b) Interview the security administrator to ask him/her what measures are taken to the third party who will visit the important area (e.g. host machine room, etc.) and whether the third party can visit until obtaining the approval of the relevant responsible-person and whether he/she is accompanied by the designated staff during the whole visit and whether his/her visit is recorded and filed;

c) Check the security responsibility or confidentiality agreement to see whether the scope and responsibilities of confidentiality, the responsibilities for breach of contract, and the valid period of agreement are specified and the signature of the responsible-person is attached;

d) Check the third party access management documents to see whether the third party visiting to some important areas is approved by the relevant responsible-person according to the relevant regulations;

e) Check the registration records on the third party visit to the important area to see whether the record describes the time of visitor entering in and departing the important area, the visited area and the accompanied staff;

f) Check whether all the institutions or persons who obtain the outsider visit authorization have signed the information security or confidentiality agreement with the financial institution and whether he/she adds, deletes, modifies or checks data without authorization or copies or discloses any information about the financial institution.

Result judgment

a) If a) ~f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The objects of personnel security management evaluation are the documents and records about 5 control points, i.e. employment, departure, performance evaluation, security education and training, and outsider access management. Please refer to Annex A.1.2.3 for details.

7.1.1.2.4 System construction management

1) System-level (G2)

Evaluation items

a) Clarify the boundary of information system and security protection class;

b) Describe the reasons and methods to classify an information system as some security protection class in the written form;

c) Ensure the class of information system is approved by the relevant agency.

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, system division documents, system-level documents, system property documents.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether the methods to divide and classify the security protection class of information system conform to the classification regulations, and whether the division and classification are specified in details; whether the classification is approved by the relevant agency (e.g. superior relevant agency);

b) Check the documents on the division of system to see whether the documents specify the reasons and methods for the division of information system;

c) Check the system-level documents to see whether the security protection class of information system and SxAyGz values composed of security protection class are specified in the documents, and whether the class is approved with the signature of the relevant agency;

d) Check the system property documents to see whether the mission, business, network, hardware, software, data, boundary and staff are specified clearly in the documents.

Result judgment

a) If there is no superior department in a) under the implementation of evaluation but the approval of security supervisor, this item is positive;

b) If a) ~e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Security program design (G2)

Evaluation items

a) Select the basic security measures based on the security protection class of system and supplement and adjust the security measures based on the results of risk analysis;

b) Specify the requirements, strategy and measures on the security protection of system in the written form which is developed into the security program of system;

c) The security program shall be specified in more details to develop into a detailed program design for the construction of security system and the procurement and use of security products;

d) Organize the relevant agency and security experts to evaluate and demonstrate the rationality and validity of security program design which can be officially implemented upon approval.

Evaluation methods

Interview and inspection.

Evaluation objects

Responsible-person of system construction, security plan, detailed design plan, expert assessment documents.

Implementation of evaluation

a) Interview the responsible-person of system construction to ask him/her whether the basic security measures are taken based on the security level of system and whether the security measures are added or adjusted based on the results of risk analysis and what these adjustments are;

b) Interview the responsible-person of system construction to ask him/her whether the system security program is formulated and the specific program design to guide the construction of security system and the procurement of security products is formulated based on the security program and whether the relevant agency and security expert are organized to evaluate the security design program and whether the security design program is approved by the security supervisor or management;

c) Check the security program of system to see whether the security protection requirements and security strategy of system are specified in details as well as the corresponding security measures that system takes;

d) Check the system's detailed program design to see whether the security program is specified in details and whether there are programs on the security construction and the procurement of security product; whether the program is approved with the signature of security supervisor or the leader of management department;

e) Check the documents on the experts' conclusion to see whether there are the evaluation opinions of the relevant agency or security expert on the security

program design.

Result judgment

a) If a) ~e) in the implementation of evaluation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Procurement and use of products (G2)

Evaluation items

a) Ensure the procurement and use of security products conform to the relevant national regulations;

b) Ensure the procurement and use of cipher code products conform to the requirements of the state cipher code administration;

c) Designate or authorize the special department in charge of the procurement of products;

d) The procurement of security products for scanning or detection shall be submitted to the technical department within its institution for approval and filing; (F2)

e) The information security products for scanning or detection are only limited to be used by the information security administrators within its institution or by the network administrator with the authorization of leader; (F2)

f) Check the logs and report messages and summary analysis related to the information security products periodically; in case of significant problems, emergency measures shall be taken immediately and the report of significant problems shall conform to the procedure; (F2)

g) Back-up and file various logs and report messages generated due to the information security products; (F2)

h) Upgrade and maintain the information security products in time; the handling of the information security products which are expired or cannot be used continuously shall conform to the fixed asset retirement approval procedure. (F2)

Evaluation methods

Interview and inspection.

Evaluation objects

Security supervisor, responsible-person of system construction, information security products.

Implementation of evaluation

a) Interview the security supervisor to ask him/her whether there is a designated department in charge of the procurement of products and which department is in charge;

b) Interview the responsible-person of system construction to ask him/her the information about the procurement of information security products and whether the procurement is in accordance with the procurement list and how the procurement procedure is controlled;

c) Interview the responsible-person of system construction to ask him/her whether cipher products are adopted for system and whether the use of cipher products conforms to the requirements of the state cipher code administration;

d) Check whether the information security products used by the system (boundary security equipment, important server operation system, database, etc.) conform to the relevant national regulations;

e) Check whether the use of cipher products conforms to the relevant regulations on the use and management of cipher code products, e.g. “Regulation on the Administration of Commercial Cipher Codes” specifies that each organization can only use the commercial cipher code products which have been approved by the state cipher code administration. If failure occurred to the commercial cipher code products, the organization which is designated by the state cipher code administration shall be invited for maintenance. The discarded cipher code products shall be reported to the state cipher code administration for filing.

Result judgment

a) If c) interview explanation under the implementation of evaluation does not involve encryption products, then evaluation implementation c) and e) are not applicable;

b) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Independent software development (G2)

Evaluation items

a) Develop software development management system; provide a clear description of development process control method and code of staff conduct;

b) Ensure that development environment and actual operating environment are physically separated;

c) Ensure that development personnel and testing personnel are different; testing personnel may not serve as system administrators or business operators; ensure that test data and testing results are under control; (F2)

d) Ensure providing relevant documents on software design and operating guide,

which are kept by a specially-assigned person.

Evaluation modes

Interview and inspect.

Evaluation objects

System construction responsible-person, relevant documents on software design and operating guide, document use and control records.

Implementation of evaluation

a) Interview system construction responsible-person; inquire whether system independently develops software, whether independent development has appropriate control measures, whether it is prepared, debugged and completed in independent simulation environment;

b) Interview system construction responsible-person; inquire whether system development document is kept by a specially-assigned person, who is this person and how it is controlled and used (e.g. restricting the scope of users and making registrations on use, etc.);

c) Inspect whether there are relevant documents on software design (application software design program file, source code document, etc.) and software operating guide or operating manual or maintenance manual, etc.

d) Check whether software development environment and system operating environment are physically separated;

e) Check whether there are use and control records of system development documentation.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Outsourcing software development (G2)

Evaluation items

a) Detect software quality in accordance with development requirements;

b) Detect possible malicious codes in software package before software installation;

c) Ensure providing relevant document on software design and operating guide;

d) Regularly audit and evaluate outsourcing service activities and service capability of outsourcing service provider; (F2)

e) Require development organization to provide software source code and review possible backdoor in software;

f) Require outsourcing service provider to retain operating traces and record complete logs; relevant contents and storage life shall meet the demands for event analysis, security forensics, independent audit and supervision inspection; (F2)

g) Prohibit transfer by outsourcing service provider and strictly control subcontracting to ensure outsourcing service level; (F2)

h) Develop data center outsourcing service contingency plan and supplier alternative scheme to cope with service interruption or reduction in service level due to bankruptcy of service provider, force majeure or other potential problems and to support continuous and reliable operation of data center. (F2)

Evaluation modes

Interview and inspect.

Evaluation objects

System construction responsible-person, software development security protocols, software development document.

Implementation of evaluation

a) Interview system construction responsible-person; inquire whether there is written document (e.g. software development security protocol) to standardize the responsibilities of software development organization, safety behavior during development process, development environmental requirements, software quality and other related contents before software outsourcing, whether there is independent daily maintenance of software and use of documents required;

b) Interview system construction responsible-person; inquire whether there is acceptance test on software function, performance, etc. in accordance with technical parameters of development protocol; acceptance detection is jointly carried out by the developer and responsible-person; whether malicious codes in software are detected before software installation, whether detection tools are commercial products of a third-party;

c) Inspect whether software development protocol provides intellectual property ownership, security behavior and other contents;

d) Inspect whether there is demand analysis specification, software design specification, software operation manual and other development documents.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system

satisfies the requirements of evaluation items of this unit.

6) Engineering implementation (G2)

Evaluation items

a) Designate or authorize special departments or personnel to be responsible for the management of Engineering implementation process;

b) Develop detailed engineering construction scheme and relevant process control document and control engineering implementation process.

Evaluation modes

Interview and inspect.

Evaluation objects

System construction responsible-person, agreement on security construction of project, implementation plan of project.

Implementation of evaluation

a) Interview system construction responsible-person; inquire whether project implementing behavior of engineering construction party is constrained in written form (e.g. agreement on security construction of project);

b) Interview system construction responsible-person; inquire whether specially-assigned personnel or department carries out schedule and quality control over implementation process of project in accordance with the requirements of Engineering implementation scheme;

c) Inspect security construction agreement of project; check whether the contents cover the responsibilities of project implementing party, task requirements, quality requirements and other aspects, which constrain project implementing party;

d) Inspect Engineering implementation plan; check whether the contents cover engineering time limit, schedule control, quality control, etc.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Evaluation and inspection (G2)

Evaluation items

a) Conduct security inspection test for system;

b) Develop acceptance inspection scheme in accordance with design program or contract requirements before acceptance inspection; record acceptance inspection results in detail in acceptance inspection process and form acceptance inspection report;

c) Organize relevant agency and relevant personnel to examine system acceptance inspection report and sign to confirm;

d) For testing carried out in production system, it is necessary to develop detailed plans on system and data backup, testing environment construction, system and data recovery after testing, production system audit, etc. to ensure the security of production system. (F2)

Evaluation modes

Interview and inspect.

Evaluation objects

System construction responsible-person, system evaluation scheme, system evaluation records, system evaluation report, system inspection report.

Implementation of evaluation

a) Interview system construction responsible-person; inquire whether information system receives independent security evaluation in accordance with design program or contract requirements before formal operation of information system;

b) Interview system construction responsible-person; inquire whether there is documentation requirement for evaluation process (including pre-evaluation, during-evaluation and post-evaluation), whether relevant agency or personnel are organized to examine compliance based on design program or contract requirements;

c) Inspect engineering evaluation program; check whether there are requirements for evaluation department, personnel and field operation process; check whether evaluation records evolve evaluation time, personnel, field operation process, evaluation results and other aspects in detail; check whether evaluation report presents problems and improvements, etc.;

d) Inspect whether there is system inspection report.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) System delivery (G2)

Evaluation items

a) Develop system delivery list and make an inventory based on equipment, software and documents stated in delivery list;

b) System construction organization shall deliver all system construction documents and system operation and maintenance documents to technical department after construction task is completed;

c) External construction organization sign relevant intellectual property protection agreement and confidentiality agreement with financial institutions and may not disclose key security technical measures and core security functional design; (F2)

d) Have appropriate training for technical personnel on system operation and maintenance.

Evaluation modes

Interview and inspect.

Evaluation objects

System construction responsible-person, system delivery list, letter of service commitment, training records.

Implementation of evaluation

a) Interview system construction responsible-person; inquire what the hand-over procedures are, whether hand-over work is handled in accordance with this procedure, whether inventory of hand-over equipment, documents and software, etc. is made based on delivery list, whether hand-over list meets relevant requirements in contract;

b) Interview system construction responsible-person; inquire whether current information system is independently maintained by internal personnel, whether system constructing party has training for operation and maintenance technical personnel and what the training involves; if it is so, whether there is written commitment to technical support services for system operation and maintenance, whether the system includes document that supports its independent operation and maintenance;

c) Inspect system delivery list; check whether it contains names of system construction document (e.g. system construction program), document of guiding users on system operation and maintenance (e.g. server operation instructions), system training manual, etc.;

d) Inspect whether there is letter of service commitment from system constructing party and training record for system.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) Security service provider selection (G2)

Evaluation items

a) Evaluate the qualifications, conduct of operations, performance, service system, service quality and other factors during selection of information security service provider; (F2)

b) Ensure the selection of security service provider conforms to relevant national provisions;

c) Sign security related agreement with selected security service provider to clearly prescribe related responsibilities;

d) Ensure that selected security service provider provide technical training and service commitment and sign service contract if necessary.

Evaluation modes

Interview.

Evaluation objects

System construction responsible-person

Implementation of evaluation

a) Interview system construction responsible-person; inquire whether security service organization that provides information system security planning, design, implementation, maintenance, evaluation and other services conform to relevant national provisions.

Result judgment

a) If a) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

Evaluation objects of system construction management mainly involve the documents and work records related to 9 control points of system-level, security program design, product procurement, independent software development, outsourcing software development, Engineering implementation, evaluation inspection, system delivery and selection on security service provider. See annex A.1.2.4 for specific contents.

7.1.1.2.5 System operation-maintenance management

1) Environmental management (G2)

Evaluation items

a) Establish machine room security management system, stipulating machine room security access, material carrying-in and out of machine room, environmental security of machine room, etc.;

b) Machine room shall adopt structured wiring system; if wiring equipment cabinet inside has coil holder, jumper wires shall be neat and jumper wire and distribution frame shall be uniformly numbered and clearly marked; (F2)

c) Designate a department for machine room security; specially assign a person to serve as machine room administrator who manages machine room access, regularly inspects machine room operation state, maintains machine room power supply and distribution, air conditioning, temperature and humidity control facilities and fill in machine room duty record and inspection record;

d) Personnel in and out of machine room must have the document issued by competent agency; (F2)

e) Machine room administrator shall receive relevant training and master the essential points of operation for various types of equipment in machine room; (F2)

f) Regularly maintain machine room facilities and strengthen the maintenance of equipment or components that wear rapidly or failure-prone; (F2)

g) Machine room entrance and exit shall be installed with 24/7 video surveillance facilities and the video shall be kept for at least one week; (F2)

h) Machine room shall be equipped with weak current well and has room for expansion; (F2)

i) Strengthen the management on office environment confidentiality, including that the staff shall immediately return office key once being transferred out of office and may not receive visitors in office area, etc.

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room security management system, machine room entry and exit registration table.

Implementation of evaluation

a) Interview physical security responsible-person; inquire whether basic facilities (e.g.

air conditioning, power supply and distribution equipment, etc.) in machine room are regularly maintained, which department/who is responsible and how long maintenance cycle is;

b) Interview physical security responsible-person; inquire whether the designated person is responsible for machine room security management and whether machine room entrance and exit management is required to be institutionalized and documented;

c) Interview physical security responsible-person; inquire whether appropriate measures are taken to ensure the confidentiality of office environment, e.g. power recovery after post-removal of personnel;

d) Inspect machine room security management system; inquire whether the contents cover physical access to machine room, material carrying in and out of machine room, machine room environmental security, etc.;

e) Inspect machine room registration form; check whether it records in-out time of visitors, names and access reasons, etc.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Asset Management (G2)

Evaluation items

a) Prepare a list of asset related to information system, involving asset responsibility department, importance, location, etc.;

b) Establish asset security management system, stipulating responsible-person or responsible department for information system asset management and standardizing asset management and use.

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, asset administrator, list of asset, asset security management system, equipment.

Implementation of evaluation

a) Interview security supervisor; inquire whether responsible-person or department for asset management is designated and which department/person is responsible for it;

b) Interview physical security responsible-person; inquire whether asset management is required to be documented;

c) Interview asset administrator; inquire whether there is asset assignment or identity management based on importance of asset and whether different types of asset have different management measures;

d) Inspect list of asset; check whether the content covers asset responsible-person, level, location, department, etc.;

e) Inspect asset security management system; inquire whether requirements on responsible department, responsible-person, etc. on asset management are defined;

f) Inspect the equipment in list of asset; check whether it has appropriate identification.

Result judgment

a) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Medium management (G2)

Evaluation items

a) Ensure that the medium is stored in a secure environment; control and protect various types of medium and make storage environment managed by a specially-assigned person;

b) All data backup medium shall be stored in anti-magnetic, moisture-proof, dust-proof, high temperature-proof anti-extrusion environment; (F2)

c) Register medium arching and inquiries; administrators shall make periodic inventories in accordance with directory of archived medium;

d) Important paper documents shall follow borrow registration system; without the approval by relevant agency head, no person is allowed to lend, copy or publicize the document; electronic documents shall be under parallel management of OA and other electronic office platform for approval;

e) For the medium to be repaired outside, first remove the sensitive data to prevent unauthorized leakage of information;

f) For destruction of storage medium of containing sensitive information, report to relevant agency for the record and have it destructed by technical department through information elimination, demagnetization or physical smashing and make destruction records. Information elimination only applies to the circumstances that storage medium will be still used in financial institutions, otherwise there will be unrecoverable destruction for information; (F2)

g) Prepare technical document based on an uniform format and timely update to meet the requirements that technical document may be used to recover normal operation of system; (F2)

h) Develop mobile storage medium use specification and regularly verify the use of removable storage medium; (F2)

i) Classify the medium and carry out identification management in accordance with the importance of carrying data and software;

j) Periodically verity the recover of main backup business data and timely transfer the storage based on service life of medium. (F2)

Evaluation modes

Interview and inspect.

Evaluation objects

Asset administrator, medium management record, various medium.

Implementation of evaluation

a) Interview asset administrator; inquire whether there are protection measures in medium storage environment to prevent from being stolen, destroyed, revised without authorization and illegal disclosure of information and whether there is specially-assigned person for management;

b) Interview asset administrator; inquire whether medium use and management is required to be documented, whether current use of medium is regularly inspected based on directory of medium and whether there is medium classification and identity management;

c) Interview asset administrator; inquire whether there is security handling before medium are repaired or destructed (e.g. clearing the sensitive data);

d) Inspect medium management record; check whether there are records on medium storage, archiving, borrowing, etc.;

e) Inspect medium; check whether medium are classified and have different identification.

Result judgment

a) If a) in implementation of evaluation involves measures on fire fighting, water proof, prevention of burglary, then this item is positive;

b) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Equipment management (G2)

Evaluation items

a) Establish equipment security management system based on declaration, approval and special assigned responsible-person, standardize model selection, procurement, distribution and receiving processes of various software and hardware equipment of information system;

b) Standardize the management on operation and use of terminal computer, workstation, portable machines, systems, network and other equipment; carry out start/stop, power on/off and other operations of main equipment (including backup and redundant equipment) based on operation specification;

c) Newly purchased equipment shall be tested and pass the test before being put into use; (F2)

d) Technical departments of organizations are responsible for maintenance management of various information related equipment (including backup and redundant equipment) and lines, etc. (F2)

e) Make equipment registration; develop equipment management practices; implement security protection responsibility of equipment users; (F2)

f) Equipment that are discarded shall be disposed by technical department to remove data information; if discarded equipment are no longer used or deployed to the organizations other than financial institution, technical departments shall make unrecoverable handling of data information storage equipment through demagnetization, physical smashing, etc.; (F2)

g) If equipment have to be sent to other organizations for repair, completely eliminate stored work-related information and sign confidentiality agreement with equipment maintenance factory; password-related hardware of equipment that match password equipment in use must be dismantled by production equipment R&D institution before being sent for repair; password related software and information must be completely eliminated; (F2)

h) Develop standardized troubleshooting process and establish detailed failure logs (including failure occurrence time, scope, phenomenon, handling results, handling personnel, etc.); (F2)

i) Ensure that information processing equipment may be taken from machine room or office space only after being approved;

Evaluation modes

Interview and inspect.

Evaluation objects

Asset administrator, system administrator, auditor, server operation specification, equipment approval and distribution management document, equipment use management document, server operation logs.

Implementation of evaluation

a) Interview asset administrator; inquire whether various facilities and equipment are regularly maintained by specially-assigned person or department, which department/who is responsible for the maintenance and how long maintenance cycle is;

b) Interview asset administrator; inquire whether the links (model selection, procurement, distribution, etc.) on equipment selection and use is approved and controlled, whether the organization that takes away equipment is audited and controlled and whether equipment operation and use require standardized management;

c) Interview system administrator; inquire whether server is correctly configured and whether the operation of server follows operation specification;

d) Interview auditor; inquire whether there is log on server operation, how log document is managed and whether the management is periodically inspected;

e) Inspect equipment use management document; check whether the content covers terminal computer, portable computer and network equipment use and operation responsible-persons, precautions, etc.;

f) Inspect equipment approval and distribution management; check whether the content stipulates the declaration and approval of equipment model selection, procurement, distribution, etc.;

g) Inspect server operation procedures; check whether the content covers the operations of server start, stop, power-on, power-off, etc.

Result judgment

a) If a) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Network security management (G2)

Evaluation items

a) Establish network security operation management system to stipulate network security configuration, log storage time, security policy, upgrading and patching, password update cycle, important document backup, etc.;

b) Carry out routine inspection for network environment running state; keep the record on routine inspection and have it signed by operation and review personnel; (F2)

c) Financial internet interconnection security is based on the security management mode of unified standardization, hierarchical management and independent duty of performance; any organization may not have internet interconnection with external organizations without the permission of technology competent agency of financial organization; (F2)

d) Develop remote access control specification; if remote access is indeed required, it shall be approved by technical department of access launching organization and submitted to technical department (post) of organization to be visited; security protection measures including making separate account, minimum permission assignment, timely close of remote access service shall be taken; (F2)

e) The organizations reasonably control multimedia network application size and scope based on the responsible-person of not affecting normal network transmission and may not provide across-jurisdiction video on demand and other multimedia network applications that seriously occupy network resources in internal network of financial organization without the approval of technology competent agency of financial organization; (F2)

f) After being approved by competent leader of this department, information security management personnel are entitled to security detection and scanning; detection and scanning results are sensitive information and may not be disclosed without authorization; any external organization or personnel may not detect or scan internal network of financial organization without the authorization from technology competent agency of financial organization;

g) Develop network access management practices; access scheme shall be audited by technical department before access network for any equipment; access network is allowed only after being approved and then appropriate network resources are assigned.

Evaluation modes

Interview and inspect.

Evaluation objects

Security responsible-person, security officer, network administrator, auditor, network vulnerability scanning report, network security management system, letter of authorization for external connection of system, network audit log.

Implementation of evaluation

a) Look up network security management system; check whether the content covers network security configuration (including security policies of network security, authorized access, minimum service, upgrading and patching), audit log storage time, upgrading and patching, etc.; inquiring whether the designated person is responsible for maintaining network operation log, monitoring record and analyzing

and processing alarm information and other network security management work;

b) Look up the division of network administrators and pick up network security operation and maintenance files to record;

c) Pick up to read the document that network administrator participates in network security technology training; check the configuration of internet interconnecting device and compare with approval record;

d) Check remote access control configuration in related network equipment and pick up remote access audit record to read;

e) Pick up the record of illegal external-access monitoring system to read and inspect whether there is sensitive work information stored in machine used for world wide web;

f) Inspect whether online video service has cross-regional restriction and whether cross-regional video on demand is approved by technical department;

g) Interview network administrator; inquire whether network equipment is upgraded based on software upgrading version provided by manufacturer, what is current version No., whether there is backup of important documents (account data, configuration data, etc.), which way is used for backup, whether network equipment receives vulnerability scanning and whether the vulnerabilities are repaired timely;

h) Inspect backup of network equipment configuration document;

i) Pick up to read approval, change time and configuration parameter backup in network change record;

j) Check the authorization from confidentiality department in world wide web application record;

k) Interview security officer; inquire external-access types of system network (internet, enterprise network of cooperative partner, network of superior department, etc.), whether all of these are authorized and approved and which department/who approves;

l) Interview auditor; inquire whether there is storage time of audit log and how long it is;

m) Inspect network vulnerability scanning report; check whether the content covers existing vulnerabilities of network, severity, cause analysis, opinions on improvement, etc.;

n) Inspect network security management system; check whether it covers security policy of network equipment, authorized access, minimum service, upgrading and patching, maintenance record, contents of log, log retention time, etc.;

o) Inspect whether there is letter of authorization for external-access of internal

network and whether there is letter of authorization for all external-access of internet network and pick up the record on change of computer uses to read;

p) Carry out virus detection for the information downloaded from internet;

q) Inspect whether there are network audit logs within prescribed storage time range.

Result judgment

a) If a) ~ q) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) System security management (G2)

Evaluation items

a) Establish system security management system that stipulates security policy, security configuration, log management, daily operation processes, etc.;

b) Analyze to determine access control policy of system based on business demands and system security;

c) System administrator may not add, delete or modify business data; if system administrator indeed needs to technically maintain database of computer system, consent shall be obtained from business department and information maintenance process shall be recorded in detail; (F2)

d) Scan vulnerability at least once a year and timely repair discovered security vulnerabilities of system timely; (F2)

e) Install the latest patch program; first carry out the test and back up important documents, and then install system patch program;

f) daily operations, operation and maintenance record, parameter setting and revision, etc.; unauthorized operation is strictly forbidden;

g) Periodically analyze running log and audit-data in order to timely discover abnormal behavior.

Evaluation modes

Interview and inspect.

Evaluation objects

Security responsible-person, security officer, system administrator, system auditor, system security management system, system audit log, system vulnerability scanning report.

Implementation of evaluation

a) Interview system supervisor; inquire whether the designated person is responsible for system security management;

b) Interview system administrator; inquire whether there is institutionalized management for system security;

c) Interview system administrator; inquire whether system is regularly installed with security patch program, whether there important documents (system configuration, system user data, etc.) is backed up before installation of system patch, which mode is adopted, whether there is vulnerability scanning for system and whether vulnerability is timely repaired;

d) Interview security officer, inquiring whether system access control policy is determined based on business requirements and system security analysis;

e) Interview system administrator, inquiring whether system users are classified, whether different levels of users only have the minimum permissions to complete the task and whether certain handling means are adopted to prevent the continuous use for system default users that are not commonly used (e.g. deleting or disabling);

f) Interview auditor; inquire whether retention period of system audit log is prescribed and how long it is;

g) Inspect whether there is system audit log in prescribed retention period;

h) Inspect system vulnerability scanning report; check whether the content covers system vulnerability, severity, cause analysis, opinion on improvement, etc.;

i) Inspect system security management system; check whether the content covers specific requirements on system security policy, authorized access, minimum service, upgrading and patching, maintenance record, log, system account, etc.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Malicious code prevention management (G2)

Evaluation items

a) Raise the all users' awareness of anti-virus; timely inform the version of anti-virus software; inspect the virus before reading the data in removable storage device or receiving data or email; inspect the virus before external computer or storage equipment is connected to network system;

b) Client of financial organization shall uniformly install virus prevention software, set user password and screen saver password or other security measures to ensure timely update of virus feature code and installation of necessary patch program;

(F2)

c) Specially assign a person to detect malicious code for network and host and keep detection record;

d) Explicitly stipulate authorized use of malicious code software, malicious code upgrading, periodic reporting, etc.

Evaluation modes

Interview and inspect.

Evaluation objects

System operation and maintenance responsible-person, malicious code prevention management document, malicious code detection document.

Implementation of evaluation

a) Interview system operation and maintenance responsible-person; inquire whether there is education on basic malicious code prevention awareness for employees, e.g. informing promptly of upgrading software version, virus inspection before receiving online document or access of external computer or storage equipment to network system;

b) Interview system operation and maintenance personnel; inquire whether designated person is responsible for malicious code detection and keeping record;

c) Inspect malicious code prevention management document; check whether the content covers authorized use of malicious code, malicious code library upgrading, periodic reporting, etc.;

d) Inspect whether there is malicious code detection record.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) Password management (G2)

Evaluation items

a) Adopted password product and encryption algorithm shall conform to relevant national provisions in password management;

b) Establish a system on management of generation, distribution and reception, use, storage, update, destruction, etc. of all secret keys; secrete key management personnel must be official employees of the organization; (F2)

b) If a) ~ j) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Lightning protection (G3)

Evaluation items

a) Machine room building shall be equipped with lightning rod and other lightning protection devices;

b) Equip with nationally certified lightning protector to prevent induction stroke;

c) Machine room shall be equipped with AC ground wire.

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, building lightning protection/design documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring which protective measures are taken in order to prevent damage from lightning strike, whether machine room building is equipped with lightning arrester, whether it passes inspection or technical detection by relevant national departments; inquire whether computer grounding system has dedicated ground wire, whether qualified lightning arrester is increased for power source and signal line in order to prevent induction lightning;

b) Interview machine room maintenance personnel; inquire whether building lightning protection device of machine room receives regular inspection and maintenance; inquire whether computer grounding system (AC working grounding, security protective grounding) conforms to the requirements of GB50174—2008 “Design Code for Electronic Computer Room”.

c) Check whether machine room has building lightning protection design/acceptance documents; check whether there is description on requirements for ground wire connection and whether it is consistent with the actual situation;

d) Check whether qualified lightning protection device is increased on power source and signal line in order to avoid induction lightning strike.

Result judgment

a) If computer room lightning protection meets the requirements in GB 50057—1994 “Design Code for Protection of Structures against Lightning” (GB157 “Design Code

for Lightning Protection of Buildings") and there is surge voltage absorbing device in frequent lightning area, then a) in implementation of evaluation is positive;

b) If leading ground leads are insulated from steel mesh of building and various steep pipes; AC grounding resistance is no greater than 4Ω; grounding resistance in security grounding area is no greater than 4Ω, grounding resistance in lightning protection area (such area is not required for buildings with lightning protection area), b) in implementation of evaluation is positive;

c) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Fire prevention (G3)

Evaluation items

a) Machine room shall be equipped with automatic fire extinguishing system, which can automatically detects fire and automatically gives an alarm through a variety of forms including smoke detector and temperature detector in working room, under raised floor, in ceiling, in main air conditioning pipe and in places near combustibles.

b) Use building materials under fire resistance rating for machine room and related work room and auxiliary room;

c) Machine room shall regional isolation fire-prevention measures to isolate important equipment from other equipment;

d) Machine room shall be equipped with automatic fire alarm system and a certain number of gas fire extinguishers that has little effect on computer equipment. Fire alarm system shall be linked with air conditioning system, new air system and access control system and normal operating state is manual triggering; (F3)

e) Cables used in machine room shall meet fire fighting requirements; paper, film and other inflammables shall be placed in metal fireproof cabinet; (F3)

f) Host room that adopts pipe-network clean gas fir extinguishing system or high-pressure water mist fire extinguishing system shall be equipped with two kinds of fire detectors and fire alarm system shall be linked with fire extinguishing system; host room with clean gas fire extinguishing system shall be equipped with air respirator or oxygen respirator; (F3)

g) Regularly inspect fire fighting facilities; organize fire drills for at least once every six months; (F3)

h) Machine room shall have at least two fire escape routes; it shall be ensured that roads from sub-region to fire fighting access are unblocked to facilitate escape of staff. There shall be evident fire fighting marks on machine room channel. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room duty personnel, machine room facilities, machine room security management system, machine room fir protection design/inspection document, automatic fire extinguishing system design/inspection document.

Implementation of evaluation

a) Interview physical security responsible-person; inquire whether machine room is equipped with fire-fighting equipment and automatic fire protection system that automatically detects fire, automatically gives an alarm or automatically extinguishes fire, whether there is specially-assigned person who is responsible for operation of this system, whether there is management system and fire plan, whether there is training on fire control;

b) Interview machine room duty personnel; inquire whether emerging potential safety hazard can be timely reported and excluded, whether there is training on use of machine room fire fighting equipment, whether fire fighting equipment and automatic fire fighting system can be correctly used (sprinkling does not apply to machine room);

c) Inspect whether machine room is equipped with automatic fire fighting system that automatically detects fire (e.g. using temperature detector or smoke detector), automatically gives an alarm or automatically extinguishes fire, whether locating place is reasonable and whether validity period is qualified; inspect whether automatic fire fighting system normally operates; check operation record, alarm record, periodic inspection and maintenance record;

d) Inspect whether there is management system document on machine room fire fighting; inspect whether there is machine room fire protection design/inspection document; inspect whether there is machine room automatic fire fighting system design/inspection document and whether document is consistent with existing fire fighting configuration; inspect whether there is inspection document for machine room and related room construction materials and area isolation and fire prevention measures or fire inspection document;

e) Inspect whether machine room has regional isolation fire prevention measures; separate important equipment from other equipment; separate important equipment from other equipment;

f) Inspect whether fire alarm system of machine room is linked with air conditioning system, new air system, UPS, etc.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Waterproof and moisture-proof (G3)

Evaluation items

a) Water pipe may not pass through roof of machine room; preventive measures shall be taken if it passes through floor;

b) Measures shall be taken to prevent rainwater permeates through machine room window, roof and wall;

c) To facilitate transfer of underground water, there shall be gutter and drain around water leakage area; when air conditioning vents are arranged in suspended ceiling, vent is better not be right above equipment in order to prevent water vapor condensation and infiltration;

d) install detection instrument or element sensitive to water for machine room waterproof detection and alarm.

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, building waterproof and moisture-proof design/inspection document, machine room humidity record, dehumidifier operation record.

Implementation of evaluation

a) Interview physical security responsible-person; inquire whether machine room has waterproof and moisture-proof measures, whether plumbing (if an) inside machine room avoids passing through roof and under raised floor; whether there are protective measures for water pipe that passes through wall and floor slab, e.g. casing pipe, whether someone is responsible for waterproof and moisture-proof matters in high-humidity area or season and whether there is dehumidifier;

b) Interview machine room maintenance personnel; inquire whether machine room leaks or gets damp again, whether plumbing (if an) inside machine room is regularly checked against water leakage, whether there are preventive measures if condensation of water vapor in machine room and underground water transfer and penetration phenomena occur;

c) Inspect whether there is building waterproof and moisture-proof design/inspection document of machine room and whether it is consistent with the actual waterproof and moisture-proof condition of machine room;

d) Inspect whether there are necessary protective measures if pipe passes through host room wall and floor slab, e.g. setting casing pipe, etc.;

e) Inspect whether machine room roof, wall, etc. have leakage, infiltration and damp phenomena, whether machine room and the environment faces obvious leakage and damp phenomena and whether infiltration and damp phenomena can be timely solved in case of any;

f) For high-humidity area or season, inspect whether machine room has humidity record, whether there is humidifier and whether it can function properly, whether there are measures to avoid transfer and infiltration of machine room underground water, whether there is waterproof and moisture-proof processing record and dehumidifier operation record and whether it is consistent with machine room humidity record.

Result judgment

a) If “if” condition in d) and f) is not satisfied, then this item is not applicable;

b) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Anti-static (G3)

Evaluation items

a) Take necessary grounded anti-static measures for main equipment;

b) Adopt anti-electrostatic floor for machine room;

c) Better use static conductive or static dissipative materials for workbench surface in host room or auxiliary area. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, anti-static design/inspection document, humidity record.

Implementation of evaluation

a) Interview physical security responsible-person; inquire whether machine room has necessary grounding and other anti-static measures, whether there are measures to control machine room humidity and whether effective anti-static measures are taken for machine room in area where static electricity is strong;

b) Interview machine room maintenance personnel; inquire whether machine room humidity is regularly inspected and controlled within the range prescribed in GB2887; inquire whether machine room suffers from electrostatic problems or failure event caused by static electricity and whether measures are taken timely to eliminate static electricity if static electricity exists;

c) Inspect whether there is anti-static design/inspection document of machine room; check whether the description content is consistent with the actual situation;

d) Inspect whether machine room has safety grounding; check relative humidity record of machine room conforms to the provisions in GB2887; check whether machine room has evident static phenomenon;

e) For the area with strong static electricity, inspect whether machine room has anti-static floor, anti-static workbench, anti-static elimination agent, electrostatic eliminator, etc.

Result judgment

a) Effective anti-static measures in evaluation implementation e) may include part or all of anti-static floor, anti-static workbench, electrostatic eliminator, etc., then this item is positive;

b) If “if” condition in e) is not satisfied, then this item is not applicable;

c) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) Temperature and humidity control (G3)

Evaluation items

a) Temperature and humidity of host room when equipment is started up shall follow level A; basic cabin may be based on two levels of A and B in accordance with equipment requirements; auxiliary room shall be based on equipment requirements.

Temperature and humidify of computer room when it is started shall conform to the provisions in following Table 4:

Table 4 Three-level requirements for temperature and humidity in machine room

Item \ Level	Level A	Level B	
	Summer	Winter	Whole Year
Temperature	23±1°C	20±2°C	18~28°C
Relative humidity (when ON)	40%~55%	35%~75%	
Relative humidity (when OFF)	40%~70%	20%~80%	

Temperature change rate	< 5°C/h, no condensation	< 10°C/h, no condensation

b) Machine room shall have dedicated air conditioning equipment; air conditioner shall be provided with communication interface; communication protocol shall meet the requirements of machine room monitoring system; (F3)

c) Main equipment of air conditioning system shall be backed up; air conditioning equipment with certain margin; (F3)

d) Air distributor and return air inlet mounted on raised floor shall be made of nonflammable material or non-combustible material; (F3)

e) When air conditioning equipment is used, leakage warning device and small waterproof embankment shall be set; attention shall also be paid to anti-freeze and fire prevention measures for cooling tower, pump, water tank and other water supply equipment. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, temperature and humidity control design/maintenance record.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether machine room is equipped with constant-temperature constant-humidity system to ensure that temperature and humidity can meet the requirements of computer equipment for operation, whether machine room management system prescribes requirements for temperature and humidity control and whether someone is in charge of this job;

b) Interview machine room maintenance personnel, inquiring whether temperature and humidity automatic adjustment facilities are regularly inspected and maintained and whether there are such events that temperature and humidity impact operation of system;

c) Inspect whether machine room has temperature and humidity design/inspection document, whether it can meet system operating needs and whether it is consistent with current situation;

d) Inspect whether constant-temperature constant-humidity system can function normally, whether there are temperature and humidity record, operation record and maintenance record; check whether machine room temperature and humidity meet the requirements of GB 2887-89 “Specification for Computation Center Field”.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) Power supply (A3)

Evaluation items

a) Configure power supply line of machine room with voltage stabilizer and over-voltage protection equipment;

b) Set redundant or parallel power cable line for power supply to computer system based on the principle of two circuit power supply;;

c) Establish electric generator and other backup power supply system (e.g. backup generator) in case of temporary interruption of power supply system and ensure that backup power supply system may be put in place in UPS power supply time; carry out simulation drilling of backup power supply system annually and regularly overhaul and maintain backup power supply equipment to ensure the proper use;

d) UPS power supply system shall adopt redundancy modes of N+1, N+2, 2N, 2 (N+1), etc. For the organizations that have no emergency power supply system of diesel oil generator, UPS backup time shall be at least 2 hours; (F3)

e) Machine room inside shall be equipped with machine room dedicated socket; power sockets for maintenance and test shall be respectively set and be marked for clear distinction. Mains supply and UPS power sockets shall be separated to meet the requirements for use of load; (F3)

f) Computer system shall adopt copper wire cable to avoid mixing of copper and aluminum. If it is unavoidable, use copper and aluminum transition joint for connection; (F3)

g) Machine room shall be equipped with emergency lighting and emergency exit light, various switches, handles and buttons inside power distribution and supply cabinet (box) and distributor shall be clearly marked to prevent mal-operation. (F3)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, power supply security design/inspection document, inspection and maintenance record.

Implementation of evaluation

a) Inspect physical security responsible-person, inquiring whether power supply line of computer system is separated from other power supply lines, inquiring whether power supply line of computer system is installed with stabilizer and over-voltage protective equipment, whether there is short-time emergency power source (e.g. UPS), whether power supply time meets minimum power supply demand of system, whether it is installed with redundant or parallel power cable line (e.g. two-circuit feeding), whether there is backup power supply system (e.g. backup generator) and whether UPS backup time is at least 2 hours if there is no generator has no emergency power supply system;

b) Interview machine room maintenance personnel, inquiring whether stabilizer, over-voltage protective equipment, short0tem backup power equipment installed at power supply line of computer system is regularly inspected and maintained and whether power voltage stabilization range may be controlled to meet normal operation of computer system;

c) Interview machine room maintenance personnel, inquiring whether redundant or parallel power cable lines (e.g. two-circuit power supply mode) can normally supply power to computer system when two-circuit power supply is switched, regularly check backup power system (e.g. backup generator) to verify whether it is normally started up or supplies power within the specified time;

d) Inspect whether there is power supply security design/inspection document of machine room; check whether the documents indicates a separate power supply for computer system as well as the requirements for voltage stabilizer, overvoltage protection device, backup power units and redundant or parallel power cable line, etc.;

e) Inspect computer power lines and check whether computer power supply is separated from other powers;

f) Inspect machine room and check whether voltage stabilizer, overvoltage protection equipment and short-term backup power equipment for computer power supply lines can operate normally; check whether power supply voltage is normal;

g) Inspect whether there is inspection and maintenance record on voltage stabilizer, overvoltage protection equipment, short-term backup power equipment and other power source equipment, redundant or parallel power line cable switching record and operation record of backup power supply system and whether operation records of above computer system power supply and whether it can meet the normal operation requirements of system;

h) Evaluate whether installed redundant or parallel power cable line (e.g. two-circuit power supply mode) can achieve two-circuit power supply switching;

i) Evaluate whether backup power supply system (e.g. backup generator) can be normally started and supply power within the specified time.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

10) Electromagnetic protection (S3)

Evaluation items

a) Adopt grounding mode to prevent outside electromagnetic interference and parasitic coupling interference of equipment;

b) Power line and communication cable line shall be isolated on laying to prevent mutual interference;

c) Key equipment and magnetic medium shall receive electromagnetic shielding;

d) Network cabling of computer system equipment may not be parallel to the cabling of non-electromagnetic shielding of power equipment; their crossing shall be based on near vertical angle and measures shall be taken to prevent flame spread. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Physical security responsible-person, machine room maintenance personnel, machine room facilities, electromagnetic protection design/inspection documents.

Implementation of evaluation

a) Interview physical security responsible-person, inquiring whether there are measures to prevent external electromagnetic interference and parasitic coupling equipment (including equipment shell has good grounding; power line and communication wires and cables are isolated) and whether measures are taken to prevent electromagnetic leakage for the equipment that process confidential information;

b) Interview machine room maintenance personnel, inquiring whether equipment shell has good grounding, whether power line and communication line are isolated, whether there are failures caused by electromagnetic protection, whether the equipment of processing confidential information is low-radiation equipment, whether it is installed with second-level electromagnetic interference unit that meets BMB4-2000 “Technical Requirement and Evaluation Method of Electromagnetic Interference”;

c) Inspect whether there is design/inspection document of machine room; check whether the description content is consistent with the actual situation;

d) Inspect whether the shell of equipment in machine room is completely grounded;

e) Inspect machine room wiring and check whether power line and communication line are separated;

f) Check whether electromagnetic interference unit is simultaneously started up when secret-associated equipment of electromagnetic interference unit is started up.

Result judgment

a) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

In content, implementation of physical security evaluation involves 10 work-units; see annex A.2.1.1 for specific check list.

7.1.2.1.2 Network security

1) Structural security (G3)

Evaluation items

a) Ensure the redundancy of major network equipment and communication lines; business processing capacity of major network equipment is required to be beyond the demand at rush hours; for double-circuit design, it shall be provided by different service providers;

b) Ensure that the bandwidth of each part of the network meets the demand in rush hours;

c) Control the route between business terminal and business server and establish secure access route;

d) Draw structural chart of network topology that is consistent with current operation;

e) Divide into different subnets or network segments based on job functions and importance of different departments, the importance of information involved and other factors; allocate address fields to subnets and network segments based on the principle of facilitating management and control; production network, internet and office network shall be effectively isolated;

f) Avoid deployment of important network segments at network boundary and direct connection to external information system;; adopt reliable technical isolation means between important network segment and other network segment;

g) Assign bandwidth allocation priority based on the order of importance to business service; ensure protection for important host in case of network congestion.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Network administrator, boundary and major network equipment, network topological graph, network design/inspection document.

Implementation of evaluation

a) Interview network administrator, inquiring the performance of boundary in information system and main network equipment as well as the flow in current rush hours of business;

b) Interview network administrator, inquiring network segment division and division principles, important segments and protective measures to important network segments;

c) Interview network administrator, inquiring the bandwidth of network, the control over bandwidth of network and bandwidth distribution principles;

d) Interview network administrator, inquiring route control policies and measures for network equipment as well as designed purposes of these policies;

e) Inspect network topological graph and check whether it is consistent with current operation;

f) Inspect network design/inspection document and check whether bandwidth occupation statement includes record on meeting or exceeding processing capacity;

g) Inspect network design/inspection document and check they are divided into different subnets or network segments in accordance with job functions and importance of various departments as well as degree of information involved, etc. and assign the design or description of address fields to various subnets or network segments based on the principle of facilitating management and control;

h) Inspect boundary and main network equipment and check whether route control policy (e.g. static route is used, etc.) to establish a secure access path; check whether the nodes on access path conforms to access control strategy at business server address of terminal trace;

i) Inspect boundary and major network equipment and whether important network segment is deployed network boundary to directly connect with external information system and whether important network segment is separated from other network segments through firewall, access control and other means;

j) Inspect boundary and major network equipment and check whether there are policies (e.g. QOS policy configuration of route and switching equipment, configuration policy of dedicated bandwidth management equipment, etc.) to control bandwidth and whether these policies ensure priority to protection for important businesses in case

of network congestion (e.g. priority of host of important businesses shall be over the priority of host of non-important businesses);

k) Evaluate network topological structure and verify whether actual network topological structure is consistent with network topological structural chart through automatic discovery and drawing tools of network topology structure;

l) Evaluate the access path between business terminal and business server; verify whether the access path between business terminal and business server is secure (e.g. whether access route is fixed, etc.) through route tracing tool;

m) Evaluate important network segments and evaluate whether adopted network address and data link address binding measures or data link layer address and exchanger binding measures are effective (e.g. trying to use non-binding measures, checking whether there is normal access, etc.);

n) Evaluate network bandwidth allocation strategy; use bandwidth evaluation tool to evaluate whether network bandwidth allocation is effective.

Result judgment

a) If f) ~ g) lack corresponding documents in evaluation implementation, then this item is negative;

b) If e) ~ n) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Access control (G3)

Evaluation items

a) Deploy access control equipment at network boundary and enable access control function;

b) Provide the capacity of permitting/denying access to data flow in accordance with dialogue status information; control granularity is port-level;

c) Filter the content of information in and out of network and achieve command-level control over application layer HTTP, FTP, TELNET, SMTP, POP3 and other protocols;

d) Terminate network connection when dialogue is inactive for some timer or dialogue is terminated;

e) Monitor maximum network traffic and network concurrent connection number at network boundary zone (internet zone boundary, external zone boundary and internal zone boundary);

f) Important network segment shall have technical measures to prevent address spoofing;

g) Permit or deny users' resource access to controlled system based on access permission rule between user and system; control granularity is single user;

h) Use digital certificate authentication mechanism for users that have dial-up access and restrict the number of users with dial-up access;

i) Set access control permissions for network equipment based on the responsible-person of minimum security responsible-person. (F3)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, network administrator, boundary network equipment (including network security equipment).

Implementation of evaluation

a) Interview security officer, inquiring which network control measures are taken, what the design principle of access control principle, whether access control policy is adjusted and what is the situation prior to and after adjustment;

b) Inspect boundary network equipment and check whether it controls data stream based on dialogue status information (e.g. source address of data packet, destination address, source port No., destination port No., protocol, access interface, dialogue serial No., name of host that gives out information and shall support the use of address wildcard character);

c) Inspect border network equipment (service network longitudinal firewall and financial city network); check whether it filters information in and out of network to achieve the control over application layer HTTP, FTP, TELNET, SMTP, POP3 and other protocols' level;

d) Inspect boundary network equipment and check whether dialogue can be set in in-active time or network connection is automatically terminated after dialogue is ended; check whether maximum flow of network and network concurrent connection number may be set;

e) Inspect major network equipment and check whether there are access control measures (e.g. VLAN, access control list, MAC address binding) to provide portable and mobile equipment for access network;

f) Evaluate boundary network equipment; evaluate whether control of access control measures over unauthorized access behavior is effective (e.g. using scanning tool for detection, etc.);

g) Evaluate major network equipment; verify whether access control policy of network

equipment is effective through access of mobile equipment to network;

h) Make permeation evaluation through network access control measures; verify whether network access control measures have no obvious weakness through verifying network access control measures.

Result judgment

a) If b) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Security audit (G3)

Evaluation items

a) Make log record on running state of network equipment, network traffic, user behavior, etc. in network system;

b) Audit records shall include event date and time, user, event type, whether event is successful and other information related to audit;

c) Be able to analyze based on data records and generate audit statement;

d) Protect audit record and avoid unexpected deletion, revision or coverage, etc.; retention time shall be no less than half a year.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Auditor, boundary and major network equipment.

Implementation of evaluation

a) Interview auditor, inquiring whether boundary and key network equipment in network system has the setting of security audit, items included, main contents of audit record and the audit record processing method;

b) Inspect log server or AAA server; check whether audit record includes network equipment running state, network traffic, user behavior, etc. in network system;

c) Inspect log server or AAA server; check whether event audit record includes event date and time, user, event type, event result and other audit-related information;

d) Inspect log server or AAA server; check whether it can give a real-time alarm based on specific mode (e.g. sound, EMAIL, SMS, etc.);

e) Inspect log server or AAA server; check whether there is the function of generating

statement (e.g. audit statement, sorting, query, statistics, analysis, combination query, etc.) and statement may be generated based on demand;

f) Evaluate log server or AAA server; verify whether the coverage of security audit and record meet requirements through some user trying to generate a number of security-related events (e.g. identification failure);

g) Evaluate log server or AAA server; verify whether the protection over security audit meets requirements through some user trying to delete, revise or cover audit record.

Result judgment

a) If b) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Boundary integrity inspection (S3)

Evaluation items

a) Inspect the behavior of privately connecting unauthorized equipment to internal network; accurately locate the position and effectively block;

b) Inspect the behavior of privately connecting internal network user to external network; accurately locate the position and effectively block.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, network administrator, boundary integrity inspection equipment, boundary integrity inspection equipment operation log.

Implementation of evaluation

a) Inspect boundary integrity inspection equipment; check whether there is access network of computer that illegal external-access client; in case of any such computer, whether it is immediately positioned and blocked;

b) Inspect boundary integrity equipment operation log; check whether the operation is normal (check whether the whole network segment is monitored);

c) Inspect boundary integrity inspection equipment; check whether there is the setting that the behaviors of illegal external-access to internet network and illegal external-access to external network can be effectively blocked;

d) Evaluate boundary integrity inspection equipment; evaluate “illegal external-access” behavior may be effectively discovered (e.g. generating illegal external-access action,

checking whether boundary integrity inspection equipment can discover this behavior);

e) Evaluate boundary integrity inspection equipment; evaluate whether the position of "illegal external-access" equipment may be determined and it is effectively blocked (e.g. generating illegal external-access action; checking whether boundary integrity inspection equipment can accurate locate and block);

f) Evaluate boundary integrity inspection equipment; evaluate whether it can inspect the behavior of privately connecting unauthorized equipment to network, accurately locate the position and effectively locate (e.g. generating illegal access action, inspecting whether boundary integrity inspection equipment may be accurately discovered, accurately located and blocked).

Result judgment

a) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Intrusion prevention (G3)

Evaluation items

a) Monitor following attack behavior at network boundary: port scanning, brute-force attack, Trojan backdoor attack, denial of service attack, buffer overflow attack, injection attack, IP fragmentation attack, network work attack, etc.;

b) When attack behavior is attacked, record attack source IP, attack type, purpose of attack, attack time; alarm shall be given in case of serious intrusion event.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, network intrusion prevention equipment.

Implementation of evaluation

a) Interview security officer, inquiring network intrusion prevention measures, whether there is special equipment for network equipment intrusion, the upgrade mode of network intrusion prevention rule base;

b) Inspect network intrusion prevention equipment; check whether following attack behaviors may be detected: port scanning, brute-force attack, Trojan backdoor attack, service denial attack, buffer overflow attack, IP fragmentation attack, network worm attack, etc.;

c) Inspect network intrusion prevention equipment; check whether intrusion event record includes invasive source IP, attack type, purpose of attack, attack time, etc.;

d) Inspect network intrusion prevention equipment and check whether production manufacturer is qualified and whether rule base is the latest;

e) Evaluate network intrusion prevention equipment and verify whether the monitoring policy is effective (e.g. simulating to generate attack action; checking the reaction of network intrusion prevention equipment);

f) Evaluate network intrusion prevention equipment and verify whether the alarm policy is effective (e.g. simulating to generate attack action, checking whether network intrusion prevention equipment can give a real-time alarm).

Result judgment

a) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Malicious code prevention (G3)

Evaluation items

a) Detect and remove malicious code at network boundary that is connected with other organizations and internet;

b) Regularly upgrade code library of malicious code protection equipment and update the system.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, anti-malicious code product, design/inspection document, running log of malicious code product.

Implementation of evaluation

a) Interview security officer, inquiring network anti-malicious code preventive measures of system, update policy and main functions of anti-malicious code products, inquiring whether system suffers from security event against malicious code intrusion;

b) Inspect design/inspection document and check measures against malicious code are taken at network boundary and core business network segment (e.g. whether there is anti-virus gateway) and whether anti-malicious code product has the description on the function of real-time update;

c) Inspect running log of malicious code product and check whether it operates continuously;

d) Inspect whether measures are taken at network boundary and core business network segment based on the characteristics of malicious code to detect from network layer and remove;

e) Inspect anti-malicious code product and check whether it is produced by qualified manufacturer, whether the operation is normal and whether malicious code is the latest version;

f) Inspect the allocation strategy of malicious code products and check whether it supports unified management of malicious code prevention (e.g. checking whether it is a distributed deployment, centralized management, etc.).

Result judgment

a) If b) in implementation of evaluation lacks corresponding document, this item is negative;

b) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Network equipment protection (G3)

Evaluation items

a) Authenticate the identity of users who log onto the network equipment;

b) Restrict administrator registration address of network equipment;

c) Identities of network equipment shall be unique;

d) For main network equipment, there shall be two or more combinations of identification technology for the same user to select for identity authentication;

e) Identity authentication information shall not be easily illegally used; password shall have complexity and replaced regularly;

f) There shall be login failure processing function; measures of ending dialogue, restricting illegal login times, automatically exiting, etc. in case of network login timeout;

g) When network equipment is under remote management, necessary measures shall be taken to prevent authentication information from being intercepted during network transmission process;

h) Achieve separation of equipment privileged users;

i) Back up configuration documents of network equipment at regular intervals and timely back up in case of any changes; (F3)

j) Regularly inspect running state of network equipment; (F3)

k) Set out built-in service ports network equipment; turn off unnecessary system service port and establish corresponding port approval system; (F3)

l) Regularly inspect information on software version of network equipment to avoid potential safety hazard of software version in use; (F3)

m) Establish clock synchronization mechanism of network equipment; (F3)

n) Regularly inspect or revoke unnecessary user account in network equipment. (F3)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Network administrator, boundary and major network equipment.

Implementation of evaluation

a) Interview network administrator whether there is AAA certification for network equipment or other certification method. Check whether user matches administrator identity and permissions in case of any log onto AAA server;

b) Interview network administrator, inquiring the password policy of network equipment;

c) Inspect the security settings of boundary and major network equipment; check whether there is setting of adopting corresponding measures in case of authentication failure; check whether there is the function of restricting the number of illegal logins;

d) Inspect the security settings of boundary and major network equipment; check whether administrator login addresses of boundary and major network equipment are restricted; check whether network login connection is time-out and exits automatically; check whether permissions of equipment privileged users are separated; check whether online network entities receive identify authentication; evaluate the security settings of boundary and major network equipment to verify whether the functions of authentication failure processing measures (the times that wrong password is used to log onto network equipment, observing network is terminated and illegal login times are restricted) and restricting administrator registration address of network equipment, etc. are effective;

e) Evaluate the security settings of boundary and major equipment; verify whether automatic exit setting is effective (e.g. long-time connection without any operation,

observing the movements of work equipment) when network login connection is time-out;

f) Make permeation evaluation for boundary and major network equipment; use a variety of permeation evaluation technology (e.g. guessing password, etc.) for permeation evaluation for network equipment and verify whether protective capacity of network equipment meets requirements;

g) Log onto remote login network equipment and check whether it adopts 22 port SSH or other encryption way;

h) Achieve separation of permissions of equipment privileged users;

i) Check backup documents in computer;

j) Interview network administrator and check whether the operation of network equipment is regularly inspected;

k) Interview network administrator whether unnecessary network equipment services are off;

l) Interview network administrator at site whether software version information of network equipment is regularly inspected and there is written record;

m) Interview network administrator whether there is regular inspection and revocation of redundant user accounts in network equipment.

Result judgment

a) If password policy in network equipment is 8 or more digits in password length; password is complex (e.g. stipulating that characters shall be a mixture of capital or small letters, figures and special characters); life cycle of password, requirements for replacement of new and old passwords (stipulating the number of replaced characters) or a token is used to facilitate memory), then b) in implementation of evaluation meets evaluation requirements;

b) If b) ~ m) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

On content, implementation process on network security involves 7 work-units; see annex A.2.1.2 for specific contents.

7.1.2.1.3 Host security

1) Identity authentication (S3)

Evaluation items

a) Allocate different user names to different users of operating system and database

system and ensure that user name is unique;

b) Carry out identity marking and authentication for users who log onto operating system and database system;

c) Identity label of operating system and database system management shall not be easily illegally used; static password of system shall include at least 7 figures and is composed of at least letters, numbers and symbols and be replaced at least once every three months;

d) Enable login failure processing function or take the measures of ending dialogue, restricting illegal number of login intervals, automatic exit, etc.;

e) Host system shall carry out identity marking or authentication for corresponding servers or terminal equipment; when server is under remote management, encryption measures shall be taken to prevent authentication information from being intercepted during network transmission process; (F3)

f) Two or more combinations of authentication technology are better used for identity authentication, e.g. taking secret key password card, biological feature as identity authentication information.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, database administrator, major server operation system, main database management system, server operation system document, database system management system document.

Implementation of evaluation

a) Inspect whether identity authentication function of server operating system and database management system has evaluation report of level II above in “Security Technical Requirements of Information Security Classified Protection System” and “Security Technical Requirements of Information Security Classified Protection Database Management System” or level TCSEC C2 above;

b) Interview system administrator, inquiring the identity marking of operating system, which measures are taken to realize authentication mechanism, which identity authentication measures and authentication failure processing measures current system provides;

c) Interview database administrator, inquiring the identity marking of database system, which measures are taken to realize authentication mechanism, which identity authentication measures and authentication failure processing measures current system provides;

d) Inspect server operating system document and database management system document; check the attribute of ensuring the uniqueness of user identity label (e.g. user name or UID, etc.);

e) Inspect server operating system and database users, groups subordinate to or whether UID is unique,

f) Inspect major server operating system and major database management system; check whether identity authentication measures are provided (e.g. user name, password, etc.) and whether identity authentication information cannot be easily illegally used; check account password policy setting, e.g. long enough password, password complexity (e.g. stipulating that password shall be a mixture of capital or small letters, figures and special characters), life cycle of password and new password and old password replacement requirements (e.g. stipulating the number of characters replaced) or token is used to facilitate memory;

g) Inspect major server operating system and major database management system; check whether identity authentication adopts a combination of two or more identity authentication technologies for identity authentication (e.g. a combination of any two of user name/password, challenge response, dynamic password, physical equipment, biological identification technology or digital-certificate identity authentication technology);

h) Inspect major server operating system and major database management system; check whether there is authentication failure processing function, whether the limit value of number of illegal logins is set; terminate the authentication dialogue for login of exceeding limit value or close the account temporarily; check whether network login connection timeout is set and it automatically exits; check whether there is authentication warning information;

i) Evaluate major server operating system; check server operating system performs identity identification and authentication;

j) Evaluate major server operating system and major database management system; try logging onto the system through wrong user name and password to identity whether failure processing function is effective;

k) Evaluate major server operating system and major database management system; whether identification (e.g. setting up an account) is required first when after login, while users who are not identified cannot enter system;

l) Evaluate major server operating system and major database management system; add a new account, identity the user the same with original user's and check whether it is successful;

m) Evaluate major server operating system and major database management system; delete a user ID, and then add a new user, the ID of which is the same with deleted user ID (user name/UID), check whether it can not succeed;

n) Evaluate major server operating system; host that has not been identified on identity identification and authenticated may be user to connect to this server and verify whether host system can correctly identify and authenticate server or terminal equipment connected to it;

o) Carry out permeation evaluation of major server operating system; password cracking tool may be used to detect password strength of server operating system; check whether user password may be cracked and whether user may log onto the system after password cracking;

p) Carry out permeation evaluation of major server operating system and verify whether existing unauthorized account (e.g. new accounts that system increases after installation of some services) and system have inactive logon management;

q) Carry out permeation evaluation of major server operating system, evaluating whether there is system login method other than authentication method, e.g. existing BUG of authentication program, social engineering or other means.

Result judgment

a) If a) in implementation of evaluation is positive, then evaluation implementation j), k) and l) are positive;

b) If user name/password method is not used for identity authentication, then n) in implementation of evaluation is not applicable;

c) If password may be cracked in 0) in evaluation implementation, then this item is negative;

d) If p) in implementation of evaluation does not provide common method of bypassing authentication method for system logon, then this item is positive;

e) If e) ~ m) under the implementation of evaluation are all positive, then this information system satisfies the requirements of evaluation.

2) Access control (S3)

Evaluation items

a) Enable access control function and control the access of user to resources based on security policy;

b) Achieve permission separation of management users based on role assignment authority of management users; only grant the minimum permission required by management users;

c) Achieve permission separation for privileged users of operating system and database system;

d) Ban or severely restrict the access permission of default accounts; rename system default accounts and revise default password of these accounts;

e) Timely delete redundant and expired accounts to avoid shared accounts;

f) Set sensitive marker for important information resource;

g) Strictly control the operation of user for important information resources with sensitive marking based on security policy.

Evaluation modes

Inspect and evaluate.

Evaluation objects

Major server operating system, major database management system, security policy.

Implementation of evaluation

a) Inspect whether discretionary access control function of server operating system and database management system has evaluation report of level II above in “Security Technical Requirements of Information Security Classified Protection System” and “Security Technical Requirements of Information Security Classified Protection Database Management System” or level TCSEC C2 above;

b) Inspect the security policy of serer operating system and database management system; check whether it is defined that access control of subject (e.g. user) in the identity of user and/or user group over subject (e.g. document or system equipment, access control over directory list and access control list), whether the coverage includes information security directly related subject (e.g. user) and object (e.g. document, database list) as well as the operation between them (e.g. reading, writing or execution);

c) Inspect the security policy of server operating system database management system; check whether it is defined that the subject (e.g. user) has non-sensitive marking (e.g. role) and can stipulate the access to subject based on non-sensitive marking;

d) Inspect the access control list of major server operating system and major database management system; check whether authorized user has expired account or useless account, whether the user and permission in access control list are consistent with security policy;

e) Inspect major server operating system and major database management system; check whether the owner of subject (e.g. document, database list, view, storage process, trigger, etc.) can change the attribute of corresponding access control list; whether authorized user can change the attribute of corresponding subject access control list;

g) Better strictly control the operation of user on important information resource with sensitivity marking based on security strategy.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, major application system.

Implementation of evaluation

a) Interview system administrator, inquiring whether business system provides access control measures, which specific measures are taken and how discretionary access control granularity is;

b) Inspect major application system; check whether system provides access control mechanism and whether access of user to subject (e.g. data in document and database) is controlled based on security strategy;

c) Inspect major application system; check whether discretionary access control covers information security directly associated subject, object and the operation between them, whether the granularity of discretionary access control is that the subject is user-level and object is document and database table-level (e.g. database table, view, stored procedures, etc.);

d) Inspect major application system; check whether application system has the function of performing system operation on authorized subject and setting data access permissions;

e) Inspect major application system; check permissions of the privileged users are separated (e.g. separating the permissions of system administrator, security officer and auditor), whether permissions have mutual constraints (e.g. system administrator and security administrator may not manage audit log; security audit may not manage audit logs on audit record opening, closing, deleting and other important events);

f) Inspect major application system; check whether it restricts the access permission of default users and has been configured to use;

g) Evaluate major application system; check whether permissions are restricted by application system through login of users with different permissions and verify whether permission separation function of system is valid;

h) Evaluate major application system; set the permissions to system operation by specific user and data access through authorized subject, and then log in through this account to verify whether user permission management function is effective;

i) Evaluate major application system; verify the restriction of system to access

permission of default user is valid through default user (default password) login and operation on this user (including legal and illegal operation);

j) Carry out permeation evaluation for major application system; evaluate whether discretionary access control covers information security directly related subject, object and the operation between them (e.g. the operation of trying bypassing system access control mechanism).

Result judgment

a) If b) ~ j) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Security audit (G3)

Evaluation items

a) Provide security audit function that covers each user; audit important security event of application system;

b) Ensure that audit process cannot be interrupted alone; do not provide the function of deleting, revising or covering audit record;

c) Audit record contents shall at least include event date, time, information of originator, type, description, results, etc.; regularly back up audit records and keep for at least six months;

d) Provide the function of audit record data's statistics, query and analysis to generate audit statement;

e) For application system that is logged in from internet client, provide the date, time, method, location and other information on successful login of previous user for user log-in each time. (F3)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security auditor, major application system.

Implementation of evaluation

a) Interview security auditor, inquiring whether application system has security audit function, what the selection requirements and policies for event audit are, what are protective measures of audit logs;

b) Inspect major application system and check whether current audit scope covers each

user;

c) Inspect major application system; check whether audit policy covers important security-related events in system, e.g. user identification and authentication, all operation records of discretionary access control, important user behavior (e.g. using super user command to change user identity and delete system table), abnormal use of system resources, use of important system commands (e.g. deleting subject), etc.;

d) Inspect major application system; check whether audit record information contains event time and date, subject and object that trigger event, event type, event success or failure, resource of request in identity authentication event (e.g. end identifier), event results, etc.

e) Inspect major application system; check whether it provides dedicated audit tool for authorized users to browse and analyze audit-data (e.g. audit record classification, sorting, query, statistics, combination query, etc.) and generates audit statement based on needs;

f) Inspect major application system; check whether it can specify real-time alarm way (e.g. sound, EMAIL, SMS, etc.) for specific event;

g) Evaluate major application system; verity whether audit function is protected through illegally terminating audit function or revising the configuration;

h) Evaluate major application system; try generating a number of security-related events (e.g. identification failure, etc.) based on some user in system; evaluate whether the coverage and records of security audit are consistent with requirements;

i) Evaluate major application; try deleting, revising or covering audit records based on some user in system and verify whether the protection of security audit is consistent with requirements.

Result judgment

a) If b) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Residual information protection (S3)

Evaluation items

a) Ensure that user authentication information memory space is completely removed before being released or reallocated to other users, regardless of whether the information is stored in hard disk or in memory;

b) Ensure that the memory space of documents, directories and database records in system are completely removed before being released or reallocated to other users.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, design/inspection document.

Implementation of evaluation

a) Interview system administrator, inquiring whether system takes measures to ensure deleting residual information in storage medium (regardless of whether the information is stored in hard disk or memory) and which specific measures are taken;

b) Inspect design/inspection document; check whether there is system description on how memory space of authentication information is completely removed before being released or reallocated to other users (regardless of whether the information is stored in hard disk or memory);

c) Inspect design/inspection document; check whether there is description on how memory space of documents, directories, database records and other resources in system are released or re-allocated to other users;

d) Evaluate major application system. After some user logs onto system and operates, make another user log in when the first user exits to try operating (reading, revising or deleting, etc.) documents, directories, database records and other resources generated by other users and check whether it is successful; verify whether the residual information protection function provided by system is correct (ensure memory space of documents, directories, database records and other resources in system are released or re-allocated to other users).

Result judgment

a) If b) ~ c) in implementation of evaluation lacks relevant material, then this item is negative;

b) If b) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Communication integrity (S3)

Evaluation items

a) Adopt cryptographic technology to ensure the integrity of key data in communication process.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, major application system, design/inspection document.

Implementation of evaluation

a) Interview security officer, inquiring whether business system ensures integrity during data transmission process and which specific measures are taken;

b) Inspect design/inspection document; check whether there is description on communication integrity; if there is such description, check whether there is description that system determines the validity of data package of opposite side and that password is used to calculate verification code of communication data message;

c) Evaluate major application system and check whether communication message contains verification code through obtaining data packages of both communication parties.

Result judgment

a) If b) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Confidentiality of communication (S3)

Evaluation items

a) Application system shall use cryptography for dialogue initialization verification before both communicating parties establish connection;

b) For the system that provides server through internet, whole message or dialogue process during communication process shall ensure the confidentiality of communication process through dedicated communication protocol or encryption way.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, major application system, relevant proof material (certificate).

Implementation of evaluation

a) Interview security officer, inquiring whether there are confidentiality measures (e.g. using password for dialogue initiation verification before connection is established, encrypting sensitive information fields during communication process, etc.) during storage and transmission process of business system data and which specific measures are taken;

b) Inspect relevant proof material (certificate); check whether the cryptographic algorithm that application system adopts conforms to the requirements of relevant agency.

c) Evaluate major application system and check whether one communication side automatically ends the dialogue if the other side makes no response in a period of time, whether system can use cryptography for dialogue initiation verification (e.g. whether cryptography is used for dialogue initialization verification before encryption channel is established) before both communication sides establish dialogues and whether the whole message or communication process is encrypted during communication process;

d) Evaluate major application system; check whether one side can automatically terminate the dialogue if the other communication side makes no response in a period of time; after the dialogue is ended, evaluate whether the function that one side can automatically terminate the dialogue if the other communication side makes no response in a period of time is valid;

e) Evaluate major application system; check the contents of data packages of both communicating sides; check whether system's function of encrypting whole message or dialogue process during communication process is valid.

Result judgment

a) If b) in implementation of evaluation lacks relevant material, then this item is positive;

b) If b) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Anti-repudiation (G3)

Evaluation items

a) Have the function of providing data original evidences for data originator or recipient under request; original evidences include system operation and management records, at least including operation time, operators and operation type, operation content, etc..; transition system shall be able to record compliance transaction data of users in detail, e.g. business serial No, account name, IP address, transaction orders and other information for audit, and shall be traced back to user;

b) Have the function of providing data reception receipt for data originator recipient under request; System operation management records for receiving evidences shall at least include system operation and management record, at least involving operation time, operation personnel and operation type, operation contents, etc.; transaction system shall be able to record user compliance transaction data in detail, e.g. business serial No., account name, IP address, transaction order and other information for audit, which can be traced back to the user.

Evaluation modes

Interview and evaluate.

Evaluation objects

Security officer, major application system.

Implementation of evaluation

a) Inspect whether the system adopts digital signature during data transmission and whether it generates valid authentication code and other anti-repudiation measures;

b) Evaluate major application system; check whether the system has the function of providing data original evidences for data originator or recipient under request through communication between both sides and whether has the function of providing data acceptance evidence for data originator or recipient under request.

Result judgment

a) If b) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) Software fault-tolerance (A3)

Evaluation items

a) Provide data validity inspection function to ensure that the format or length of data input through man-machine interface input or communication interface input conform to set requirements of system;

b) Provide automatic protection function to automatically protect all current states in case of any failure and ensure system recovery;

c) Effectively system technology error message and do not feed back error information generated by system to customer directly. (F3)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, major application system.

Implementation of evaluation

a) Interview system administrator, inquiring whether business system has measures to ensure that software has fault-tolerance capacity (e.g. verifying the validity of data input through man-machine interface or communication interface) and what the

specific measures are;

b) Inspect major application system; input interface through inputting different data formats or lengths to check whether business system inspects the validity of data input through man-machine interface (e.g. user interface data input) and communication verify, whether it is allowed to backspace (e.g. revoking operation) based on operation sequence, whether some functions are continuously provided to ensure implementation of necessary measures (e.g. storage of important data) in case of failure occurrence;

c) Evaluate major application system; verity whether the validity inspection function of system man-machine interface is correct through input difference (e.g. data format or length conforms to or does not conform to software setting the requirements);

d) Evaluate major application system; verify whether system can backspace correctly based on operation sequence by multi-step operation and backspacing;

e) Evaluate major application system; verify whether the system can detect fault condition at real time and give an alarm in case of failure occurrence and automatically protect all current states through some man-made failure of system (e.g. system abnormalities).

Result judgment

a) If b) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) Resource control (A3)

Evaluation items

a) For application systems that have dialogues or short connections, when one communication side in application system makes no response in a period of time, the other side shall be able to automatically end the dialogue;

b) Be able to restrict the maximum concurrent dialogue connection number of system;

c) For application system with dialogues, be able to restrict multiple concurrent dialogues of single account;

d) Be able to restrict possible concurrent dialogue connection number in a period of time;

e) Better be able to sett limit on system resources and give prompts for limit exceeding;

f) Be able to detect whether system-level of system reduces to a predetermined minimum value and give an alarm;

g) Provide service priority setting function and set the priority of access account or request process based on security strategy after installation and allocate system

resources based on priority.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, major application system.

Implementation of evaluation

a) Interview system administrator, inquiring whether business system has resource control measures (e.g. restricting maximum concurrent dialogue connection number of application system, whether it forbids concurrent login of the same account at the same time, whether possible concurrent dialogue connection number in the same period of time is restricted, maximum and minimum quota limits on resource distribution to the same access user or the same request process) and which specific measures are taken;

b) Inspect major application system; check whether is multiple concurrent dialogue of restricting single use, whether the system has limit on maximum concurrent dialogue connection number, whether possible concurrent dialogue connection number in the same period of time is restricted, whether service priority of subject is set based on security strategy, whether resources are allocated based on priority to ensure the processing capacity of subject with low priority will not impact the processing capacity of subject with high priority;

c) Inspect major application system; check whether operation timeout lockout and authentication failure lockout of login terminal are set according to security strategy and unlocking or termination mode is stipulated, whether it forbids concurrent login of the same user account at the same time, whether there is maximum limit or minimum limit on resources that the same access user or application process occupies;

d) Inspect major application system; check whether it allows ore deny users establishing dialogue connection based on security attributes (user identity, access address, time range, etc.); check whether there is minimum setting on service level, and whether the system gives an alarm when service level of system reduces to the predetermined minimum value.

e) Evaluate major application system; verify whether system can correctly restricts multiple concurrent dialogue number of single user through multiple concurrent dialogue connection of system for two or more users; verify whether system can correctly restricts maximum concurrent dialogue connection number through system connection of beyond maximum concurrent dialogue connection number;

f) Evaluate major application system; use concurrent connection number beyond setting to connect system in a period of time and check whether the connection is successful

in order to verify the system function of restricting possible concurrent dialogue connection number in a period of time is correct;

g) Evaluate major application system; verify whether the system may be locked and unlocked and whether termination mode is the same with setting mode through setting terminal login operation timeout locking and authentication failure locking, stipulating unlocking or termination mode and causing operation timeout and authentication failure.

h) Evaluate major application system; verify system can correctly allow or deny users establishing dialogue connection based on security attributes through setting allowing or denying some user establishing dialogue connection based on security attributes (user identity, access address, time range, etc.) and then operating based on this user; verify whether system can correctly detect and give an alarm by trying make service level reduce to a predetermined minimum value.

Result judgment

a) If b) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

On contents, implementation process in application security level involves 9 work-units; see annex A.2.1.4 for specific contents.

7.1.2.1.5 Data security and backup recovery

1) Data integrity (S3)

Evaluation items

a) Be able to detect that integrity is damaged during collection, transmission, use and storage process of system management data, authentication information and important business data, and take necessary recovery measures after integrity error is detected.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, system administrator, major application system, design/inspection document, relevant supporting materials (e.g. certificates, inspection reports, etc.).

Implementation of evaluation

a) Interview security officer, inquiring whether there are business system data integrity supporting measures during transmission process, what the specific measures are, whether it can recover when integrity error is detected, what recovery measures are;

b) Inspect operating system, network equipment and database management system design/inspection document or related proof materials (e.g. certificate, inspection report, etc.); check whether there is description that it can detect/verify that integrity of system management data (e.g. WINDOWS domain management, directory management data), authentication information (e.g. user name and password) and user data (e.g. data file of user) is damaged during transmission process, that integrity of system management data and identity authentication information (e.g. access control rule of fire wall) is damaged during stored procedure and that integrity of important system is damaged, and that necessary recovery measures are taken when integrity error is detected; check whether the configuration is correct if there is relevant information;

c) Inspect major application system; check whether it is equipped with the function of detecting/verifying whether the integrity of system management data, authentication information and user data is destructed during transmission process, whether it is equipped with the function of detecting/verifying whether the integrity of system management data, authentication information and user data is destructed during storage process, whether it is equipped with the function of detecting whether the integrity of important system/module is destructed and whether it can take necessary recovery measures when integrity error is detected/verified;

d) Inspect major application system; check whether it has the function of detecting whether system integrity is destructed and whether it takes necessary recovery measures after detecting integrity error.

Result judgment

a) If b) in implementation of evaluation lacks relevant material, then this item is negative;

b) If b) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Data confidentiality (S3)

Evaluation items

a) Use encryption or other effective measures to ensure the confidentiality of system management data, authentication information and important business data during collection, transmission, use and storage process.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System administrator, network administrator, security officer, database administrator, major application system, design/inspection document, relevant supporting materials (e.g.

certificate, etc.).

Implementation of evaluation

a) Interview network administrator, inquiring whether authentication information of network equipment, sensitive system management data and sensitive user data in information system are encrypted or have other valid measures to ensure confidentiality of transmission and whether encryption or other protective measures are taken to achieve storage confidentiality;

b) Interview system administrator, inquiring whether authentication information of operation system, sensitive system management data and sensitive user data in information system are encrypted or have other effective measures to ensure confidentiality of transmission and whether encryption or other protective measures are taken to achieve storage confidentiality;

c) Interview database administrator, inquiring whether authentication information of database management system, sensitive system management data and sensitive user data in information system are encrypted or have other effective measures to ensure confidentiality of transmission and whether encryption or other protective measures are taken to achieve storage confidentiality;

d) Interview database administrator, inquiring whether authentication information of application system, sensitive system management data and sensitive user data in information system are encrypted or have other effective measures to ensure confidentiality of transmission and whether encryption or other protective measures are taken to achieve storage confidentiality;

e) Interview security officer, inquiring whether portable and mobile equipment are encrypted or use removable disk to store sensitive information;

f) Inspect operation system, network equipment, database management system and key application system design/inspection document; check whether there is such description on that authentication information, sensitive system management data and sensitive user data are encrypted or have other effective measures to transmission confidentiality and that whether encryption or other protective measures are taken to achieve storage confidentiality;

g) Inspect relevant proof materials (e.g. certificate or other related materials, etc.); check whether there is such description that communication channel of specific business communication conforms to national provisions;

h) Inspect major application system; check whether there is such description on that whether authentication information, sensitive system management data and sensitive user data are encrypted or have other effective measures to achieve transmission confidentiality and that encryption or other protective measures are taken to achieve storage confidentiality;

i) Evaluate major application system; obtain system transmission data package through sniffing toll; check whether encryption or other effective measures are taken to achieve transmission confidentiality.

Result judgment

a) If f) in implementation of evaluation lacks relevant material, this item is negative;

b) If there are no relevant proof materials (e.g. certificate, inspection report, etc.), then g) is negative;

c) If f) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Data backup and recovery (A3)

Evaluation items

a) Provide local data backup and recovery function; adopt real-time backup and asynchronous backup or incremental backup and full backup; incremental data is backed up once a day; full data is backed up once a week; backup medium is stored off-site; data storage life follows relevant national regulations;

b) Provide offsite data backup function and use communication network to transmit key data in bulk to standby site;

c) City-wide data backup center shall have a straight-line distance of at least 30 km from production center and can take over the operation of all core businesses; off-side data backup center shall have a straight distance of at least 100 km to production center; (F3)

d) Meet the requirements of disaster recovery policy; carry out verification test for the feasibility of application of key technologies in technical scheme; record and keep verification test results; (F3)

e) Data backup storage shall take the mode of redundancy and compete data backup shall ensure data redundancy with one week as the cycle;

f) Off-site backup center shall be equipped with the operating environment required for recovery, and shall be in ready state or running state; “ready state” means that the necessary resources (related hardware and software, data and other resources) of backup center have been fully satisfied, but the equipment’s CPU is not yet run; “running state” means that the CPU is also in running state, besides that all required resources of backup center are satisfied. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

System administrator, network administrator, database administrator, operating system, network equipment, database management system, major application system, design/inspection document.

Implementation of evaluation

a) Interview network administrator, inquiring whether network equipment in information system provides automatic backup mechanism for local and remote backup of important information, whether it provides the function of recovering important information, whether it provides important network equipment, communication lines and server hardware redundancy;

b) Interview system administrator, inquiring whether operation system in information system provides automatic backup mechanism for local and remote backup of important information, whether it provides the function of recovering important information;

c) Interview database administrator, inquiring whether database management system in information system provides automatic backup mechanism for local and remote backup of important information, whether it provides local system-level hot backup of important business system and whether it provides the function of recovering important information;

d) Inspect design/inspection document; check whether there is such description on that operation system, network equipment, database management system, application system have the configurations of local system-level hot backups and important information recovery function;

e) Inspect operation system, network equipment, database management system, major application system and check whether there is configuration of remote backup and important information configuration recovery function and whether the configuration and whether the configuration is correct;

f) Inspect whether important network equipment, communication line and server provide hardware redundancy;

g) Inspect whether important business system has local system-level hot backup function.

Result judgment

a) If there is no design/inspection document, d) in implementation of evaluation is negative;

b) If d) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

Data security class-evaluation involves network security, host security, application security, etc.; on content, implementation process on data security level involves 3 work-units; see annex A.2.1.5 for specific contents.

7.1.2.2 Security management evaluation

7.1.2.2.1 Security management system

1) Management system (G3)

Evaluation items

a) Develop overall policy and security strategy of information security work, indicating overall objectives, scope, principles and security framework of security work and forming security policy institutional document;

b) Establish security management system for management contents in security management activities;

c) Establish operation specification for daily management operations carried out by technological management personnel or operation personnel;

d) Form a comprehensive information security management system composed of security policy, management system, operation specification, etc.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, general guidelines, policy documents and security policy documents, list of security management systems, operation procedures, review record.

Implementation of evaluation

a) Inspect whether institutional system is composed of security policy, security strategy, management system, operation procedures, etc., whether management system is regularly reviewed and how long review period is;

b) Inspect general guidelines, policy documents and security policy documents of information security work; check whether document provides overall objectives, scope, policies, principles, responsibilities, etc.; whether security strategy of information system is defined;

c) Inspect security management system list; check whether it covers physical, network, host system, data, application, management and other aspects;

d) Inspect whether there are operation procedures of important management;

e) Inspect whether there is review record of security management institutional system; check whether recording date is consistent with review cycle and whether review opinions of relevant personnel are recorded.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Development and releasing (G3)

Evaluation items

a) Technology department of financial organization headquarter is responsible for developing security management system that applies to whole organization; the branch organizations are responsible for developing security management system in applicable jurisdiction; (F3)

b) Security management system shall have a uniform format and version control;

c) Organize relevant personnel to demonstrate and review developed security management system;

d) Security management system shall be released in a formal and effective way;

e) Release range of security management system shall be indicated and document sending and receiving shall be registered.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, management document of system development and issuance requirements, evaluation record, security management system, send-receive registration record.

Implementation of evaluation

a) Inspect whether security management system is uniformly developed under the leadership of information security leading group or committee and who participate in the development;

b) Interview security officer, inquiring the development procedures of security management system, whether security management system developed is demonstrated and reviewed, which demonstration and review mode is taken (e.g. convening review meeting, examination by letter, internal audit, etc.), whether it is developed based on unified format standard or requirement;

c) Develop management document of system development and issuance requirements; check whether the document provides security management system development and issuance procedures, format requirements, version number and other related contents;

d) Inspect management system review record; check whether there are review comments of relevant personnel;

e) Inspect whether the issuance process of security management system is formal and effective and which issuance way is adopted;

f) Inspect send-receive registration record of security management system; check whether send-receive meets prescribed procedures and requirements on issuance scope.

Result judgment

a) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Review and revision (G3)

Evaluation items

a) Information security leading group shall regularly organize relevant agency and relevant personnel to review the reasonableness and application of security management system;

b) Establish audit, management and monitoring mechanism for the publishing of website contents; (F3)

c) Regularly or irregularly inspect and review security management system; revise the management system that is imperfect or needs improvement.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, management personnel, security management system list, review record, list of corresponding responsible-persons and responsible departments for security management system.

Implementation of evaluation

a) Interview security officer, inquiring whether security management system is regularly reviewed and who/which department is responsible for the review;

b) Interview management personnel (personnel who are responsible for regular review, revision and routine maintenance), inquiring the regular review and revision of security management system and daily maintenance situation, review cycle, review and revision procedures and maintenance measures.

c) Interview management personnel (responsible-personnel), inquiring whether security management system is reviewed when system has major security incidents and new security vulnerabilities and when technical infrastructure and organizational structure changes, whether system that requires improvement is revised;

d) Inspect system revision and review record and security management system list that shall be periodically reviewed; check whether the list indicates review cycle;

e) Inquire whether security management system is regularly reviewed, whether revision is required when it is found imperfect or needs improvement, review cycle, revision procedures and maintenance measures;

f) Inspect security management system review record; check whether record date is consistent with review cycle, check whether there is revised version of security management system if the system has been revised;

g) Check whether there is review record of security management system when system suffers from major security accident of new security vulnerabilities, and when technological infrastructure and organizational structure changes greatly;

h) Inspect whether there is list of security management systems that require regular revision and check whether the list indicates review cycle;

i) Inspect whether there is a list of corresponding responsible-persons or responsible departments of all security management systems.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

Evaluation objects of security management system are mainly document information and work records related to 3 control points of management system, development and release, review and revision. See annex A.2.2.1 for specific contents.

7.1.2.2.2 Security management mechanism

1) Post setting (G3)

Evaluation items

a) Information security management work of financial organization is under unified leadership and level-to-level management; the headquarter has centralized leadership for information security management of branches; the organizations are

responsible for information security management of the organization and within the jurisdiction; (F3)

b) Establish a information security leading group that is led by the organization and composed of responsible-persons at relevant agency of business and technology to be in charge of information security management work of the organization and within the jurisdiction and decide major events on information security of the organization and within the jurisdiction;

c) Establish a dedicated information technology risk audit post, which is responsible for implementation of information technology audit system and procedures, developing and implementing information technology audit plan and auditing whole life cycle and major events throughout life cycle of information technology; (F3)

d) Establish a functional department for information security management work; set security officer and responsible-person posts on various levels of security management and define the responsibilities of responsible-persons;

e) Establish system administrator, network administrator, security administrator and other posts and define the responsibilities of various work posts;

f) Primary responsible-person of financial organization is the first responsible-person for computer information system security protection work in this organization. Computer information system security protection leading group of financial organization, full-time department and full-time (part-time) security management personnel and other relevant personnel shall assist the first responsible-person in implementing relevant provisions; (F3)

g) Adhere to principle of three-separation, including separation of foreground and background, separation of development and operation and separation of technology and business. Information technical personnel shall have specific responsibility for special post; business personnel may not serve concurrently or serve the concurrent post of business; (F3)

h) Except technical department, other departments shall designate at least one security officer of the department, who is specifically responsible for information security management work of the department and collaborates with technology department to carry out information security management work. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, responsible-person on some aspect of security management, responsible-person of leading group routine management work, system administrator, network administrator, security officer, department and post duty document, letter of

appointment authorization, work record.

Implementation of evaluation

a) Interview security responsible-person; inquire whether there is committer or leading group that guides or manages information security work; whether the top leader is appointed by the competent leader of the organization or authorized person;

b) Interview security officer, inquiring whether a full-time security management organization is set (e.g. functional department of information security management work), inquiring the settings of departments in the organization and whether assignment of responsibilities of departments is defined;

c) Interview security officer, inquiring whether responsible-persons on various aspects of security management are set, which inspections of job are set, whether the assignment of responsibility for various posts (e.g. post supervisor, responsible-persons on various aspects of security management, machine room administrator, system administrator, network administrator, security officer and other important posts) are defined;

d) Interview security supervisor and responsible-person on some aspect of security management, responsible-person of routine management work of information security management committee or leading group, system administrator, network administrator and security officer, inquiring which contents post responsibilities include;

e) Inspect department and post responsibility document; check whether the document defines the responsibilities of security management organization, whether it defines the responsibilities and division of labor for various departments in the organization, whether department responsibilities cover physical, network, system and other aspects; check whether the document clearly stipulates security supervisor and the principles on various aspects of security management, machine room administrator, system administrator, network administrator, security officer and other posts, whether the responsibilities of each post are clear, whether technical requirements for post personnel are defined and whether personnel are put on records;

f) Inspect whether information security management committee or leading group has letter of authority for top leadership from the competent leader of the organization;

g) Inspect the document on responsibilities of information security management committee and check whether the responsibilities of committee and the responsibilities of top leading post are defined;

h) Inspect whether information management departments and information security management committee or leading group has document or work record on implementation of routine management work (e.g. meeting minutes/summary, information security decision-making documents, etc.).

Result judgment

a) If the statement of interviewed personnel in d) in implementation of evaluation is consistent with document description, this item is positive;

b) If a) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Personnel allocation (G3)

Evaluation items

a) Allocate a number of system administrators, network administrators, security administrators, etc.;

b) Allocate full-time information security management personnel; implement A and B post system; concurrent post is not allowed;

c) Key affairs post shall be allocated several persons for co-management.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, personnel allocation requirement management document, list of management personnel.

Implementation of evaluation

a) Inspect personnel allocation document; check post division list and work shift at regular intervals (including work shift cycle, work shift procedures); interview security supervisor, inquiring the personnel allocation of security management posts (inquiring based on document of post responsibilities, including machine room administrator, system administrator, database administrator, network administrator, security officer and personnel at other important posts), including quantity, full time, part time, etc.;

b) Interview security responsible-person, inquiring the key posts of implementing regular work shift, regular work shift situation, work shift cycle, work shift procedures;

c) Inspect personnel allocation requirements management document; check whether it defines the allocation of security management personnel, whether it contains machine room administrator, system administrator, database administrator, network administrator, security officer and the personnel at other important posts and defines that full-time security officers shall be allocated; check whether it defines the key posts (list is required) that implement regular work shit, work shift cycle, work shift procedures, etc.;

d) Inspect post division list; confirm whether it contains specific information on machine room administrator, system administrator, database administrator, network administrator, security officer and the personnel at other important posts and whether security administrators are full-time;

e) Inspect the multi-management situation of key affairs post (e.g. regular work shift, work shift cycle, shift procedures, etc.).

Result judgment

a) If security officer referred to in a) in implementation of evaluation is full-time, this item is positive;

b) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Authorization and approval (G3)

Evaluation items

a) Define authorization approval matters, approval department, approver, etc., based on the responsibilities of departments and posts;

b) Establish approval procedures for system changes, important operation, physical access, system access and other matters; implement approval process based on approval procedures and establish level-by-level approval system;

c) Regularly review approval matters; timely update information on the items that require authorization and approval, approval department, approver, etc.;

d) Record approval process and keep approval document;

e) User shall be provided with the minimum permissions required to complete undertaken tasks; personnel at important tasks shall form a mutual restraint relationship. Changes of permissions shall follow relevant approval procedures and have complete change records; (F3)

f) Establish list of system users and permissions; regularly check the permissions of employees; find the reason and make adjustment in case of any unauthorized users discovered, meanwhile remove the permissions of expired users and record for filing. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, approver for key activities, authorization management document,

approval document, approval record, review record, authorization elimination record.

Implementation of evaluation

a) Inspect whether it is stipulated that key activities in information system shall be approved, which department is responsible for the approval, who approves, whether their approval activities are authorized, inquiring whether audit items are regularly reviewed and updated and how long review cycle is;

b) Inspect whether there are established approval procedures on system change, important operations, physical access, system access and other issues and whether approval process is based on approval procedures, inquiring the scope for approval of key activities (e.g. access to network system, application system, database management system, important server and equipment and other important resources development and issuance of important management systems, personnel allocation and training, product procurement, access of persons from a third party, management, project cooperated with operation unit, etc.) and specific approval procedures;

c) Inspect record on approval process of key activities; check whether recorded approval procedures are consistent with document requirements;

d) Inspect review records; check whether recorded data is consistent with review cycle;

e) Inspect whether there are permissions that are no longer applicable or there are records on that authorization is revoked.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Communication and cooperation (G3)

Evaluation items

a) Strengthen the cooperation and communication between various management personnel, between internal organizations and between internal functional departments of information security; convene coordination meetings regularly or irregularly to cooperate to deal with information security issues and form meeting minutes;

b) Strengthen the cooperation and communication with associate organizations, public security agencies and telecommunication companies;

c) Strength the cooperation and communication with suppliers, industry experts, professional security companies and security organizations;

d) Establish a contact list of external-access organizations, including name of external-access organization, contents of cooperation, contact person,, contact way

and other information;

e) Engage information security expert to serve as security consultant to guide information security construction and participate in security planning, security review, etc.

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, security management personnel, conference papers, meeting minutes, document on description of external-access organizations, list of security consultants.

Implementation of evaluation

a) Interview security supervisor, inquiring whether there is a mechanism for communication and cooperation with external-access organizations (public security agencies, telecommunication companies, associate organizations, suppliers, industry exerts, professional security companies, security organization, etc.) and with other departments in organization and personnel of internal management departments as well as contents of cooperation with external organizations and other departments, communication and cooperation way;

b) Inspect meeting documents and meeting minutes of information security leading group, coordination between departments, security inspection, etc.; check whether there is description on meeting contents, meeting time, participants, meeting results, etc.; interview security supervisor, inquiring whether department coordination meeting is convened to organize the personnel of other departments to jointly deal with information system security related issues, whether security management organization convenes an internal security work meeting to deploy the implementation of security work, which departments and who attend the meeting, what the meeting results are, whether information security leading group r security management committee regularly convenes meeting;

c) Interview security supervisor, inquiring whether information security expert is engaged as long-term security consultant to guide information security construction and participate in security planning, security review, etc.;

d) Interview security management personnel (randomly selected from system administrators and security officers), inquiring the ways of communication with personnel of external organizations, personnel of other departments in the organization and management personnel of internal departments as well as main communication contents;

e) Inspect department coordination meeting document and meeting minutes; check

whether there is description on meeting content, meeting time, participants, results, etc.

f) Inspect security meeting document or meeting minutes; check whether there is description on meeting content, meeting time, participants, results, etc.

g) Inspect regular meeting document or meeting minutes of information security leading group or security management committee; check whether there is description on meeting content, meeting time, participants, results, etc.

h) Check the list of external-access organizations; whether there is a mechanism of communication and cooperation with external-access organizations (public security agencies, telecommunication companies, associate organizations, suppliers, industry exerts, professional security companies, security organization, etc.), whether there is description on external-access organization contact person, contact way, etc.;

i) Inspect whether there is list of security consultants or documentary evidence of engaging security consultant; check relevant documents or records on that security consultants guides information security construction and participate in security planning and security review, whether there are relevant documents on that proposed information security experts approved by security consultant serve as long-term security consultant to guide information security construction and participate in security planning and security review, etc.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Audit and inspection (G3)

Evaluation items

a) Develop security audit and security inspection system to standardize security audit and security inspection work; regularly carry out security audit and security inspection activities based on requirements;

b) Security administrator shall be responsible for regular security inspection, which involves daily operation of system, system vulnerabilities, data backup, etc.;

c) Internal personnel or supervisions organization shall conduct comprehensive security inspection on a regular basis; inspection contents include the validity of existing security technical measures, the consistency of security configuration and security strategy, implementation of security management system, etc.

d) Prepare security inspection form; implement security inspection; summarize security inspection data to form security inspection report; if deadline rectification is required, relevant rectification situation shall be under follow-up tracking, and security

h) **Regular filing shall be conducted for log and statement of all kinds of information security product for at least 3 month;. (F3)**

i) **Timely upgrade and maintain information security products; all these product not in service life or unable to use anymore shall be disposed by approval procedures for fixed asset rejection. (F3)**

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, responsible-person for system construction, management system for product purchase, testing result record of product selection, check record of candidate products.

Implementation of evaluation

a) Interview security supervisor and inquiry whether there is specialized department for product purchase and which department;

b) Interview responsible-person for system construction and inquiry the purchase condition of system information security products, whether product selection is conducted in advance to confirm the candidate scope of products, whether there is product purchase list, how to control the purchase process, whether the candidate product list is regularly checked and updated and the check period;

c) Interview responsible-person for system construction and inquiry whether passwords products are used for system, and whether the use of products complies with the requirements of State Encryption Administration;

d) Inspect management system for product purchase and check whether it specifies the controlling method of purchase process (e.g. product selection before purchase, specifying product performance indicators needed, confirmation of candidate product scope) and standard of behavior;

e) Inspect whether relevant information security products used for system comply with state relevant regulations;

f) Inspect whether the use of passwords products comply with relevant regulations for passwords product use and management; for instance, *Regulations on the Commercial Passwords* specifies that any organization may only use commercial password products approved by the State Encryption Administration, any commercial password products malfunctioning may only be maintained by organizations assigned by State Encryption Administration, rejected products shall be filed by State Encryption Administration, *Temporary Regulations on Confidentiality for Computer Information System* specifies that secret-related system shall be equipped with

qualified equipment specialized for confidentiality, confidential measures taken shall be in line with the security level of information processed;

g) Inspect whether there are result record of product selection, checking record of candidate product list or updated list.

Result judgment

a) Under the implementation of evaluation, if c) no password products adopted as specified in the interview, c) and f) are negative;

b) If a) ~g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Self-developed software (G3)

Evaluation items

a) Formulate management system for software development and security regulations for code writing, specify the controlling method of developing process and standard of behavior for workers, require developers write code referring to the regulations, not allowed to write backdoor code or malicious code procedures; (F3)

b) Ensure that the separation of developing environment and physical environment for practical operation, **the separation of developers from testers**, **developers may not be system administrator or business operator**, evaluation data and result shall be under control;

c) Ensure that the relevant documents and manual for software design are offered and reserved by specially-assigned person;

d) Ensure the authorization and approval of modification, update and release of procedure resource library;

e) In the process of developing, compilation of relevant documents manuals shall be finished simultaneously to ensure the completeness and veracity of relevant materials. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction, relevant documents and manuals for software design, approval documents or records, controlling records for document use.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry whether the system develops software itself, whether there are authorization and approval for modification, update, release of procedure resource library and which department gives the authorization and who is the approver, whether there are corresponding measures for developing, whether require developer may not be testers (separation of them), whether it is written, tested and finished in an independent simulation environment;

b) Interview responsible-person for system construction and inquiry whether the system developing documents are reserved by specially-assigned person and who is that person, how to control use (e.g. restrict scope of users and use shall be registered), whether evaluation data and result are under control;

c) Inspect whether there are relevant documents for software design (design procedure documents for application software, illustration documents for source code and etc.), software user manual, maintenance manual and etc.;

d) Inspect whether the soft-developing environment is physically separated from the system-operating environment;

e) Inspect authorization and approval documents or records for the modification, update, release of procedure resource library, and check whether there is signature of approver;

f) Inspect there are use-controlling records for relevant documents of system software developing (documents for software design and developing procedures, evaluation data and result, maintenance manual and etc.)

Result judgment

a) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Outsourcing software development

Evaluation items

a) Test software quality according to development need;

b) Test malicious codes that are likely contained in software package before installation of software;

c) Require developing organization to offer relevant documents and manuals for software design;

d) Require developing organization to offer the source code of software, and check backdoor and covert channels likely contained in software;

e) Require outsourcing service provider to keep operation tracks and record

complete log, relevant contents and storage life shall meet the needs for event study, security forensics, independent audition, supervision and inspection; (F3)

f) **Require outsourcing service provider to implement risk evaluation for information security at least once a year, and submit the evaluation report, also require them to employ external institute to conduct security audition and submit the report so as to urge the provider to solve problems found; (F3)**

g) **Forbid subcontracting of outsourcing service provider and strictly control subcontract to ensure outsourcing service quality; (F3)**

h) **Make emergency plan for outsourcing in data center and substitute plan of provider to cope with service suspend or deterioration of service caused by bankrupt of outsourcing service provider, force majeure or other potential problems, which is to support continuous and reliable operation of data center. (F3)**

Evaluation modes

Interview and inspect.

Responsible-person for system construction, security protocol for software development, software development document, software training document.

Implementation of evaluation

a) Interview responsible-person for system construction, any inquiry whether before software outsourcing, there is written document (security protocol for software development) for software-developing organization to specify its responsibilities, security behavior in the developing process, developing environment requirements, software quality, post-development commitment and service, and etc.;

b) Interview responsible-person for system construction and inquiry whether there are documents needed for independent daily maintenance and use of software, whether developing organization offer technical supports for the normal operation and maintenance of software and how to offer.

c) Interview responsible-person for system construction and inquiry whether there is acceptance test for software function and performance based on the technical index in the development agreement before delivery, whether the test is jointly participated by both the developer and client; whether there is test for malicious codes before software installation, and whether the testing tool is commercial product form the third party;

d) Inspect software development agreement and check whether it specifies the ownership of intellectual property, security behavior and other contents;

e) Inspect whether there are need-analysis instruction, software design instruction, software manuals and other development documents, and user-training plan, processor-training manuals and other documents for later technical supports;

Result judgment

a) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Engineering implementation (G3)

Evaluation items

a) Make management system concerning Engineering implementation and clearly specify controlling methods and personnel behavior standards;

b) Designate and authorize specialized department or personnel for the controlling of engineering implementation;

c) Make detailed engineering implementation plan for controlling the implementing process; make relevant controlling documents for process controlling which shall be required to be formally put into practice by project-implementation organization;

d) Make integration and test plan for disaster recovery system and implement it. Ensure that the function and performance meet the requirements of design index by technical and service test; (F3)

e) Construction, upgrade and expand and other projects of network system shall go through scientific plan, full demonstration and technical check, and relevant materials shall be well-reserved and inspected by department supervisor. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction, project security construction agreement, engineering implementation plan and management system for engineering implementation.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry whether there is written form of constraint (e.g. project security construction agreement) for engineering implementation against the implementing party;

b) Interview responsible-person for system construction and inquiry whether specialize personnel or department is designated to conduct schedule and quality control in the

implementing process according to engineering implementation plan, whether the controlling methods and behavior standards for project personnel are systemized, whether project implementing organization is required to provide qualification proof and capacity guarantee for safe implementation of system construction;

c) Inspect project security construction agreement and check whether it specifies responsibilities, task requirements, quality requirements and other contents to constrain project implementing behavior;

d) Inspect engineering implementation plan and check it specifies project time limit, schedule control, quality control and other contents, whether various documents are formed according to implementation plan in the process, such as periodic project report;

e) Inspect management system for engineering implementation and check whether it specifies controlling methods in the implementing process (e.g. internal periodic control or controlling of external supervision organization), various behavior of implementation participants and other contents.

Result judgment

a) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Acceptance check of evaluation (G3)

Evaluation items

a) Written regulations are needed for controlling methods and personnel behavior standards of system-test acceptance check;

b) Undertaking organization (or department) or impartial third party shall make a security test plan to test system security and issue security test report which shall be submit to technology department for examination; (F3)

c) Acceptance check plan shall be made according to design plan or contract requirements before test acceptance check, acceptance check result for test shall be recorded in detail in the check process to form a report of test acceptance check;

d) Designate or authorize specialized department for the management of acceptance check for system test, and finish the check work according to requirements stipulated in the management;

e) Organize relevant agency and personnel to examine the acceptance check for system test and sign for confirmation;

f) Simulation operation not less than 1 month and trial operation not less than 3 months shall be taken before the new application system put into production. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction, evaluation plan, evaluation report, acceptance check report and management system for acceptance check and evaluation.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry whether evaluation agency from the third party is authorized to conduct independent security evaluation to information system based on design plan or contract requirements before formal operation of information system;

b) Interview responsible-person for system construction and inquiry whether specialized department is designated for acceptance check work of the evaluation and by which department, and whether the evaluation process (including before, in and after evaluation) is documented and systemized;

c) Interview responsible-person for system construction and inquiry whether relevant agency or personnel is organized to take conformity examination to the evaluation report based on the design plan or contract requirements;

d) Inspect project evaluation plan and check whether it specifies evaluation participant departments, personnel, on-site operation and etc.; check whether the evaluation record records the evaluation time, personnel, operation process, evaluation result and other contents; check whether the evaluation report presents problems existed and improvement suggestions;

e) Inspect whether there system acceptance check report;

f) Inspect whether management system for acceptance check and evaluation specifies the process controlling, participants and behavior of system acceptance check and evaluation.

Result judgment

a) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

8) System delivery (G3)

Evaluation items

a) Written regulation shall be set for controlling method and personnel behavior standards of system delivery;

b) Make a detailed system delivery list, based on which all delivered equipment, software and documents shall be checked;

c) System construction organization shall hand over all documents for construction process and system operation and maintenance to science-technology department after finishing the construction task; (F3)

d) System construction organization shall take corresponding technical training against technical personnel responsible for system operation and maintenance;

e) Designate or authorize specialized department for delivery management work and finish the work according to requirements in management regulations;

f) External construction shall sign relevant IPR agreement and confidential agreement with financial institute, not allowed to disclose the key security technology and core security function design. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction, system delivery list, letter of service commitment, system training record, and management system for system delivery.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry the delivery procedures, whether the delivery work is handled by specialized department based on the procedures, whether all the delivered equipment, documents, software and etc. are checked according to the delivery list, whether the delivery list meets the requirements of contract; whether the delivery work is systemized;

b) Interview responsible-person for system construction and inquiry whether the current information system is independently operated and maintained by internal personnel, if yes, whether the implementer of system construction takes training against operation and maintenance personnel and for which aspects, whether written commitment is made to offer certain technical support for system operation and maintenance, whether technical support has once been offered according to the letter of commitment and in which form, whether the system has documents needed for its independent operation and maintenance;

c) Inspect system delivery list and check whether it has system construction documents (e.g. system construction plan), documents to guide users for system operation and maintenance (e.g. operating instruction), system training manuals and other document names;

d) Inspect whether there are letter of service commitment from the system constructor

and training record to system;

e) Inspect management system for system delivery and check whether it specifies controlling method in the delivery process, behavior restrictions for delivery participants and other contents;

f) Inspect contract or agreement financial institute signs with external construction organization, whether there are relevant binding clauses to ensure. Measures for key security technique and design for core security function that the system adopts may not be disclosed.

Result judgment

a) Under the implementation of evaluation, if in a), d), no change to relevant documents due to absence of problems in delivery work, a) and d) is negative;

b) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) System filing (G3)

Evaluation items

a) Designate specialized department or personnel for relevant materials for the level of system management and control the use of these material;

b) System-level and relevant materials shall be reported to competent agency for filing;

c) System-level and other materials needed to be filed shall be reported to corresponding public security bureau for filing.

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, document administrator, and filing record.

Implementation of evaluation

a) Interview security supervisor and inquiry whether there are specialized personnel or department for the administration of documents concerning system-level, system attribute and so on, and by which department/person;

b) Interview document administrator and inquiry what controlling methods (e.g. restriction for using scope, record for using registration) are taken for documents of system-level, system attribute and so on;

c) Inspect whether there are filing records or documents for reporting system-level

documents and system attribute documentation and other materials to competent agency for filing;

d) Inspect whether there are filing records or proof for reporting system-level, system attribute, level basis and other filing materials to corresponding public security bureau for filing;

e) Inspect whether there are using control records for system-level documents and system attribute documentation.

Result judgment

a) If a) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

10) Class-evaluation (G3)

Evaluation items

a) In the process of system operation, at least one class-evaluation shall be taken to the system every year, and rectification and reform shall be taken timely to those not conforming to corresponding level protection standard;

b) Class-evaluation shall be taken timely to system once there is any change in the system. Level adjustment shall be taken timely along with security rectification and reform once there is change in the level, also rectification and reform shall be taken timely to those not conforming to corresponding level protection standard;

c) Choose evaluation organizations in the **"National Class-evaluation Agency Recommended Directory" approved by the Ministry of Public Security** for evaluation work and sign security confidential agreement with them;

d) Designate and authorize specialized department or personnel for the administration of class-evaluation.

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry whether there are relevant regulations and requirements and other documents for class-evaluation. Whether the annual class-evaluation, rectification and reform may be taken according to the requirements for the third system regulated by the Ministry of Public Security;

b) Interview responsible-person for system construction and inquiry whether the corresponding level protection requirements may be timely adjusted when there is change in the system-level;

c) Interview responsible-person for system construction and inquiry whether there relevant regulation for the choosing of class-evaluation institutes and whether there are relevant tracking documents;

d) Interview responsible-person for system construction whether there are specialized department or personnel for the administration of class-evaluation.

Result judgment

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

11) Selection of security service provider (G3)

Evaluation items

a) Assess its qualification, business behavior, performance, service system, service quality and other elements when choosing a service provider for information security; (F3)

b) Ensure that the choosing of security service provider conforms with the state relevant regulations;

c) Sign security-related agreements with security service provider to clearly contract relevant responsibilities;

d) Ensure that the security service provider chosen providers technical training and service commitment; service contract shall be signed if needed.

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system construction.

Implementation of evaluation

a) Interview responsible-person for system construction and inquiry whether the service provider for security planning, design, implementation, maintenance, evaluation and other service to the system conforms with the state relevant regulations.

Result judgment

a) If a) under the implementation of evaluation is positive, then this information system

satisfies the requirements of evaluation items of this unit.

The main evaluation objects of system construction management are relevant document materials of 11 controlling points as system-level, security plan designing, product purchase, self-developed software, outsourcing software development, engineering implementation, acceptance check of evaluation, system delivery, system filing, class-evaluation, and the choosing of security service provider. See details in Annex A.2.2.4.

7.1.2.2.5 System operation management

1) Environmental management (G3)

Evaluation items

a) Establish the centralized machine room to provide operation environment for information systems uniformly. The equipped facilities of machine room shall conform to the relevant standard request of national computer room;

b) Machine room shall adopt the structured cabling system, if the distribution equipment cabinet is equipped with HHT-LXB; the jumper shall be regular, the serial number of jumper and distribution frame shall be uniform and marked clearly; (F3)

c) Establish the security management system of machine room, make regulations about the management of physical access of machine room, the goods' in and out of machine room and the environmental security of machine room etc.;

d) Designate a department to take charge of the security of machine room, assign specially-assigned person to act as the administrator of machine room, patrol the operating condition of machine room regularly, maintain and manage the supply and distribution facilities, air-condition and temperature and humidity control facilities, fill in the duty records and patrol records of machine room;

e) The administrator of machine room shall receive relevant training and acknowledge the operating essentials of various facilities in the machine room; (F3)

f) Repair and maintain facilities in the machine room regularly and strengthen the maintenance of facilities or parts which are vulnerable and easy to fail; (F3)

g) The machine room personnel shall show the certificates issued by administration department when they need to get in and out of machine room; (F3)

h) Set weak current well and remain adequate expansible space; (F3)

i) The area where machine room locates shall install the 24-hour video surveillance device; the important area of machine room shall assign security guards to be on duty for 24 hours a day; the machine room shall implement the closed-off management; set one main entrance-exit and one or multiple entrance-exits; keep the entrance-exit control data, the intrusion alarm data and operating data of TV surveillance device

well, the storage life shall not less than 3 months, destroy the data of video etc. shall acquire the permission of leader of institution; (F3)

j) Strengthen the confidentiality management of work environment; regulate the behaviors of personnel in the work environment, including that the working personnel should submit the key of office immediately if he has transferred to another position, don't entertain visitors in the working zone, the working personnel should ensure the terminal computer is in the state of log out and there is no sensitive paper file on the desktop if he leave the seat.

Evaluation modes

Interview and inspect.

Evaluation objects

The responsible-person of physical security, the person on duty in the machine room, the working personnel in the machine room, the security management system of machine room, the management documents of work environment, the maintenance records of facilities, the registry form for in and out of machine room, the electronic access control system of machine room and its electronic recording.

Implementation of evaluation

a) Interview the responsible-person of physical security, ask whether the specially-assigned person or department of the basic facilities maintenance (such as air condition, the supply and distribution facilities etc.) of machine room regularly has been assigned, which is the department /person in charge and how long is the maintenance period;

b) Interview the responsible-person of physical security, ask whether specially-assigned person who takes charge of the security management work of machine room has been assigned and whether the systematism and documentation of the in and out of machine room have been required;

c) Interview the person on duty in the machine room, ask whether the in and out of visitors have adopt double control of manual recording and electronic recording;

d) Interview the working personnel; ask them about the confidentiality requirement of work environment;

e) Inspect the security management system of machine room, examine whether its contents have covered the physical access of machine room, the goods' in and out of machine room, the environmental security of machine room and so on;

f) Inspect the management documents of work environment, examine whether it has regulated the secrecy of working personnel after he leaves the seat (such as clearing the files in desktop and locking the screen and so on), the behaviors of personnel

after he has transferred to another position etc.;

g) Inspect the registry form of in and out of the machine room, examine whether the in-out time of visitors and the visiting reasons etc. have been recorded; examine whether there is the electronic access control system and whether the electronic recording has the information of time and visitors etc.;

h) Inspect the maintenance record of basic facilities in the machine room, examine whether the maintenance date, the maintaining person, the maintenance facilities, the fault causes and the maintenance results etc. have been recorded.

Result judgment

a) If the interviewee in clause c) can state the confidentiality announcements of work environment under the implementation of evaluation (such as the person shall log out when he leaves the seat and collects the sensitive documents well etc.), this item is positive;

b) If a) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Asset management (G3)

Evaluation items

a) Prepare and save the asset list which is relevant with information system, including the responsible department, the degree of importance and the location etc. of asset etc.;

b) Establish the security management system of asset, regulate the responsible-person or responsible department of asset management in information system and regulate the behavior of asset management and use;

c) Conduct identifying management on asset according to the degree of importance of asset and select the corresponding management measures according to the value of asset;

d) Regulate the classification and identifying methods of information; moreover, conduct standardized management on the use, transfer and save of information.

Evaluation modes

Interview and inspect.

Evaluation objects

The security supervisor, the responsible-person of physical security, the asset administrator, the asset list, the asset security management system, the documents of information classification and identity, the facilities

Implementation of evaluation

a) Interview the responsible-person of physical security, ask whether the specially-assigned person or department of asset management have been assigned and which is the department /person in charge;

b) Interview the responsible-person of physical security; ask whether the systematism and documentation of the asset management have been required;

c) Interview the asset administrator; ask whether the valuation and identifying management on asset have been conducted according to the degree of importance of asset, whether the different management measures have been adopted according to the different types of asset;

d) Inspect the asset list, examine whether its contents have covered the responsible-person of asset, the corresponding level, the location and the corresponding departments tec.;

e) Inspect the asset security management system, examine whether its contents have covered the use, borrowing and maintenance etc.;

f) Inspect the documents of information classification, examine whether it has regulated the principles and methods for classification and identifying (e.g. classify according to the degree of importance, the degree of sensitivity, and the different uses of information);

g) Inspect the facilities on asset list and examine whether they have the corresponding identifying.

Result judgment

a) If the interviewee in clause c) can describe the different asset management measures under the implementation of evaluation, this item is positive;

b) If the facilities identifying in clause g) conforms to the requirement of identifying in the information classification document under the implementation of evaluation, this item is positive;

c) If a) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Medium management (G3)

Evaluation items

a) Establish the security management system of medium, regulate the storage environment, the use, the maintenance and destruction etc. of medium;

b) Ensure to storage medium in the safe environment and have obvious identifying,

control and protect various medium, assign the specially-assigned person to manage the storage environment;

c) All the data shall backup and the storage of medium shall be stored in the antimagnetic, moisture-proof, dustproof, high temperature prevention and extrusion prevention environment; (F3)

d) Conduct security control over the personnel selection, packaging and delivery etc. during the physical transmission process of medium;

e) Conduct registry records for the filing and inquiry of medium, the administrator shall inspect regularly according to the category listserv of archive medium;

f) For the important document, conduct the lending registry system if it is the paper document, no one person can lend, copy or disclose it without the approval of leader of relevant agency; adopt the electronic office and approval platform, such as OA etc. to manage the electronic document; (F3)

g) Compile and update the technical documents as per the uniform format and achieve the requirement that it is able to recover the normal operation of system based on the technical documents; (F3)

h) Conduct content encryption and monitoring management on the storage medium which have been taken out of the work environment;

i) Clear sensitive data of the medium which need to be sent out to repair, the storage medium which have relatively high confidentiality cannot be destroyed without approval;

j) Report to relevant agency for the record for destruction of storage medium which are loaded with sensitive information, make destruction of information elimination, degaussing or physical crushing by the science-technology department and make the corresponding destruction records, the destruction process of information is restricted to the situation that the storage medium will still be used in the interior of financial institutions, otherwise, it shall make the irretrievable destruction of information; (F3)

k) Formulate the usage regulations of removable storage medium and verify the usage conditions of the removable storage medium regularly; (F3)

l) Establish multiple backup mechanisms for the important data, and storage at least 1 copy of backup in safe area of the same city or off-site which is specified by the science-technology department; (F3)

m) Adopt encrypted storage for data and software in the important medium; conduct classification and identifying management on medium according to degree of importance of the loading data and software;

n) Conduct validity period management on technical documents; lower the confidential

level of technical documents which are beyond the period of validity; regularly clear the technical documents which have lost efficacy and strictly execute the destruction and destruction supervision provisions in the management system of technical documents; (F3)

o) Recover and verify the main backup of business data regularly and dump data timely according to the service life of medium. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

The asset administrator, the management records of medium, the security management system of medium, the various kinds of medium, the storage area of medium and the off-site storage area.

Implementation of evaluation

a) Interview the asset administrator, ask whether there are protective measures in the storage environment of medium to prevent the medium from being stolen, destroyed, modified without approval and the illegal disclosure of information, whether there are specially-assigned person to manage;

b) Interview the administrator of asset; ask whether the systematism and documentation of usage management of medium have been required, whether the regular inspection on current usage conditions of medium has been conducted according to the category lists, whether the regular inspection on its integrity (whether the data have been damaged or lost) and usability (whether the medium have been damaged physically) has been conducted, whether the classification and identifying management of medium has been conducted according to the importance of its loading data and software;

c) Interview the asset administrator, ask whether the confidentiality process has been made for the medium which have been taken out of the work environment (e.g. be sent out to repair or destroy) and the data and software of important medium; whether the destruction of medium which have relatively high confidentiality has obtained the approval of leader, whether the data of medium which need to be sent out to repair or destroy have been purified; ask whether the physical transmission process of medium has selected the reliable transmission personnel and strictly controlled the packaging of medium (e.g. adopt the unpacking prevention devices), selection of the safe physical transmission way and the delivery of both parties at present;

d) Interview the asset administrator; ask whether some important medium have been off-site stored; whether the environment of off-site storage is the same with local environment;

e) Inspect the management records of medium, examine whether the storage, filing and lending of medium have been recorded;

f) Inspect the management system of medium, examine whether its contents have covered the storage environment, use, maintenance and destruction etc. of medium;

g) Inspect medium and examine whether the medium have been classified and have different identifying;

h) Inspect whether the practical environment of local storage of medium is safe, whether the environment and management requirement of off-site storage is the same with local and whether there is specially-assigned person to manage the storage area.

Result judgment

a) If a) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Equipment management (G3)

Evaluation items

a) Establish equipment security management system based on approval and in the charge of specially-assigned person so as to carry out standardized management to the selection, purchase, distribution, reception and other process of software and hardware equipment of information system;

b) Establish management system for supporting facility, and software and hardware maintenance to achieve effective maintenance management, including clarifying the responsibilities of maintenance personnel, approval of foreign-related maintenance and service, supervision and control over maintenance process etc.;

c) For equipment needed to be maintained by external organizations, work-related information existed shall be removed thoroughly and sign confidential agreement with equipment-maintenance factory, for supporting equipment of passwords equipment, ask R&D institute producing the equipment to remove password-related hardware before it is sent for maintenance, and dispatch specially-assigned person for on-site supervision; (F3)

d) Establish standardized procedures for failure process and detailed failure log (including the time, scope, phenomenon, process, result, processing personnel and other contents concerning failure); (F3)

e) Take standardized management to the operation and use of terminal computer, workstation, portable computer, system, network and other equipment, achieve the start/stop, power-up/power-off and other operation of main equipment (including backup and redundancy equipment) according to operation instruction;

f) Science-technology department of every institute shall be responsible for the

maintenance management of all equipment (including backup and redundancy equipment) and circuit related to information system; (F3)

g) Newly-purchase equipment shall be test for qualification before put in use; (F3)

h) Registration work for equipment shall be done well, equipment management regulations shall be made and security protection responsibilities for equipment-user shall be implemented; (F3)

i) For equipment which needs abolishing, its data information shall be removed by science-technology department by using special tools; if the abolished equipment will be out of use or transferred to the organizations other than the financial institute, degaussing, physical smashing or other unrecoverable destruction shall be conducted to its memory equipment of data information by science-technology department, and file for this; (F3)

j) Ensure that information-processing equipment may only be taken away from computer room or office location upon approval.

Evaluation modes

Interview and inspect.

Evaluation objects

Asset manager, system manager, controller, management document for equipment approval, equipment operation instruction, management document for equipment sue, management system for equipment, software and hardware maintenance system, server operation log, and configuration document.

Implementation of evaluation

a) Interview asset manager and inquiry whether there are specially-assigned person or department to take regular maintenance to all equipment, which department / person dose the maintenance word and the period;

b) Interview asset manager and inquiry whether there is approval control over every procedure of equipment selection (e.g. model selection, purchase, distribution and so on), whether there is approval control over institute who takes the equipment away, whether the operation and use of equipment is under standardized management;

c) Interview system manager and inquiry whether the server is correctly configured under unified security strategy, whether the operation of server is in compliance with operation instruction;

d) Interview system manager and inquiry whether he takes systemized management to software and hardware maintenance;

e) Interview controller and inquiry whether log is established for server operation, how

the log document is managed, whether regular check is taken to the management condition;

f) Inspect management document for equipment approval and distribution and check it specifies the report and approval of equipment selection, purchase, distribution, equipment-taken-away institute and other procedures; check whether there are report material and approval report for equipment selection, purchase, distribution and other procedures;

g) Inspect management document for equipment use and check whether it covers the use and operation principles, precautions and other contents of terminal computer, portable computer, network and other equipment;

h) Inspect server operation instruction and check whether it covers the start, stop, power-up, power-off and other operations;

i) Inspect software and hardware maintenance system and check whether it covers the responsibilities of maintenance personnel, approval of foreign-related maintenance and service, supervision and control over maintenance process and other aspects.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Monitoring management and security management center (G3)

Evaluation items

a) Monitoring alarming work shall be conducted to communication line, network equipment, mainframe, operation condition of application software, network flow, user behavior and etc., which shall be recorded and well-kept;

b) Establish weekly, monthly or quarterly report system for operation monitoring of computer system to count and analyze operation condition; (F3)

c) Regular analysis, review shall be taken against monitoring and alarming record to discover suspicious acts and form report, **any significant hidden danger and operational accident shall be immediately coordinated and settled, and reported to relevant agency of higher organization;**

d) Establish security management center to take centralized control over equipment condition, malicious code, patch updating, security audit and other security-related events.

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for system operation, and monitoring record document.

Implementation of evaluation

a) Interview responsible-person for system operation and inquiry whether he monitors resource index of main server, such as the usage of CPU, memory, process disk and etc.

b) Interview responsible-person for system operation and inquiry whether the operation of current information system is in the charge of institute itself, if so, how the documents from system operation (e.g. letter of responsibilities, certificate of authorization, license, strategy documents, accident report and settlement document, security configuration document, system logs and so on) are managed;

c) Inspect monitoring record and check whether it records monitoring object, monitoring content, settlement of abnormal phenomenon monitored and so on.

Result judgment

a) If a) ~ c) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Network security management (G4)

Evaluation items

a) Designate special person for network management, responsible for operation log, daily maintenance of network monitoring record, and the analysis and settlement of alarming information, **all this work shall be signed by operation and re-check personnel; maintenance record shall be well-kept for at least 3 months;**

b) Establish management system for network security operation, which specifies network security configuration (the minimum service configuration), log-kept time, security strategy, patching and patch updating, command update period, **backup of important file** and other aspects;

c) Establish management regulations for network access, access plan shall be examined by science-technology department before network access of any new equipment which may only have access to network and be distributed with corresponding network resources;

d) Establish controlling regulations for remote access, remote access needed for work shall be approved by the science-technology department of access-sponsoring institute, and submitted to the science-technology department (position) of accessed institute for starting remote access, and security protection measures like separated account, distribution of minimum permission, timely close of remote access service and so on shall be taken;

(F3)

e) Every institute reasonable controls the scale and scope of multi-medium by the principle of not affecting normal network transmission, cross-jurisdiction VOD offered in internal network or other multi-medium network applications which severely occupy network resources is not allowed unless being approved by science-technology department; (F3)

f) After approval of supervisor and leader of the department, management personnel of information security have access to security test and scanning of network of the institute or jurisdiction, testing and scanning result is sensitive information which may not be disclosed, any external institute or personnel is not allowed to test or scan internal network without authorization from science-technology department; (F3)

g) Security management mode of unified regulation, classified management, and responsibilities shall be taken against network interworking security of financial industry, under which any institute itself may not interwork network with external institute without approval from science-technology department of financial institute; (F3)

h) Regular threat and vulnerability assessment shall be taken for all application system of network interworking and external network zone; assessment report shall be provided. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, security officer, network manager, auditor, network vulnerability scanning report, system external-access authorization, network auditing log.

Implementation of evaluation

a) Look up management system for network security and check whether it covers network security configuration (security strategy for network equipment, authorization access, minimum service, patching and updating), kept time of auditing log, updating and patching and other aspects; interview security supervisor and inquiry whether special person is designated for maintenance of network operation log and monitoring record, analysis and settlement of alarming information and other security management work;

b) Interview security officer and inquiry whether the management work for network security (including network security configuration, network user, log and etc.) is systemized; look up the division of network manager and retrieve maintenance files for network security operation;

c) Retrieve files for network security technique training which network manager participates, check configuration for network-interworking equipment and compare it with approval record;

d) Retrieve record from monitoring system of illegal external-access, and check on the international internet-access machine whether there is sensitive working information saved;

e) Interview security offer and inquiry the variety of network external-access (internet, enterprise network of partner, higher department network and so on), whether they are all authorized and approved and by which department/person; whether there is regular inspection of illegal networking;

f) Inspect controlling settings for remote access on relevant network equipment and retrieve examination record of remote access;

g) Inspect whether is cross-jurisdiction restriction on network video service, whether cross-on demand is approved by science-technology department;

h) Interview network manager and inquiry whether there has been updating for network equipment according to the updated version offered by provider, what is the version No. of current version, whether there is backup of important files (account and configuration data and so on) before updating and how it is updated; whether there is vulnerability scanning to network equipment, and whether the vulnerability is timely patched;

i) Inspect backup file of network equipment configuration and how the minimum service configuration of network equipment is achieved, and retrieve off-line backup of configuration files;

j) Retrieve the approval and change time and backup of configuration in the network change record;

k) Inspect authorization from confidential department on the application record of computer accessing to international internet;

l) Inspect report for network vulnerability scanning and check whether it covers network vulnerabilities, severity level, reason analysis, improvement suggestions and other aspects;

m) Inspect management system for network security and check whether it covers network security configuration (including security strategy for network equipment, authorization access, minimum service, updating and patching), network account (user’s responsibilities, obligations and risks, rights approval and distribution, account logout), auditing log, generation, backup and change approval of configuration file, compliance inspection and so on;

n) Inspect whether there are all authorization instruments of ratification for

external-access of internal network; retrieve record for computer use change;

o) Inspect virus of information downloaded online;

p) Inspect there is network auditing log during the kept time specified.

Result judgment

a) If a) ~ p) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) System security management (G4)

Evaluation items

a) Establish management system for system security which concretely specifies security strategy, security configuration, log management, daily operation procedures and other aspects;

b) Designate special person for system management, divides roles of system management personnel and clarity the rights, responsibilities and risks of each role, the set of rights shall comply with the principle of minimum authorization;

c) System manager may not be the business operator at the same time, and he may not add, delete or modify any business data; if system manager does have to take business data maintenance to the database system, he shall get a written agreement from business department; maintenance content, personnel time and other information shall be recorded in detail; (F3)

d) One vulnerability scanning shall be taken at least every half year; system security vulnerability discovered shall be patched timely; scanning result shall be reported to the leadership; (F3)

e) Install latest system patch program, the installation may only be implemented after passing the test in the testing environment and backing up of important files, and this system change shall be recorded;

f) System maintenance shall be based on operation manual, operation record shall be recorded in detail, including important daily operation, operation and maintenance record, setup and change of parameter and other contents, **two people shall be on the ground for the system setup of important computer system;**

g) Regular analysis shall be taken to operation log and audit-data for timely discovery of abnormal behavior;

h) Change in system user's rights shall be recorded in written and approved by relevant management level. (F3)

Evaluation modes

Interview and inspect.

Evaluation objects

Security supervisor, security officer, system manager, auditor, management system for system security, system auditing log, system vulnerability scanning report.

Implementation of evaluation

a) Interview security supervisor and inquiry whether special person is designated for system security management; inspect regulations on system security strategy, security configuration, log management, daily operation procedures and other aspects in the organization's squadron of security management system;

b) Interview system manager and inquiry whether measures are taken to control using personnel and number for the use of system tool (e.g. vulnerability-scanning tool));

c) Interview system manager and inquiry whether regular installation of security patch program to system, whether it is tested for its impact on application system in the testing environment; whether important files (system configuration, system user's data and etc.) are backed up before installation of system patch, and how; whether vulnerability scanning is taken to system, and whether the vulnerabilities discovered are timely patched;

d) Interview security officer and inquiry whether the management work of system security (including system security configuration, system account, auditing log and etc.) is systemized;

e) Interview system manager and inquiry whether certain settlement measures (e.g. deletion or forbidden) are taken to stop the continual use of default user for not commonly-used system; whether regular inspection and analysis are taken to management condition of system account security;

f) Interview auditor and inquiry whether the kept-time of system auditing log is specified and how long it is;

g) Inspect whether there is system auditing log during the kept-time specified;

h) Inspect report for system vulnerability scanning and check whether it covers system vulnerabilities, severity level, reason analysis, improvement suggestions and other aspects;

i) Inspect management system for system security and check whether it covers system security configuration (including system security strategy, authorization access, minimum service, updating and patching), system account (user's responsibilities, obligations and risks, rights approval and distribution, account logout), auditing log, generation, backup and change approval of configuration file, compliance inspection and so on.

room and underground water transfer and penetration phenomena occur;

c) Inspect whether there are design/inspection documents for building waterproof and moisture-proof, and whether they can meet waterproof and moisture-proof demands of machine room and conform with the actual situation of waterproof and moisture proof in machine room;

d) If there are pipes of passing through primary machine room wall and floor, check whether there are necessary protection measures like casing pipes and so on;

e) Inspect whether machine room has been free from leakage, penetration and phenomena whether machine room and the environment have obvious leakage and damping threats, and whether leakage, penetration and damp can be promptly repaired and resolved in case of their occurrence;

f) In high-humidity areas or seasons, check whether machine room has humidity records, whether there are humidification devices that can operate properly, whether there are measures to prevent transfer and penetration of machine room underground water, whether there are records waterproof and moisture-proof processing and dehumidification devices, and whether they are consistent with machine room humidity records.

g) If machine room is under great threat of leakage, inspect whether there is water-sensitive instrumentation or part to test and alarm waterproof, and check whether the instrumentation or part works properly and its operation records, and whether there is someone responsible for the checking work.

Result judgment

a) Under the implementation of evaluation, if “if” conditions in d), f), g) are false, then this item is negative;

b) If a) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Anti-static (G4)

Evaluation items

a) grounding anti-static measures shall be taken for equipment;

b) Anti-static floor shall be adopted for machine room;

c) Shoe cover shall be prepared for entry into machine room to reduce dust brought; (F4)

d) Static eliminator shall be adopted to reduce static

e) Static conduction or static dissipation materials shall be used for working

platform of primary machine room and auxiliary areas. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for physical security, maintenance personnel for machine room, machine room equipment, anti-static design/inspection documents, humidity record, dehumidification operation record.

Implementation of evaluation

a) Interview responsible-person for physical security and inquiry whether machine room adopts necessary grounding anti-static measures and whether there are measures to control machine room humidity; whether there are anti-static measures to strong-static areas in machine room;

b) Interview maintenance personnel for machine room and inquiry whether machine room humidity is regularly checked and controlled within the scope prescribed in GB2887, inquiring whether machine room has static problem or failure event caused by static; whether static elimination measures are taken immediately for existing static;

c) Inspect whether there are anti-static design/inspection documents and their compliance with actual situation;

d) Inspect whether machine room has safe grounding, whether relative humidity of machine room conforms to the provisions of GB2887 and whether machine room is free from significant electrostatic phenomenon.

e) If it is strong-static areas, inspect whether there are measures like anti-static floor, anti-static workbench, static inhibitor, static eliminator and so on taken for machine room; check the dehumidification operation records of using static inhibitor and eliminator;

f) In strong-static areas, evaluate whether relative humidity conforms with regulations in GB2887.

Result judgment

a) Under the implementation of evaluation, if in e) effective anti-static measures include all or part of measures like anti-static floor and workbench, static-inhibitor or eliminator, etc., then this item is positive;

b) Under the implementation of evaluation, if “if” conditions in e), are false, then this item is negative;

Responsible-person for physical security, maintenance personnel for machine room, machine room equipment, design/inspection documents for temperature and humidity control, temperature and humidity record, operation and maintenance record.

Implementation of evaluation

a) Interview responsible-person for physical security and inquiry whether machine room is equipped with constant temperature and humidity system to ensure temperature and humidity can meet the needs of computer equipment operation, whether temperature and humidity control requirements are specified in machine room management system, and whether there is someone responsible for it;

b) Interview maintenance personnel for machine room and inquiry they regularly inspect and maintain automatic adjustment equipment of temperature and humidity in machine room, inquiring whether there has been events of temperature and humidity affecting system operation;

c) Inspect whether there are design/inspection documents for temperature and humidity control in machine room, whether they can meet the needs of system operation, and whether they conform with current actual situation;

d) Inspect whether constant temperature and humidity system can work properly, check temperature and humidity record, operation and maintenance record; check whether machine room temperature and humidity meet the requirements in GB2887-89”Specification for Computation Center Field”.

Judgment Criterion

a) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

9) Power supply (A4)

Evaluation items

a) Power supply of computer system shall be separated from others; (F4)

b) Configure voltage stabilizer and over-voltage protection device on power supply line of machine room

c) Based on the principle of duplicate supply, set redundant or parallel power cable lines for power supply of computer system;

d) Provide short-term backup power supply (e.g. generators) in case of power off of provisional power supply; ensure backup up power supply is in place during UPS in power supplying; simulation drilling of backup power supply shall be taken annually; regular overhaul and maintenance shall be taken for backup power supply to ensure its normal functioning;

e) Redundancy mode of UPS power supply shall be N+1, N+2, 2 (N+1) and so on, with load power less than 80% of UPS rated power and by two independent AC offering UPS input, UPS backup time shall be at least 4 hours. Core areas and important equipment shall be supplied by different UPS double circuit; (F4)

f) There shall be special socket for machine room where there shall be set with power socket for maintenance and test respectively with obvious mark for each. AC and UPS power sockets shall be separated to meet the requirements of load; (F4)

g) Copper wire cable shall be used for computer system. Mixture of copper and aluminum shall be avoided, if unavoidable, transition contact shall be used to connect them; (F4)

h) Machine room shall be set with indicator light emergency light and exit, all switches, handles and buttons in power supply cabinet and distributor shall be clearly marked to avoid mis-operation. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for physical security, maintenance personnel for machine room, machine room equipment, design/inspection documents for power supply security, check and maintenance record.

Implementation of evaluation

a) Interview responsible-person for physical security, inquiring whether power supply lines of computer system are separated from other power supply, whether power supply lines of computer system are installed with voltage stabilizer and over-voltage protection device, whether power supply lines of computer system are installed with short-term backup power equipment (e.g. UPS) and whether power supply time meets minimum power supply demand of system; whether redundant or parallel power cable line (e.g. duplicate supply); whether backup power supply (e.g. generators) is established.

b) Interview maintenance personnel for machine room, and inquiry whether voltage stabilizer, over-voltage protection device, short-term backup power equipment, etc. on power supply lines of computer system are regularly inspected and maintained, whether power supply voltage stabilization range can be controlled sot that computer system is normally operating;

c) Interview maintenance personnel for machine room and inquiry whether redundant or parallel power cable line can normally supply power to computer system when it switch over in duplicate supply; whether backup power supply (e.g. generators) is

regularly checked, and whether it can star and supply power normally in specified time;

d) Inspect whether machine room has design/inspection documents for power supply security; check whether documents indicate separate power supply of computer system is separated as well as the requirements of equipping voltage stabilizer, over-voltage protection device, backup power equipment, and redundant or parallel power cable line, etc.; check whether they conform with actual situation of machine room power supply;

e) Inspect power supply lines of computer and check whether power supply of computer system is separated from other power supply;

f) Inspect machine room and check whether voltage stabilizer, over-voltage protection device and short-term backup power supply on power supply line of computer system are operating normally;

g) Inspect whether there are inspection and maintenance records of stabilizer, over-voltage protection device, short-term backup power source, redundant or parallel power cable line switchover, backup power supply operation, and operation records of power supply to the above computer system; whether they can conform with the requirements for system normal operation;

h) Evaluate whether redundant or parallel power cable line (e.g. duplicate supply) installed can achieve duplicate supply switchover;

i) Evaluate whether backup power supply (e.g. generators) can start and supply power normally in the specified time;

j) Inspect redundancy mode of UPS power supply shall use N+1, N+2, 2N, 2 (N+1) with load power less than 65% of UPS rated power and by two independent AC offering UPS input. For organizations without diesel generator emergency power supply, UPS backup time is at least 2 hours; core areas and important equipment are supplied by different UPS double circuit.

Result judgment

a) If a) ~j) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

10) Electromagnetic protection (S4)

Evaluation items

a) Grounding shall be adopted to prevent external electromagnet interference and equipment parasitic coupling interference;

b) Power lines and communication cables shall be separately laid to prevent mutual interference.

c) Electromagnetic shielding shall be used for key area and **important equipment**;

d) Network wiring of computer system equipment shall not be parallel to that of passive electromagnetic shielding for air-conditioning and power supply equipment; if overlapped, they shall try to be made in square crossing with extended fire prevention measures taken. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for physical security, maintenance personnel for machine room, machine room equipment, electromagnetic protection design/inspection documents, electronic shielding devices or design/inspection documents for shielding machine room, electromagnetic leakage evaluation report.

Implementation of evaluation

a) Interview responsible-person for physical security and inquiry whether there are measures to prevent external electromagnetic interference and equipment parasitic coupling interference (equipment housing has good grounding, power line, communication wires and cables isolation, etc.); whether electromagnetic leakage prevention measures are taken against equipment for secret information; whether electronic shielding is adopted for machine room or shielding machine room is installed when necessary;

b) Interview maintenance personnel for machine room and inquiry whether equipment housing has good grounding, whether power lines and communication cables are isolated, whether there are any failures due to external electromagnetic interference and other problems; whether equipment for secret information is low-radiant and is installed with 2nd-rated electromagnetic effect jammer required by BNB4-2000”Specifications and Methods of Measurement on Electromagnetic Interference ”;

c) Inspect whether there are electromagnetic protection design/inspection documents and their conformity with actual situation; whether there are design/inspection documents for electronic shielding or shielding machine room; whether there are management system documents for electronic shielding or shielding machine room;

d) Inspect whether machine room equipment housing has safe grounding;

e) Inspect machine room wiring and check whether power lines and communication cables are isolated;

f) Inspect the starting up of secret-related equipment with electromagnetic effect jammer, and whether the jammer is started up simultaneously.

g) If electronic shielding is adopted for machine room, inspect whether it is open when there is equipment operating in machine room; if shielding machine room is installed, inspect whether power lines and non-optical communication lines go through filter, whether optical communication lines through waveguide, whether machine room door is closed timely, electromagnetic leakage is regularly evaluated for shielding machine room, and check evaluation report for electromagnetic leakage;

h) If electronic shielding is adopted for machine room or shielding machine room is installed, evaluate electromagnetic situation of shielding machine room (Refer to GB12190-90 ”Methods of Measurement on High Shielding Performance”).

Result judgment

a) Under the implementation of evaluation, if “if” conditions in g), h) are false, then this item is negative;

b) If a) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

In content, implementation process of physical security evaluation involves 10 work-units; see annex A.3.1.1 for specific inspection table.

7.1.3.1.2 Network security

1) Structural security (G4)

Evaluation items

a) Ensure that the redundancy of **main network equipment and communication lines**, **business processing capacity of main network equipment** is as **2 times as needed** for business rush hours; **dual-line design shall be offered by different service provider;**

b) Ensure that the bandwidth of every part for network meet the needs of business rush hours;

c) Route control shall be conducted between business terminal and server to establish safe access path;

d) Draw network topology structure chart consistent with current operation;

e) Divided into different subnets or network segments based on job functions and significance of various departments as well as importance degrees of information involved, etc. and distribute address fields to networks and network segments in accordance with the principle of facilitating management and control; **production net, internet and office net shall achieve effective isolation**.

f) Avoid important network segment from being placed at network boundary and directly connecting to external information system, reliable technology isolation shall be

adopted between important segment and other segments;

g) Specify the priority level of broadband distribution according to its importance to business service so as to ensure preferential protection to important host during network congestion hours;

h) Use premises equipment to achieve the isolation between inter-institute networking system and business host system of net-in financial institutes so as to prevent external system from direct access and operation to business host of net-in financial institutes; (F4)

i) Special network which shall be separated from public data network shall be used for significant information exchange between financial institutes; (F4)

j) Institute shall access to inter-institute transaction and exchange network by at least 2 backbone links, choosing special communication links according to actual situation. 2 backbone links shall have different route control where the another one can load all transaction data when an exception happens to one. (F4)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Network manager, boundary and important network equipment, network topological graph, network design/inspection documents.

Implementation of evaluation

a) Interview network manager and inquiry the performance of boundary and important network equipment of information system as well as the flow during rush hours;

b) Interview network manager and inquiry network segment division and principle of division, inquiring important network segments and protective measures for important network segments;

c) Interview network manager and inquiry bandwidth of network, inquiring bandwidth control and bandwidth allocation principles;

d) Interview network manager and inquiry control policies and measures of route on network equipment and the design purpose of these policies;

e) Inspect network topological graph; check whether it is consistent with current operating conditions;

f) Inspect network design/inspection documents; check whether boundary and important network equipment bandwidth occupation statement have records conforming to or

exceeding processing capacity;

g) Inspect network design/inspection documents; check whether there are descriptions on division of different subnets or network segments based on job functions and significance of various departments as well as importance degrees of information involved, etc. and allocation of address fields to networks and network segments in accordance with the principle of facilitating management and control;

h) Inspect boundaries and important network equipment; check whether route control policy (e.g. using static route, etc.) is used to establish a secure access patch and check whether the nodes of access patch conforms to route control policy at business terminal trace business server address;

i) Inspect boundary and important network equipment; check whether important network segments are deployed to network boundary for direct connection with external information system, whether important network segments and other network segments are isolated by firewall, access control and other means;

j) Inspect boundary and important network equipment; check whether there are polices to broadband control (e.g. route control, QQS policy configuration on exchange equipment, configuration policy for special broadband management equipment, etc.) and whether these policies can ensure the preferential protection to significant businesses (e.g. the priority level of significant business host shall be higher than that of insignificant one) during network congestion hours;

k) Evaluate network topological graph structure by which the auto discovery and drawing tools can be achieved, and whether the actual network topological graph is consistent with the network topological graph can be tested;

l) Evaluate the access path between business terminal and server, and test whether the path is safe (e.g. Whether the path if fixed) by using tracer;

m) Evaluate important network segments, and test whether the measures that their network address is binding with data link address, or data link address with switch port taken are effective (e.g. trying to use non-binding address, checking whether normal access is allowed and etc.);

n) Evaluate network broadband distribution policies, and test whether the distribution is effective by using broadband evaluation tools;

o) Interview network manager whether the special network for networking between net-in banks and information exchange center is separated from public data network;

p) Interview network manager whether premises equipment is used for the isolation between inter-bank networking system and business host system of net-in bank so as to prevent external system from direct access and operation to net-in bank business host;

q) Interview network manager whether institutes access to inter-bank transaction and exchange network by at least 2 backbone links, and choose DDN, FR or other communication links based on actual situation. 2 backbone links shall have different route control where the another one can load all transaction data when there is an exception to one;

r) Interview network manager whether institutes have at least one backup line (e.g. dial-up line) connected to inter-bank transaction and exchange network, backup link shall be able to load all transaction data when there is an exception to both backbone links;

s) Interview network manager and inspect whether the connection between institutes and exchange center is solely confirmed by local IP address and port number, remote IP address and port number.

Result judgment

a) If f) ~ g) under the implementation of evaluation are lack of corresponding documents, then this item is negative;

b) If e) ~ s) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Access control (G4)

Evaluation items

a) Deploy access control devices at network boundary and start access control functions;

b) Data with general protocol is not allowed to go through;

c) Allow or deny the data going through according to data sensitive marks;

d) Remote-dial access shall not open;

e) Decide to allow or deny resource access of users to controlled system in accordance with allowed access rules between users and system; control granularity is single user;

f) Monitor **network maximum flow and network concurrent connection** at network area boundary (internet area, external and internal area boundary)

g) Network equipment shall be set with access control rights according to minimum security access. (F4)

Evaluation modes

Interview, inspect and evaluation.

Evaluation objects

Security officer, **network manager**, boundary and important network equipment.

Implementation of evaluation

a) Interview security officer and inquiry network access control measures taken; inquiry design principles of access control policies; inquiry whether the policies have been adjusted and the situation before and after adjustment;

b) Inspect important network equipment and check whether there are corresponding access measures (e.g. VLAM, access control list, MAC address binding) taken to forbid the access to network of portable and mobile equipment;

c) Inspect boundary network equipment and check whether there are corresponding access control measures taken to forbid data going through with general protocol;

d) Evaluate boundary and important network equipment, and whether access control measures for network equipment are effective by trying using mobile equipment for network access;

e) Evaluate boundary and important network equipment, and whether access control measures are effective to stopping the connection by transmitting data with general protocol (e.g. http tunnel tool).

f) Restrict the physical access of wireless access points, gateways and handheld equipment;

g) Shut down network communication ports not in use;

Result judgment

a) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Security audit (G4)

Evaluation items

a) Make log records on network equipment running state, network flow, user behavior, etc. in network system;

b) Audit records shall include event date and time, user, event type, whether audit is successful and other information related to audit;

c) Analyze and generate statement according to recorded data;

d) Protect audit records from unexpected deletion, modification or coverage, with **retention time not less than 1 year;**

e) Define the threshold value of audit trail limit, when memory is close to limit, necessary measures may be taken to prevent audit-data lose;

f) Achieve centralized audit by the unified security strategies of information system, clock shall be synchronous with clock server.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Auditor, boundary and important network equipment (including security equipment).

Implementation of evaluation

a) Interview auditor and inquiry whether boundary and important network equipment in network system are audited and the audit contents, inquiring the main contents of audit records, inquiring audit record processing mode;

b) Inspect audit records of log server or AAA server; check whether there are records on network equipment running state, network flow, user behavior and other events in network system;

c) Inspect log server or AAA server event audit policies; check whether it involves event data and time, user, event type, success case of event and other audit related information.

d) Inspect log server or AAA server; check whether true-time alarm with specified mode can be offered to specific events; (e.g. sound, email, message, etc.)

e) Inspect log server or AAA server; check whether the it has statement-generation function (e.g. classification, sequence, inquire, statistics, analysis, combined inquire, etc. of audit record) for the browse and analysis of audit-data by authorized users, and generate audit statement according to their needs;

f) Inspect log server or AAA server; check whether audit trail set defines the threshold value of audit trail limit, whether necessary measures can be taken when memory is run out, such as alarming and deriving, abandoning unrecorded audit information, suspending audit or covering previous audit records, etc.;

g) Evaluate log server or AAA server; test whether the coverage and record state of security audit is consistent with requirements by some user trying causing some significant security-related events (e.g. failure of identity identification and etc.);

h) Evaluate log server or AAA server; test whether the protection state of security audit is consistent with requirements by some user trying deleting, modifying or covering audit records;

i) Evaluate log server or AAA server; test whether they can track and monitor possible security events, and whether their function to stop illegal process is correct (e.g. generating certain security events, then checking whether security audit can test them and stop their process).

Result judgment

a) If b) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Boundary integrity inspection (S4)

Evaluation items

a) Be able to inspect unauthorized equipment connecting to internal network without permission, pinpoint its position and block it effectively;

b) Be able to inspect internal network users connecting to external network without permission, pinpoint the position and block them effectively.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, **network manager**, boundary integrity test equipment, running log for test equipment of boundary integrity

Implementation of evaluation

a) Inspect boundary integrity test equipment; check whether there are network access of computers that are installed with illegal external connected client end; if any, whether positioning and blocking are adopted;

b) Inspect running log for boundary integrity test tool; **check whether operation is normal (check whether whole network segment is continuously monitored);**

c) Inspect boundary integrity test tools; check whether illegal connection to internal and external network are monitored; check whether illegal connection is effectively blocked;

d) Inspect boundary network equipment; check whether it is set with relevant measures which are able to block important information outflow (network equipment mark, specified route control information mark) according to information flow controlling policy and information flow sensitive mark;

e) Evaluate boundary integrity test tools and check whether “illegal external-access” behavior (e.g. generating illegal external-access action, checking whether boundary

integrity inspection tools can discover the behavior in a timely manner) can be effectively discovered.

f) Evaluate boundary integrity test tools and check it can confirm the position of “illegal external-access” equipment and effectively block it (e.g. generating illegal external-access, then checking whether boundary integrity equipment can position accurately and block it);

g) Evaluate boundary integrity test tools and check whether unauthorized equipment connecting to network without permission can be inspected, pinpointed and effectively blocked (e.g. generating illegal connection, then checking and evaluating whether boundary integrity equipment can discover, positioning and the connection accurately, and blocking it).

Result judgment

a) If b) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Intrusion prevention (G4)

Evaluation items

a) Monitor following attacks at network boundary: port scanning, brute force attacks, Trojan backdoor attacks, denial of service attacks, buffer overflow attacks, injection attacks, IP fragmentation attacks, network worm attacks, etc.

b) Any attacks tested shall be recorded with attack source IP, attack type, attack object, and attack time; there shall be alarm and automatic corresponding actions when severe intrusion happens;

c) Management system for intrusion test shall be classified with distribution by degrees to system deployment. (F4)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, network intrusion prevention devices.

Implementation of evaluation

a) Interview security office, inquiring network intrusion prevention measures, inquiring whether there are special devices to guard against network intrusion, inquiring, inquiring the measures taken to upgrade network intrusion prevention rule base;

b) Inspect network intrusion prevention equipment, and inquiry whether following attacks

may be detected: port scan, brute force attack, Trojan backdoor attacks, denial of service attacks, buffer overflow attacks, IP fragmentation attacks, network worm attacks;

c) Inspect network intrusion prevention equipment, and check whether intrusion event records include intrusion source IP, attack type, attack object, attack time, etc.; check whether there are security-alarming modes (e.g. true-time screen tips, E-mail alarming, sound alarming, etc.);

d) Inspect network intrusion prevention equipment, and check whether its manufacturer is qualified and whether rule base is the latest;

e) Evaluate network intrusion prevention equipment, and verify whether the monitoring policies are effective (e.g. simulating to generate attack action, checking the reaction of network intrusion prevention equipment);

f) Evaluate network intrusion prevention equipment, and verity whether the monitoring policies are effective (simulating to generate attack action, and checking the reaction of network intrusion prevention equipment can alarm in true time).

Result judgment

a) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

6) Malicious code prevention (G4)

Evaluation items

a) Test and remove malicious code at the network boundary of **external organizations connecting to internet;**

b) Code base and system shall be updated regularly to malicious code prevention equipment.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, malicious code prevention products, design/inspection documents, running log of malicious code prevention products.

Implementation of evaluation

a) Interview security officer; inquiry preventive measures for network malicious code prevention in system; inquiry update polices for malicious code base; inquiry main functions of malicious code prevention products; inquiry whether there are security

events of malicious code intrusion in system;

b) Inspect design/inspection documents; check whether they have measures taken to malicious code at network boundary and core business network segments (e.g. whether there are anti-virus gateways), whether there is description for true-time update function of malicious code prevention products;

c) Inspect running log of malicious code prevention products and check whether the products keep running;

d) Inspect whether at network boundary and core business network segments, measures are taken to test and remove malicious code in network layer according to features of malicious code;

e) Inspect malicious code prevention products, and check whether they are from qualified manufacturers and works properly or not, whether malicious code base id the latest version;

f) Inspect configuration policies for malicious code prevention products, and check whether they support the unified management of malicious code prevention (e.g. Checking whether it is distributed deployment, centralized management and etc.).

Result judgment

a) If b) under the implementation of evaluation lack of corresponding documents, then this item is negative;

b) If b) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

7) Network equipment protection (G4)

Evaluation items

a) Authenticate the identify of users who log onto network equipment;

b) Restrict the administrator login address of network equipment;

c) Identification of network equipment user shall be unique

d) Important network equipment shall choose 2 or more than 2 combined authentication technologies for identity authentication to the same user;

e) Identity authentication information shall have the feature of not being illegally used; password shall have complexity and be replaced regularly;

f) At least one kind of identity authentication information of network equipment users shall be unforgeable;

g) There shall be login failure processing function; measures of terminating dialogues, restricting illegal logins, exiting automatically in case of network login connection timeout;

h) For remote management of network equipment, necessary measures shall be taken to prevent bugging of authentication information during network transmission process;

i) Achieve the separation of rights for equipment privilege users;

j) Sort out built-in service ports of network equipment system; turn off unnecessary system service ports and establish corresponding port openness approval system; (F4)

k) Test software version information of network equipment quarterly, and take corresponding update by effective evaluation and verification; (F4)

l) Establish clock synchronization mechanism of network equipment; (F4)

m) Monthly back up the configuration documents of network equipment, any change shall be timely backed up; (F4)

n) Quarterly inspect and lock or cancel unnecessary users' account in network equipment. (F4)

Evaluate modes

Interview, inspect and evaluate.

Evaluation objects

Network manager, boundary and important network equipment (including security equipment).

Implementation of evaluation

a) Interview network manager and check whether there is AAA certification or other certification mode for network equipment. In case that AAA server is logged in, check whether user matches administrator identity and permissions;

b) Interview network manager, inquiring password policy of network equipment;

c) Inspect security settings of boundary and important network equipment; check whether there are settings to take appropriate measures for identification failure and there is a function to limit illegal login frequency;

d) Inspect security settings of boundary and important equipment; check whether there are restrictions on administrator login address of main network equipment; check whether there is automatic exit in case of network login connection timeout; check

whether right separation of equipment privileged users is achieved; check whether peer entities on the network are authenticated on identity; evaluate security settings of boundary and important equipment, and verify whether identification failure processing measures are effective (e.g. Logging in network equipment with wrong passwords for several times, and observing whether the dialogue is ended and restrict illegal login times), and verify whether the function of restricting administrator login address of network equipment is effective (e.g. Logging in with any random address, observing the movement of network equipment);

e) Evaluate security settings of boundary and critical network devices; verity whether the setting of automatic exit in case of network login connection timeout is effective (if there is no operation under long-time connection, observe the action of network equipment);

f) Make penetration evaluation for boundary and important network devices; use a variety of penetration techniques (e.g. password guessing solution, etc.) for penetration evaluation for network devices; verify whether protective capacity of network equipment meets requirements;

g) Make remote login of network devices and check whether 22 ports SSH modes or other encryption modes are adopted;

h) Look up backup documents on computer;

i) Check checklist whether there is weekly inspection to running state of network equipment;

j) Inspect whether unnecessary network equipment services are closed;

k) Spot interview network equipment manager whether software information version of network equipment is checked weekly and recorded in written, and updated correspondingly by effective test and verification;

l) Interview network equipment administrator, inquiring whether there is weekly inspection and lock or revocation of redundant user account in network equipment.

Result judgment

a) If password policy of network equipment involves password length of more than 8 digits and password complexity (e.g. stipulating that characters shall be a mixture of upper and lower case letters, digits and special characters), password life cycle, new password and old password replacement requirements (stipulating number of replaced characters) or use of token in order to facilitate memory, then b) under the implementation of requirements meets evaluation requirements;

b) If b) ~ h) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

In terms of content, implementation process of evaluation in network security level involves 7 work-units; see annex A.3.1.2 for specific contents.

7.1.3.1.3 Host security

1) Identity authentication (S4)

Evaluation items

a) Label and identify the identify of users who log in operating system and database system;

b) Identification label of operating system and database system management users shall have the feature that illegal use is not easy; **static password of key system shall have more than 8 digits and are a mixture of letters, numbers, symbols and other components and be changed at least once a month**;

c) Start login failure processing function; measures of terminating dialogues, restricting illegal login intervals and times, automatic exit, etc. may be adopted;

d) Set identification alarm information, based on which system may automatically prompt unauthorized access when there is exceeding access or trying illegal access;

e) Host system shall conduct identifying label and authentication to severs or terminal equipment it connected to; for remote management of servers through internet, necessary measures shall be taken to prevent bugging of information during network transmission process;

f) Allocate different user names to different users of operating system and database system to ensure that user name is unique;

g) 2 or more than 2 combined authentication technologies shall be adopted for identity authentication of management users, and at least one kind of identity authentication information is unforgeable, **such as key certificate, dynamic password card, biological features and etc. (F4)**

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, database manager, key server operating system, key database management system, server operating system documents, database management system documents.

Implementation of evaluation

a) Inspect whether identity authentication function of server operating system and database management system has at least the 2nd level or TCSEC2 evaluation report in “Information Security Protection-Security Techniques Requirement for Operating System” and “Information Security Protection-Security Techniques Requirement for Database Management System”’

b) Interview system manager, and inquiry the measures taken to achieve identity label and authentication system of operating system; inquiry identity authentication and authentication failure processing measures offered currently by system;

c) Interview database manager, and inquiry the measures taken to achieve identity label and authentication system of operating system; inquiry identity authentication and authentication failure processing measures offered currently by system;

d) Inspect server operating system and database management system documents; check the attributes of guaranteeing the uniqueness of user identity authentication (e.g. user name, UID, etc.);

e) Inspect key server operating system and key database management system; check whether there are identity authentication measures (e.g. user name, password, etc.) and whether identify authentication information has the feature that illegal use is not easy; check account password policy setting, e.g. efficient password length, password complexity (e.g. stipulating a mixture of upper and lower case letters, figures and special characters), password life cycle, new and old password replacement requirements (e.g. stipulating character amount for replacement) or token is used to facilitate memory;

f) Inspect key server operating system and key database management system; check whether at least 2 technology combinations of identity authentication are adopted for identity authentication (e.g. adopting 2 random combinations of identity authentication technologies as user name/password, challenge response, dynamic password, physical equipment, bio-identification technology and digital certificate), and at least one of them is difficult to forge (e.g. digital certificate or bio-identification technology);

g) Inspect key server operating system and key database management system; check whether they are equipped with authentication failure processing function and limit value for illegal login times based on which logins exceeding limit value shall be terminated with their authentication dialogue and account be closed; check whether network login connection timeout automatic exit are set;

h) Inspect important server operating system, and check whether server operating system has identity label and authentication of servers or terminal equipment connected;

i) Evaluate key server operating system and key database management system; verity whether authentication failure processing function is effective by trying logging in

system with wrong user name and password;

j) Evaluate key server operating system and key database management system; check whether it is needed marking first (e.g. establishing account) before logging in system while users without label is unable to log in;

k) Evaluate key server operating system and key database management system; add a new user whose user label is the system original one (e.g. user name or UID), and then check if it will work out;

l) Evaluate key server operating system and key database management system; delete a user label, and then add a new user whose label is the one of the deleted (e.g. user name or UID), and check whether it will work out;

m) Evaluate key server operating system; by using host without identity label and authentication to connect to the server, verity whether host system may correctly conduct identity marking and authentication of servers or terminal equipment it connects to;

n) Penetration evaluation shall be taken to key server operating system; test the strength of user password to server operating system by using password cracking tools, check whether user passwords can be cracked and whether it is able to log in system after cracking;

o) Penetration evaluation shall be taken to key server operating system; verity whether existing unauthorized account (e.g. some new accounts added by system after being served) is able to take interactive login management with system;

p) Penetration evaluation shall be taken to key server operating system; whether the evaluation uses system log-in methods bypassing authentication, such as security flaws existing in authentication process, social engineering or other methods;

q) Inspect whether users of server operating system, database and affiliated groups or UID are unique.

Result judgment

a) If a) under the implementation of evaluation is positive, then j), k), and l) are positive;

b) If user name/password is not adopted for identity authentication, then n) under the implementation of evaluation is inapplicable;

c) Under the implementation of evaluation, if in o) passwords can get cracked, then n) is inapplicable;

d) Under the implementation of evaluation, if in p) there are no common system log-in method bypassing authentication, then this item is positive;

e) If e) ~ m) in evaluation implementation are positive, then this information system

satisfies the requirements of evaluation items of this unit.

2) Security mark (S4)

Evaluation items

a) Sensitive marks shall be set to all subjects and objects.

Evaluation modes

Inspect and evaluate.

Evaluation objects

Key server operating system, key database management system, security strategies.

Implementation of evaluation

a) Inspect whether the security marking function of server operating system and database management system has at least the 2nd level or TCSEC2 evaluation report in “Information Security Protection-Security Techniques Requirement for Operating System” and “Information Security Protection-Security Techniques Requirement for Database Management System”;

b) Inspect security marks of server operating system and database management system, and check whether subject and object sensitive marks are clarified.

3) Access control (S4)

Evaluation items

a) Control the access of subjects to objects based on security strategies and all sensitive marks set for subjects and objects;

b) Granularity of access control shall achieve that subjects are user or process level, and objects are file, database table, record and field level;

c) Distribute privileges according to the role of managing users to achieve the separation of managing users’ privileges with minimum privileges needed for managing users authorized;

d) Achieve the privilege separation of privileged users for operating system and database system, **system manager may only have the privilege to operation management of operating system while database manager only the privilege to operation management of database;**

e) Forbid or strictly restrict the access privilege of default accounts by renaming system default accounts and modifying default passwords of these accounts;

f) Timely delete redundant or delinquent accounts to avoid shared account existing.

Evaluation modes

Inspect and evaluate.

Evaluation objects

Key server operating system, key server database system, security strategy.

Implementation of evaluation

a) Inspect whether discretionary access function of server operating system and server database system has at least the 2nd level or TCSEC2 evaluation report in “Information Security Protection-Security Techniques Requirement for Operating System” and “Information Security Protection-Security Techniques Requirement for Database Management System”’

b) Inspect security strategy of server operating system and server database system; check whether it clarifies subjects with users or user group identity (e.g. users) specify access control to objects (e.g. file or system equipment, access control for catalog and access control lists, etc.), whether its coverage includes subjects directly related to information security (e.g. users) and objects (e.g. files, database table, etc.) and operations between them (e.g. read, write or execute);

c) Inspect security strategy of server operating system and server database system; check whether it clarifies subjects have non-sensitive marks (e.g. roles), and specifies the access to objects based on the marks;

d) Inspect the access control lists of key server operating system and key server database system; check whether there are delinquent and useless accounts in authorized users; whether users and privileges in access control lists are consistent with security strategy;

e) Inspect key server operating system and key server database system; check whether owner of objects (e.g. files, database table, records, fields, etc.) can change the property of its corresponding access control list, whether authorized users can change property of corresponding object access control list;

f) Inspect the access control lists of key server operating system and key server database system; check whether the privileges of privileged users are separated, such as being divided into system manger, security manage, security auditor, etc.; check whether minimum authorization principle is adopted (e.g. system manger may only have access to system maintenance while security manager only to strategy configuration and settings, and security auditor maintenance of auditing information, etc.);

g) Inspect key server operating system and key server database system; check whether there are interactive relationships among system manager, security manager and security auditor (e.g. system and security manager may not manage auditing log

while security audit manager may not manage the auditing log of start, close, deletion, and other events of audit-data, etc.);

h) Check key server operating system and key server database system; check whether the access privileges of anonymous/default users are forbidden or strictly restricted (e.g. restricted in limited range);

i) Check key server operating system and check whether anonymous/default users are forbidden;

j) Evaluate key server operating system and key server database system; according to security strategy of system access control, try accessing to objects with unauthorized users/roles and verify whether the access is not allowed.

Result judgment

a) If a) under the implementation of evaluation is positive, then e) and j) are positive;

b) If b) ~ j) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Trusted path (S4)

Evaluation items

a) When identity authentication to users remotely accessing to operating system and database system through the internet is under implementation, a safe information transmission path shall be established between system and users;

b) When users are remotely accessing to operating and database system through the internet, a safe information transmission path shall be established between system and users.

Evaluation modes

Interview and inspect.

Evaluation objects

Security manager, key server operating system, key database management system, server operating system documents, database management system documents.

Implementation of evaluation

a) Inspect whether the trusted path function of server operating system and database management system has at least the fourth-class-evaluation report in “Information Security Protection-Security Techniques Requirement for Operating System” and “Information Security Protection-Security Techniques Requirement for Database Management System”;

b) May interview security manager and inquiry under what circumstance that trusted path is started to conduct initial login/authentication; what trusted paths have been offered by system currently;

c) Inspect server operating system documents and check the trusted path functions offered by system;

d) Inspect key server operating system and check whether trusted paths declared in documents are effective;

e) Interview security manager and inquiry under what circumstance that trusted path is started to conduct initial login/authentication; what trusted paths have been offered by system currently;

f) Inspect database management system documents and check the trusted path functions offered by system;

g) Inspect key database management system and check the trusted path functions offered by system.

Result judgment

a) If a) under the implementation of evaluation is positive, then d) and g) are positive;

b) If d) and g) under the implementation of evaluation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Security audit (G4)

Evaluation items

a) The scope of audit shall cover each operating system user and database user of server and critical client side;

b) Audit contents shall contain critical user behavior, abnormal use of system resources and use of critical system orders, **distribution**, establishment and change of accounts, adjustment of auditing strategies, start and close of audit system function and other critical security-related events in system;

c) Audit records shall contain date and time, type, subject label, object label, event result, etc., **and audit records shall be regularly backed up with retention time not less than 1 year**;

d) Analyze according to recorded data and generate audit statement;

e) Protect audit process from unexpected interruption;

f) Protect audit process from unexpected deletion, modification or coverage, etc.;

g) Achieve centralized audit according to unified security strategy of information system.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security auditor, key server and critical terminal operating system, key database management system.

Implementation of evaluation

a) May interview security auditor; inquiry whether host system is set with security audit; inquiry the selection requirements and strategies for host system to event auditing; processing methods to audit log;

b) Inspect key server operating system, critical terminal operating system and key database management system, and check whether the current auditing scope covers every user;

c) Inspect key server operating system, critical terminal operating system and key database management system, and check whether audit strategy covers important security-related events in system, such as users' label and authentication, all operation records for discretionary access control, critical user behavior (e.g. changing user identity and deleting system table by using super user order), abnormal use of system resources, use of critical system orders (e.g. deleting objects), etc.;

d) Inspect key server operating system, critical terminal operating system and key database management system; check whether audit record information contains event date and time, subject and object triggering events, event type, success or failure of events, request source of identity authentication event (e.g. end marking symbol), event result, etc.;

e) Inspect key server and critical terminal operating system; check whether special auditing tools are offered to authorized users to browse and analyze audit-data (e.g. classification, sequence, inquire, statistics, analysis, combined inquire, etc.), and generate audit statement according to their needs;

f) Inspect key server operating system, critical terminal operating system and key database management system, and check whether they can designate true-time alarming mode to specific event (e.g. sound, email, message, etc.);

g) Inspect key server operating system, critical terminal operating system and key database management system; check whether audit trailing setting defines the threshold value of audit trailing limit; when memory is close to limit value, necessary measures may be designated (e.g. alarming and deriving); when memory is run out,

auditable events may be terminated;

h) Inspect key server, critical terminal operating system and key database management system, and check whether connecting port for centralized audit is offered and can transmit audit-data according to requirements of centralized system;

i) Inspect the clock of key sever, and check whether it is synchronized with clock server;

j) Evaluate key server operating system, critical terminal operating system and key database management system; by illegal terminating audit function or modifying its configuration, verity whether audit function is under protection;

k) Evaluate key server operating system, critical terminal operating system and key database management system; try generating some critical security-related events in system by using certain user in system, and then evaluate whether coverage of security audit is consistent with recorded situation;

l) Evaluate key server operating system, critical terminal operating system and key database management system; try deleting, modifying or covering audit records by using certain user in system, and then evaluate whether protection situation of security audit is consistent with requirements;

m) Evaluate key server operating system, critical terminal operating system and key database management system; generate some security events, and then check whether security audit can trail and monitor these events and terminate illegal process.

Result judgment

a) If b) ~m) under the implementation of evaluation are positive during evaluation, this information system fulfills the requirements of evaluation.

6) Residual information Protection (S4)

Evaluation items

a) Ensure the memory space where authentication information of operating system and database management system users shall be totally removed before being freed or re-allocated to personnel for use, no matter whether this information is stored in disk or memory;

b) Ensure that the memory space of files, catalogs and database records, etc. in system shall be totally removed before being freed or re-allocated to other personnel for use.

Evaluation modes

Interview and inspect.

Evaluation objects

System manager, database manager, maintenance/operation manual for key server operating system, maintenance/operation manual for key database management system.

Implementation of evaluation

a) Inspect whether redundant information protection function of server operating system and database management system has at least the 2nd class-evaluation report in "Information Security Protection-Security Techniques Requirement for Operating System" and "Information Security Protection-Security Techniques Requirement for Database Management System";

b) Interview system manager; inquiry whether the memory space of authentication information for system operating system users is totally removed before being freed or re-allocated for other users; whether the memory space of files, catalogs in system is totally removed before being freed or re-allocated to other users;

c) Interview database manager; inquiry whether the memory space of authentication information for database manager users is totally removed before being freed or re-allocated for other users; whether the memory space of database records and other resources is totally removed before being freed or re-allocated to other users;

d) Inspect maintenance/operation manual for key server operating system and key database management system; check whether it clarifies the processing methods and process to the memory space of user's authentication information before its being freed and re-allocated to other users, processing methods and process to the memory space of files, catalogs, database records, etc. before its being freed and re-allocated to other users;

Result judgment

a) If a) under the implementation of evaluation is positive, then b) and d) are positive;

b) If b) ~d) under the implementation of evaluation are positive during evaluation, this information system fulfills the requirements of evaluation.

7) Invasion prevention (G4)

Evaluation items

a) Be able to test invasion behavior to key servers, record invasion source IP, attack type, attack object, attack time, and alarm when there are severe invasion events;

b) Be able to test the integrity of important process, and take recovery measures when testing invasion damage or **block in advance when testing there will be invasion damage soon**;

c) Operating system shall comply with the principle of minimum installation with only needed modules and application processes installed, and keep the timely update of system patches by setting update server, preventive maintenance service to system

software and other methods.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, key server system.

a) Interview system manager; inquiry whether there are preventive measures taken to host system, whether invasion prevention contents contain host-running monitoring, resource use exceeding pre-warning value, specific process monitoring, invasion behavior testing, integrity testing, etc.;

b) Interview system manager; inquiry the manufacturer and version of invasion prevention products, and the installation and deployment state of the products in host system; inquiry whether there is deployment improvement or product replacement, whether products are updated according to requirements (e.g. true-time or regular update);

c) Inspect key server system; check whether host running is monitored, whether monitoring contents contain the use condition of host CPU, disk, memory, network and other resources with using history given;

d) Inspect key server system; check whether resource alarming threshold value is set (e.g. threshold value for CPU, disk, memory, network and other resources) for alarming when resource using is exceeding specified value, and check alarming methods;

e) Inspect key server system; check specific processes are monitored (including primary system processes like Explorer process of WINDOWS), whether illegal process list can be set;

f) Inspect key server system, and check host accounts (e.g. system manager) is controlled to restrict addition and modification, etc. to important accounts;

g) Inspect key server system; check whether it can record attacker’s source IP, attack type, attack object, attack time, etc., whether alarming is offered when there are severe invasion events (e.g. sound, message, email, etc.), whether blocking to some events is contained in its response processing methods and configured for use;

h) Evaluate key server system, and verify whether it can restrict the running of illegal process by trying running an illegal process; verify whether host can restrict the addition and modification of important accounts by trying adding or modifying important accounts;

i) Evaluate key server system, and verify whether host can test the integrity damage of important process by trying damaging important process (e.g. executing important

process of system task).

Result judgment

a) Under the implementation of evaluation, if in b) the manufacturer is authorized (e.g. sales license), and the edition is new, the improvement is reasonable and the software is updated periodically, this item is positive.

b) If a) ~i) in evaluation implementation are positive, this information system fulfills the requirements of evaluation.

8) Malicious code prevention (G4)

Evaluation items

a) Install genuine malicious code prevention software certificated by the **state security department**; **for malicious code checking and killing software attached to virus base,** version of malicious code prevention software and malicious code base shall be timely updated; f**or malicious code defensing software not relying on virus base like proactive defensing software, effectiveness and timeliness of feature database adopted by software shall be ensured; for system unable to be installed with corresponding software, other security protection measures shall be taken to ensure the system free from malicious code attack;**

b) Malicious code prevention products of host shall have different malicious code base from those of network;

c) Support the unified management to malicious code;

d) Establish virus-monitoring center to monitor computer infection in network. (F4)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Security officer, key server, key terminal, network malicious code prevention products, hose security design/inspection documents.

Implementation of evaluation

a) Interview security officer; inquiry whether true-time testing, checking and killing measures of malicious code are taken to host system, and the deployment of these measures; why deployment is improved or products is replaced, whether products are updated as required (e.g. regular or real-time update);

b) Inspect design/inspection documents concerning malicious code prevention to host,

and check the described installing scope contains server and terminal equipment (including mobile equipment);

c) Inspect key server system and terminal system; check whether software products that are true-time testing, checking and killing malicious code are installed; check whether software products that are true-time testing, checking and killing malicious code support unified management of malicious code prevention; check the manufacturer, version number and malicious code base name of testing and checking software products of malicious code;

d) Inspect network malicious code prevention products, and check their manufacturer, version number and malicious code base name.

Result judgment

a) Under the implementation of evaluation, if in a) deployment of true-time testing, checking and killing measures to malicious code covers all servers and important terminals, then this item is positive;

b) If a) ~d) under the implementation of evaluation are positive and it is inspected that different malicious code databases are used by the host system and network malicious code prevention products (e.g. different manufactures, version numbers and the names of malicious code databases), then this information system satisfies the requirements of evaluation items of this unit.

9) Resource control (A4)

Evaluation items

a) Restrict the login of terminal through the setting of the terminal connection methods and the scope of network address, etc.;

b) Set the login terminal overtime operation locking based on the security strategy;

c) Monitor key sever, including monitoring the using condition of server CPU, disk, memory, network and other resources;

d) Restrict the maximum or minimum limit of single user to use the system resources;

e) Regular planning shall be made to system performance and capacity, able to test and alarm when system service level decreases to pre-set minimum value;

f) All servers shall be customization, not used for email collecting and internet browse. (F4)

Evaluation modes

Inspect and interview.

Evaluation objects

Key server operating system.

Implementation of evaluation

a) Inspect key server operating system; check whether multi-concurrent dialogue quantity of single user is restricted; check whether login terminal overtime operation locking and authentication failure locking are set, and whether it specifies the unlocking or terminating method; check whether terminal connecting method and network address scope, etc. restrict the terminal login;

b) Online inspection: whether host operating system, database and important application system set the overtime terminal login locking according to the security strategy;

c) Inspect key server operating system; check whether there is restriction to concurrent dialog connection quantity possible to happen in a period of time; whether the same user account concurrently logging in at the same time is forbidden; whether the maximum or minimum using limit to system resources by a single user (e.g. CPU, memory and disk, etc.);

d) Check whether relevant resources of key server are monitored in online checking or operation monitoring system;

e) Inspect key server operating system; check whether it can test and alarm when service level decrease to pre-set minimum value, and the alarming methods; whether the service priority of subject (e.g. process) can be set based on security strategy, and then configure the system resources based on the priority, insuring that the processing capability of lower-priority subject shall not affect the one of higher-priority subject;

f) Evaluate key server operating system; randomly choose a user to log in server, trying starting multiple-concurrent dialog, and then verity whether the system restricts the multi-concurrent dialog of a single user; try establishing some concurrent dialog connections in a period of time, and then verify whether the system restricts concurrent dialog connection quantities in a certain period of time;

g) Evaluate key server operating system; randomly choose a user and log in server with different terminal connecting methods and network address, and then verify whether key server operating system restricts terminal login with terminal connecting methods and network address scope, etc.;

h) Evaluate key server operating system; try decreasing the service level to pre-set minimum value, and then verity whether the system can correctly test and alarm;

i) Evaluate key server operating system; randomly choose a user to log in server without any movement in certain time, and then verify whether the system can lock the terminal of operation overtime; randomly choose a user with several failures of

logging in server, verify whether the server can lock the terminal of authentication failure, and whether it can unlock or terminate based on specified unlocking or terminating methods after locking.

Result judgment

a) If a) ~i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The key host security evaluation system contains the operation systems of network server, application server and database server and from the aspect of contents, the implementation process of security system is involved with 9 work-units. Please refer to Annex A.3.1.3 for details.

7.1.3.1.4 Application security

1) ID authentication (S4)

Evaluation items

a) Provide the login control module to identify the ID of logging user;

b) 2 or more than 2 combined authentication technologies shall be adopted to the **key operation** of same user, one of them shall be unforgeable: e.g. **using magnetic-card, IC card, dynamic password equipment, mobile message dynamic password, fingerprint recognition etc. to intensify authentication;**

c) Provide the functions of user ID uniqueness inspection and authentication information complexity inspection to ensure there are no repeated user authentications in the application system and the user authentication information cannot be used illegally;

d) Provide the function to handle the failure of login, measures such as end of dialogue, restriction of illegal login times and automatic exit can be adopted;

e) Enable the functions of user authentication, user ID uniqueness inspection, user authentication information complexity inspection and login failure handing and set the relevant parameters according to the security strategy

f) Application software may automatically lock the use of terminal when designated idle time interval expires; (F4)

g) System shall compel clients to modify initial passwords in first login. (F4)

h) New passwords are not allowed to be same as the old on in modification. (F4)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, application system, design/inspection documents, operation rules.

Implementation of evaluation

a) Interview the system manager to ask him/her whether the user authentication measures are taken and what the specific measures are; what measures that system adopts to prevent user authentication information being used illegally (e.g. the mixture of capital or small letters, number and special characters or the setting of command cycle, etc.);

b) Inspect whether the application system has user management module and whether the system has compulsory requirements on the intensity of user account and password

c) Interview the system manager to ask him/her whether the user authentication of application system is unique (e.g. the UID, user name or other information is unique in the system and this authentication can only identify this user);

d) Inspect the design/inspection documents to check whether the system adopts a unique authentication (e.g. user name, UID or other properties);

e) Inspect operation rules and records, and check whether they have operation rules, approval and operation records for managing ID label and authentication;

f) Inspect application system; check whether 2 or more than 2 combined authentication technologies are adopted for ID authentication (e.g. adopting any two combinations of user name/passwords, challenge response, dynamic passwords, physical equipment, bio-authentication technology), one of them shall be unforgeable (e.g. digital certificate or bio-authentication technology); for system with anti-repudiation requirements, check whether it adopts digital certificates for ID authentication;

g) Inspect key server application system; check whether there are identity label (establishing account) and authentication function (e.g. passwords) and whether identify authentication information has the feature that illegal use is not easy, e.g. password complexity (e.g. stipulating a mixture of upper and lower case letters, figures and special characters), or token is used to facilitate memory;

h) Inspect application system and check it has and use login failure processing function (e.g. login failure time exceeding set value, system automatically exiting, etc.);

i) Evaluate application system, and verify its login failure processing, illegal login time restriction, automatic exit for login connection overtime, etc. are effective;

j) Evaluate application system and verify whether it timely removes dynamically-used authentication information of memory space (e.g. login system, re-login system after exiting system, checking the existence of last login authentication information);

k) Evaluate application system and verify whether it has authentication alarming function (e.g. a prompt given to user when locking the user after three login failures);

l) Penetration evaluation shall be taken to system to evaluate whether ID authentication information is difficult for illegal use (e.g. entering system by brutal force attack or other methods, and adopting SQL injection, etc. to bypass ID authentication to WEB system);

m) Evaluate system whether login passwords are sent to clients in password envelope or login passwords are unified initial passwords, whether systems force clients to modify initial passwords in first login;

n) Evaluate whether modified passwords are the same as the old one.

Result judgment

a) Under the implementation, if in d) relevant documents have the description of user uniqueness, then this item is positive;

b) Under the implementation, if in d) lack of corresponding documents, then this item is negative;

c) If c) ~ m) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Security mark (S4)

Evaluation items

a) Offer security marking function to subjects and objects and use the function after start up.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, application system.

Implementation of evaluation

a) Interview system manager and inquiry whether business system offers setting security marking function to subjects and objects;

b) Inspect application system and check whether it offer security marking function and conduct corresponding application based on security marking function.

Result judgment

a) If a) ~ b) in evaluation implementation are positive, this information system satisfies the requirements of evaluation.

3) Access control (S4)

Evaluation items

a) Offer discretionary access control function, control the access of users to file, database table and other objects according to security strategy;

b) Coverage of discretionary access control shall include subject, object directly related to information security and operation between them;

c) Access control strategy shall be configured by authorized subject and forbid access of default accounts;

d) Authorize minimum needed for different accounts to finish their own tasks undertaken and form interactive relationships between them;

e) There shall be relationship table key account and privilege in production system; (F4)

f) There should be sensitive mark setting function to important information resources;

g) Comparing security mark should be conducted to confirm authorizing or denying access to object by subject.

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, application system.

Implementation of evaluation

a) Interview system manager and inquiry whether business system offers access control measure and what are the detailed measures and how about the granularity of access control;

b) Inspect application system and check whether system offers access control mechanism; whether control the access of users to objects (e.g. data in file and database) according to security strategy;

c) Inspect application system and check whether coverage of discretionary access control includes subject and object directly related to information security and their operation; whether the granularity of discretionary access control reaches that subject is user level while object is file and database table level (e.g. database table,

view and memory process, etc.);

d) Inspect application system and check whether it has the function to set the privilege of authorized subjects to conduct system function operation and access to data;

e) Inspect application system and check whether privileges of its privileged users are separated, whether privileges are interactive (e.g. system and security manager are unable to manage audit log while security auditor to manage the start, close and deletion, etc. of auditing function of audit log, etc.);

f) Inspect application system and check whether it has the function of restrict default users and whether the function is configured for use;

g) Inspect application system and check whether its function to confirm authorizing or denying access of subject to object by comparing security label is effective;

h) Evaluate application system; by logging in with user with different privileges, check its privileges are restricted by application system, and verify whether the function of system privilege separation is effective;

i) Evaluate application system; by authorized subject setting the privileges for user to operate system function and access to data, then logging in with the user, verify whether user privilege management function is effective;

j) Evaluate application system; by logging in with default user (default passwords) and operating with it (including legal and illegal operation), verify the restriction by system on default user access privilege is effective;

k) Penetration evaluation shall be taken to application system, evaluating whether the coverage scope of discretionary access control contains subjects and objects directly-related to information security and operation between them (e.g. trying bypassing system access control mechanism, etc.);

l) Penetration evaluation shall be taken to application system; by trying bypassing system access control, check whether there is flaw in system discretionary access control.

Result judgment

a) If b) ~ k) in evaluation implementation are positive, this information system satisfies the requirements of evaluation.

5) Trusted path (S4)

Evaluation items

a) When application system authenticates identity of users, a safe information transmission path shall be established;

b) When users are accessing to sources through application system, application system shall ensure a safe information transmission path established between accessed resources and users.

Evaluation modes

Interview and inspect.

Evaluation object

Security manager, key application system, application system documents, database management system documents, etc.

Implementation of evaluation

a) Inspect whether the trusted path function of application has at least the fourth-class-evaluation report in “Information Security Protection-Security Techniques Requirement for Operating System” and “Information Security Protection-Security Techniques Requirement for Database Management System”;

b) May interview security manager and inquiry under what circumstance that trusted path is started to conduct initial login/authentication; what trusted paths have been offered by system currently;

c) Inspect application system documents and check the trusted path functions offered by system;

d) Inspect application system and check whether trusted paths declared in documents are effective;

e) Interview security manager and inquiry under what circumstance that trusted path is started to conduct initial login/authentication; what trusted paths have been offered by system currently;

f) Inspect database management system documents and check the trusted path functions offered by system;

g) Inspect key database management system and check whether the trusted paths declared by documents are effective.

Result judgment

a) If a) under the implementation of evaluation is positive, then d) and g) are positive;

b) If d) and g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Security audit (G4)

Evaluation items

a) Offer security auditing function with every user covered and important security events of application system audited;

b) Ensure that it is unable to suspend audit process alone, and the function of deletion, modification or coverage of audit records shall not be offered;

c) Audit records shall contain date and time, type, subject label, object label, event result, etc., **and audit records shall be regularly backed up with retention time not less than 1 year**;

d) Offer the function of counting, inquiring, analyzing audit record data and generating audit statement;

e) Offer centralized auditing connection based on unified system security strategy;

f) For application system logging in from the internet client side, date, time, method, position and other information of the users' last successful login shall be offered for users to timely discover possible problem when they log in every time. (F4)

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

Auditor, application system.

Implementation of evaluation

a) May interview security auditor; inquiry whether application system is set with security audit; inquiry the selection requirements and strategies for application system to event auditing; protection measures to audit log;

b) Inspect application system and check whether the current auditing scope covers every user;

c) Inspect application system; check whether audit strategy covers important security-related events in system, such as users' label and authentication, all operation records for discretionary access control, critical user behavior (e.g. changing user identity and deleting system table by using super user order), abnormal use of system resources, use of critical system orders (e.g. deleting objects), etc.;

d) Inspect application system; check whether the record of security-related events contains event date and time, type, subject and object label, object sensitive mark, event result, etc.;

a) If g) under the implementation of evaluation, lack of relevant materials, then this item is negative;

b) If there is absence of relevant proof materials (certificates, test reports, etc.), then h) under the implementation of evaluation is negative;

c) If g) ~ i) under the implementation of evaluation is positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Backup and recovery (A4)

Evaluation items

a) Provide function of local data backup and recovery, adopting true-time and asynchronous backup, or incremental and full backup; **incremental backup shall be conducted once a day**, full backup once a week with backup medium stored off-site and **storage time of data at least 15 years**;

b) Data backup shall be stored in redundancy mode, data full backup shall ensure data redundancy with at least one month of cycle; (F4)

c) Establish remote disaster backup center with communication lines, network equipment and database processing equipment configured, providing true-time seamless switchover for business application;

d) Provide remote true-time backup function to timely back up data to disaster backup center by using communication network;

e) As for intra-city data backup center, straight-line distance to production center shall be at least 30 kilometers to take over of operation of all core businesses; as for remote data back up center, the distance shall at least 100 kilometers; (F4)

f) **In order to meet the requirements for disaster backup, verification test shall be taken against the feasibility of key technology application in technology plan, and the result shall be recorded and stored; (F4)**

g) Adopt redundancy technology to design network topological structure, avoiding the existence of single point of failure;

h) **Remote back up center shall be equipped with operation environment for recovery, and shall be in ready or operation state; “ready state” means that resource needed for backup center (relevant hardware and data, etc.) are totally satisfied while equipment CPU has to run yet; ”operation state” means that CPU is running while all resources needed for backup center is totally satisfied. (F4)**

Evaluation modes

Interview, inspect and evaluate.

Evaluation objects

System manager, network manager, security officer, database manager, operating system, network equipment, database management system, business system, design/inspection documents for business system.

Implementation of evaluation

a) May interview network manager; inquiry whether network in information system provides automatic backup mechanism for local and remote backup function to important information; whether hardware redundancy is provided for important network equipment, communication line and server; whether automatic mechanism is provided to realize the function of automatic business switchover and recovery when there is disaster;

b) May interview system manager; inquiry whether operating system in information system provides automatic backup mechanism for local and remote backup function to important information; whether automatic mechanism is provided to realize the function of automatic business switchover and recovery when there is disaster;

c) May interview database manager; inquiry whether database management system of information system provides automatic backup mechanism for local and remote backup function to important information; whether local and remote hot backup with system-level to important business system; whether automatic mechanism is provided to realize the function of automatic business switchover and recovery when there is disaster;

d) Inspect design/inspection document; check whether they have description on local and remote hot backup with system-level; check whether they have description on the function of automatic business switchover and recovery when there is disaster;

e) Inspect operating system, network equipment, database management system, business system; check whether they are equipped with local and remote hot backup with system-level to important system, and whether the configuration is correct;

f) Inspect whether important network equipment, communication line and sever provide hardware redundancy;

g) Inspect whether important business system is equipped with local system-level hot backup function; whether it is equipped with the function of the function of automatic business switchover and recovery when there is disaster;

h) Inspect important business system; verify whether its function of local system-level hot backup is effective or not; whether the function of automatic business switchover and recovery is effective or not.

Result judgment

a) If there is absence of design/inspection documents, then d) under the evaluation is negative;

b) d) ~h) under the implementation of evaluation is positive, then this information system satisfies the requirements of evaluation items of this unit.

The data security is evaluated from the aspects of network security, host security and application security. From the aspect of content, data security involves 3 work-units. Please refer to Annex A.3.1.5 for details.

7.1.3.2 Security management evaluation

7.1.3.2.1 Security management system

1) Management system (G4)

Evaluation items

a) The general guideline and security policy for information security shall work within the whole organization. The overall objective, range, principle and security framework, etc. of security work shall be described.

The document on information security policy and system shall be established.

b) A comprehensive security management system, covering various management contents in management activity, shall be established;

c) An operating instruction shall be established for daily management and operation executed by technological manager or operator.

d) A comprehensive system for information security management, composed by security strategy, management system and operating instruction, etc., shall be formed.

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security; general guideline, policy document and safety strategy document; list of security management system; operating instruction; review record.

Implementation of evaluation

a) Check whether the system is composed by security policy, security strategy, management system and operating instruction, etc.; whether regular review is conducted for security management system; what is the review period?

b) The general guideline, policy document and safety strategy document of information security work shall be checked. Check whether general objective, range, guideline, principle and responsibility, etc. of institution security work are clear in document. Whether security strategy of information system is clear;

c) The list of security management system shall be checked. Check whether levels of physics, network, host system, data, application and management, etc. are covered;

d) Whether there are operating instructions for key management operations, such as system maintenance manual and user operating instruction, shall be checked;

e) Whether there are review records of security management system shall be checked. Check whether the record date is consistent with review period, and whether review comments of relevant personnel are recorded.

Result judgment

a) If items a) - e) in implementation of evaluation are yes, the information system meets the evaluation items' requirements of this unit.

2) Formulation and issuance

Evaluation items

a) Science-technology department in headquarters of financial institution shall be responsible for formulating security management system applying to the whole institution. The science-technology department of each branch shall be responsible for formulating security management system for area under jurisdiction;

b) The security management system shall have unified format and version control;

c) Relevant personnel shall be organized to verify and examine the formulated security management system;

d) Security management system shall be issued in a formal and effective way;

e) The issue range shall be marked on security management system. The document sent or received shall be registered;

f) The security classification, if any, shall be marked on security management system. The management of security classification shall be conducted.

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security, manager, management document on system formulation and issue requirement, review record, security management system, send-receive registration record.

Implementation of evaluation

a) Whether security management system is uniformly formulated under the overall charge of information security leading group or committee. Who are the decision-makers?

b) The director of security shall be interviewed. The formulation procedure of security management system will be asked. Whether verification and examination are conducted for formulated security management system? What are the verification and examination methods (such as holding review meeting, examination by letter and internal audit, etc.). Whether uniform format standard or requirement are followed to formulate. In terms of how to control and use the management system with security classification, whether corresponding measures are adopted to effectively manage;

c) The management document on system formulation and issue requirement shall be checked. Check whether the document indicates relevant contents, such as formulation and issuance procedure of security management system, format requirement, version No. and mark of security classification;

d) Review record of management system shall be checked. Whether there are review comments of relevant personnel shall be checked;

e) Whether the issuance process of security management system is formal and effective, and whether the security management system is issued to relevant personnel in a certain way;

f) The send-receive registration record of security management system shall be checked. Whether send-receive meets established procedure and requirement of issuance range shall be checked.

Result judgment

a) If items a) - f) in implementation of evaluation are yes, the information system meets the evaluation items' requirements of this unit.

3) Review and revision (G4)

Evaluation items

a) The information security leading group shall be responsible for regularly organizing relevant agency and relevant personnel to review the reasonability and applicability of security management system;

b) The security management system shall be checked and examined regularly or irregularly. The security management system having shortcoming or need to be improved shall be revised;

c) The security management system in need of regular revise shall be clarified. A person or department shall be assigned to take charge of the daily maintenance of system;

d) A review, management and monitoring mechanism on issuing web portals content shall be established; (F4)

e) The scope of review and revision shall be determined according to corresponding security classification of security management system.

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security, manager, list of security management system, review record, list of personnel or department in charge of security management system.

Implementation of evaluation

a) Director of security shall be interviewed. Whether security management system is reviewed regularly. Which department/Who is responsible for;

b) The managers (personnel in charge of review, revise and daily maintenance) shall be interviewed. The condition of regular review, revise and daily maintenance of security management system will be asked. What's the review period? What's the review and revision procedure? What's the maintenance measure?

c) The managers (responsible officers) shall be interviewed. Whether security management system is examined, and whether system in need of improvement is revised, when the system has major safety accident, when new security hole is appeared, and when basic structure of technology and structure of organization, etc. are changed;

d) The managers (personnel in charge of regular review and revision) shall be interviewed. Whether corresponding confidentiality requirement is considered for personnel participating in review and when security management system with security classification is reviewed and revised;

e) The review record of security management system shall be checked. Check whether record date and review period are consistent. If the system has been revised, check whether there is any revised edition of security management system;

f) The revise and review record of system, and list of security management system in need of regular review shall be checked. Whether review period is marked on list;

g) Whether security management system is reviewed regularly. Whether revise is conducted if shortcoming is found or the system needs to be improved. What's the review period? What's the review and revision procedure? What's the maintenance measure?

h) whether there is any examination record of security management system, when the system has major safety accident, when new security hole is appeared, and when basic structure of technology and structure of organization, etc. are changed;

i) whether there is a list of corresponding personnel or department in charge of security management system shall be checked.

Result judgment

a) If items a) - i) in implementation of evaluation are yes, the information system meets the evaluation items' requirements of this unit.

Evaluation objects of security management system mainly include document and log related to 3 control points, namely, management system, formulation and issuance, review and amendment.

Refer to Appendix A.3.2.1 for specific content.

7.1.3.2.2 Security management institution

1) Post setting (G4)

Evaluation items

a) The information security management of financial institution implements unified leadership and level-to-level administration. The headquarters has unified leadership for information security management of branches. Each institution shall be responsible for the information security management within this organization and area under jurisdiction; (F4)

b) An information security leading group, composed by leaders of this institution and responsible-person of business and technology departments, shall be established, to take charge of coordinating information security management of this institution and area under jurisdiction, and make decisions on key information security matters within area under jurisdiction;

c) A post dedicated for information technology risk audit shall be established, to take charge of implementing information technology audit system and process, formulating and executing information technology audit plan, and auditing the whole life cycle of information technology and major events; (F4)

d) A functional department for information security management shall be established. Director of security and responsible-persons for all aspects of security management shall be established.

The responsibility of responsible-persons shall be defined;

e) Posts such as system administrator, network administrator and security administrator shall be established. The responsibility of posts shall be defined;

f) Except for science-technology department, at least one computer security officer shall be assigned for each department, who will be responsible for the information security management of that department, and be responsible for cooperating with science-technology department to carry out information security management; (F4)

g) The responsible-person of financial institution shall be the first person responsible for security protection work of computer information system of this organization. The security protection leading group for computer information system of financial institution, full time department, full time (part time) security manager and other relevant personnel shall assist the first person responsible to organize and implement relevant provision; (F4)

h) The three-separation principle shall be insisted, to realize the separation of foreground and background, separation of development and operation, separation of technology and business. IT personnel shall have specific post and specific responsibility. The IT post cannot be held by business personnel. The IT personnel also cannot hold the post of business. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security; responsible-persons for all aspects of security management; responsible-person of daily management of leading group; system administrator, network administrator and security administrator; document on department and post responsibility; letter of appointment; log.

Implementation of evaluation

a) Director of security shall be interviewed. Ask whether committee or leading group guiding and managing information security work is established, whether the top leader is the person appointed or authorized by leader in charge of organization;

b) The director of security shall be interviewed. Ask whether a full time security management institution (functional department of information security management) is established. What's the setup of departments within institution? Whether the responsibility of each department and division of labor are clear;

c) Whether the assignment of responsibility of each post (important posts such as director of security, responsible-persons for all aspects of security management,

apparatus room administer, system administer, network administer and security officer) is clear shall be checked. The director of security shall be interviewed and asked whether responsible-persons for all aspects of security management are established. Which posts (important posts such as director of security, responsible-persons for all aspects of security management, apparatus room administer, system administer, network administer and security officer) are set up? Whether the assignment of responsibility of each post is clear.

d) Director of security, responsible-persons for all aspects of security management, information security management committee or responsible-person of daily management of leading group, system administrator, network administrator and security officer shall be interviewed and asked for their responsibilities;

e) The document on department and post responsibility shall be checked. Check whether the document clearly indicates responsibility of security management institution; whether the responsibility and division of labor of each department within institution are clear; whether department responsibility covers aspects of physics, network and system, etc. Check whether posts such as director of security, responsible-persons for all aspects of security management, apparatus room administer, system administer, network administer and security officer are clearly set up in document; whether responsibility range of each post is clear; whether skill requirements for post holders are clear; whether personnel are put on records;

f) Whether the top leaders of information security management committee or leading group have the letter of appointment from leader in charge of this organization;

g) The responsibility document of information security management committee shall be checked. Whether the responsibility of committee and the responsibility of top leader are clearly described in document shall be checked.

h) Whether the security management departments and information security management committee or leading group have document or log (such as meeting minutes/summary and decision-making document on information security) of execution condition of daily management shall be checked.

Result judgment

a) If the statement of interviewee for Item d) in implementation of evaluation is consistent with document description, this item shall be Yes;

b) If items a) - h) in implementation of evaluation are yes, the information system meets the evaluation items' requirements of this unit.

2) Personnel allocation

Evaluation items

a) A certain amount of system administrator, network administrator and security administrator, etc. shall be provided;

b) Full time information security administers shall be provided. The system of A and B posts shall be implemented. Posts A and B cannot be held by the same person;

c) More than one person shall be provided for key posts for joint management;

d) IT personnel holding key IT posts shall be rotated regularly or irregularly. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security; document related to personnel allocation requirement; list of administers.

Implementation of evaluation

a) Relevant documents of personnel allocation shall be checked. List of post division and condition of regular rotation (including rotation period and rotation procedure) shall be checked;

b) List of post division shall be checked. Whether security administrator is a full-time staff shall be confirmed;

c) The management condition of multi-holders of key posts (including regular rotation condition, rotation period and rotation procedure, etc.) shall be checked;

d) The director of security shall be interviewed. The personnel allocation condition of security management posts (The inquiry shall be made based on post responsibility document. personnel holding key posts, such as apparatus room administer, system administer, database administer, network administer and security officer, shall be included) shall be asked, including quantity, full time or part time, etc.

e) The director of security shall be interviewed and asked the following questions: which key posts implement regular rotation (such as security officer of central apparatus room) ? what's the regular rotation condition? What's the rotation period? What's the rotation procedure?

f) The director of security shall be interviewed and asked whether he/she has a certain requirement for security officers of key area or part (such as security officer of central apparatus room, security officer of key server and administer of confidential data), and what's the allocation for administer of key work (such as key management personnel), and whether 2 or above people are provided for joint management, mutual restriction and supervision;

g) Document related to personnel allocation requirement shall be checked. Whether which security manager shall be provided is clarified. Whether personnel holding key posts, such as apparatus room administer, system administer, database administer, network administer and security officer, are included. Whether full time security officer shall be provided is clarified. Whether the following matters are clarified shall be checked: which key post (list shall be provided) implement regular rotation? Contents such as rotation period and rotation procedure, which key area or part shall be provided with security officer meeting condition of confidential employee? Which key business shall be provided with 2 or above managers for joint management?

h) The list of managers shall be checked. Whether information of personnel holding key posts, such as apparatus room administer, system administer, database administer, network administer and security officer, is clear. Whether security officer is a full time staff shall be confirmed.

Result judgment

a) If security officer in a) of Implementation of evaluation is a full time officer, this item shall be Yes;

b) If items a) - h) in implementation of evaluation are yes, the information system meets the evaluation items' requirements of this unit.

3) Authorization and approval (G4)

Evaluation items

a) The authorization and approval matters, approval department and approver, etc. shall be clarified according to responsibility of each department and post;

b) An approval procedure shall be established for matters such as system change, important operation, physical access and system access. The approval process shall be executed as per approval procedure. A level-by-level approval system shall be established for important activities;

c) The approval matters shall be examined regularly. Information such as project in need of authorization and approval, approval department and approver, etc. shall be updated timely;

d) Approval process shall be recorded. Approval document shall be saved;

e) The user shall be granted the least privilege needed by completing the task undertaken. A mutual restriction relationship shall be formed between the employees holding key post. Relevant approval process shall be executed for privilege change, and there shall be a complete change record; (F4)

f) List of system user and privilege shall be established. Employee privilege shall be checked regularly. The reason of unauthorized user shall be found out, and timely

adjustment shall be conducted. The privilege of overdue user shall be terminated, and filing shall be conducted. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Director of security; approver of key activity; authorization management document, approval document, approval record, examination record, revocation record

Implementation of evaluation

a) Whether approval is specified for key activities in information system shall be checked. Whether approval project is examined and updated regularly, and what's the examination period shall be asked;

b) The approver of key activities shall be interviewed and asked what's his/her approval range of key activity (access to key resources such as network system, application system, database management system, important server and equipment; formulation and issuance of important management system; allocation and training of personnel; purchase of product; access and management of third party personnel; cooperative project with cooperator, etc.), and what's the approval procedure;

c) The authorization management document shall be checked. check whether the document includes list of approval matters; whether the list clearly indicates approval matter, dual approval matter, approval department, approver and approval procedure, etc. (such as, in the list, which matter shall be approved by information security leading group? which matter shall be approved by security management institution? which key activities need the dual approval of department, etc.). Whether the document states clearly that the project in need of approval shall be examined and updated regularly, and the examination period, etc. Whether an approval procedure is established for matters such as system change, important operation, physical access and system access. Whether approval process is executed as per approval procedure;

d) The document after dual approval shall be checked. Whether it has the signature of dual approvers and the seal of approval departments shall be checked;

e) The record on approval process of key activities shall be checked. Whether recorded approval procedure is consistent with document requirement shall be checked;

f) The examination record shall be checked. Whether the record date is consistent with examination period shall be checked;

g) Whether there is the record on revocation of privilege not applicable shall be checked.

Result judgment

a) If items a) - g) in implementation of evaluation are yes, these Evaluation items meet the requirement.

4) Communication and cooperation (G4)

Evaluation items

a) Strengthen the cooperation and communication among various types of management personnel, among agencies within the organization and among the functional departments of information security, regularly or irregularly have coordinate meetings to treat information security problems through collaboration and form meeting minutes.

b) Strengthen the cooperation and communication with fraternal organizations, public security bureaus and telecommunications companies.

c) Strengthen the cooperation and communication with suppliers, industry experts, professional security companies and security organizations.

d) Establish contact list of external-access organizations, including the name of external-access organization, cooperation content, contactor, contact information and other information.

e) Hire an information security expert as a security consultant to guide the construction of information security, to participate in the security plan and security review and others.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, security manager, conference papers, meeting minutes, external-access organization documentation and security consultant list.

Implementation of evaluation

a) Inspect the conference papers and conference papers about the coordination between information security leadership group and departments of it, security inspection and so on and check whether there are description about the conference content, conference time, participants, conference results and others. Interview the security officer and inquire whether communication and cooperation systems have been established among external-access organizations (public security bureaus, telecommunications companies, fraternal organizations, suppliers, industry experts, professional security companies and security organizations and so on), among other departments of the organization and among management personnel of each internal departments, what the cooperation contents are and what communication and cooperation means are;

b) Interview the security officer and inquire whether coordination conference among departments have been convened to organize personnel from other departments to deal with problems related to information system security together, whether security conference among internal security management agencies have been convened to deploy the implementation of security work, what participants of the conference are, what the conference result is and whether regular conference has been regularly convened by information security leadership group or security management committee;

c) Interview the security officer and inquire whether an information security expert has been hired to be perennial security consultant to guide the construction of information security and to participate in the security plan and security review and so on.

d) Interview the security officer (do spot check among system administrators, security guards and others) and inquire what the main communication means with other organizations, staff of other departments in the organization and managers of each internal department are and what the main communication contents are;

e) Inspect whether the papers of coordination conference between departments or meeting minutes include the description of conference content, conference time, participants, conference results and so on;

f) Inspect the papers of security work conference or meeting minutes and check whether they include the description of conference content, conference time, participants, conference results and so on;

g) Inspect the papers of regular conferences of information security leadership group or security management committee or meeting minutes and check whether they include the description of conference content, conference time, participants, conference results and so on;

h) Inspect the list of external-access organizations and check whether the communication and cooperation system have been established among external-access organizations (public security bureaus, telecommunications companies, fraternal organizations, suppliers, industry experts, professional security companies and security organizations and so on) and whether the contactor, contact information and others have been described.

i) Inspect the record document about hiring an information security expert as a perennial security consultant to guide the construction of information security and to participate in the security plan, security review and so on.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) Audits and Inspections (G4)

Evaluation items

a) Develop security audits and security inspection system, standardize the work of security audit and security inspect and carry out the activity of security audit and security inspection regularly.

b) The security officer shall take charge of regularly carrying out security inspection and the inspection content shall include the situation of system daily operation, system vulnerabilities and data backup and others;

c) The overall security inspection shall be regularly done by internal staff or parent bodies and the inspection content shall include the effectiveness of the current security technology measures, the consistence between the security configuration and security strategy, the implementation situation of security management system and others.

d) Develop a security checklist, implement the security inspection, summarize the security inspection data, form a security inspection report and follow up the implementation of rectification for those need to be rectified by limiting the time, report the summary of each time of security inspection and the implementation of rectification to the science-technology departments of a higher level institution for filing.

e) Develop rules of penalty to violating and refusing to implement the security management measures. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, security guard, security inspection system, security inspection reports, audit analysis reports, security inspection process records and security inspection form.

Implementation of evaluation

a) Interview the security officer and inquire whether personnel are organized to do security inspection to the information system, how long the inspection cycle is and whether the abnormal behavior of audit records has been regularly analyzed and audited.

b) Interview the security officer and inquire what the contents of security inspection are, what the inspection personnel are, whether the inspection procedure is done according to relevant strategies and requirements of the system, whether security inspection form has been developed to implement the security inspection, what the inspection result is, whether the inspection result has been reported, what the report form is and what the range of the report is;

c) Inspect the security inspection system document and check whether the document has specified the inspection content, the inspection procedure, inspection cycle and others, whether the inspection content includes the effectiveness of the current security technology measures, the consistent between the security configuration and security strategy, the implementation situation of security management system and others and whether the content include the situation of user account, the situation of system vulnerabilities, the situation of system audit and others;

d) Inspect the security inspection report and check whether the report date is in line with the inspection cycle and whether the report has description of the inspection content, inspection personnel, inspection data summary table, inspection result and others;

e) Inspect the security inspection process records and check whether the recorded inspection procedure is consistent with document requirements;

f) Check whether the report data is consistent with the inspection cycle, whether the report includes the description of analyzers, abnormal problems, analysis results and others and whether corresponding measures have been put forward to the found problems;

g) Inspect whether there is a security inspection form.

Result judgment

a) If a) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The main evaluation objects of security management agency are documents and working records related to five control points, the post setting, personnel allocation, authorization and approval, communication and cooperation, and audit and inspection. The specific contents are shown in Annex A.3.2.2.

7.1.3.2.3 Staff security management

1) Staff recruitment

Evaluation items

a) Designate or authorize a special department or a special person to take responsible for the staff recruitment;

b) Strictly regulate the staff recruitment process, review the identity, background, professional qualifications and other qualifications of the recruited staff and examine their technical skills;

c) Signe confidentiality agreements with employees;

d) Select personnel in the internal staff for key posts and sign jog security agreements with them;

e) File and manage information security managers, timely report the allocation of security management staff and change situation of them to the science-technology departments of a higher level department for filing and the information management staff of the headquarter of financial institutions shall be filed at the science-technology department of the headquarter; (F4)

f) The staff who have been punished and disposed for violating national laws and regulations and relevant provisions of the financial institutions cannot engage in information security management work. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Responsible-person for personnel, human-resource staff, staff recruitment requirements management documents, staff review documents or records, review documents or records, confidentiality agreements, job security agreement and examine records.

Implementation of evaluation

a) Interview the responsible-person for personnel and inquire what requirements for the qualification of staff in hiring them are and whether the hired security management and technology staff has the capability of complementing the work corresponding to their duties;

b) Interview the human-resource staff and inquire whether the identity, background, professional qualification and qualification of hired staff have been reviewed, whether the technical skills of technical staff have been assessed, whether a confidentiality agreement has been signed with them after the hire and whether the duties of them haven been described.

c) Interview the responsible-person for personnel and inquire whether the staff of key posts are selected from internal staff, whether the jog security agreements have been required to sign, whether the credit of staff at key posts has been reviewed regularly and how long the review cycle;

d) Inspect the staff recruitment requirements management documents and check whether the hired staff are equipped with conditions, such as requirements for education and education background, whether the technical staff are equipped with professional skills and whether the management staff are equipped with security management knowledge;

e) Inspect whether there are documents or records related to the review of identity, background, professional qualification, qualification and others to hired staff in staff recruitment and check whether they have recorded the review contents, review results and so on;

f) Inspect the technical skill assessment document or record and check whether they have recorded the assessment contents, assessment results and so on;

g) Inspect the confidentiality agreements and check whether it includes the scope of confidentiality, duty of confidentiality, responsibility of default, the expiration date, the sign of responsible-person and others;

h) Inspect the jog security agreement and check whether it includes the job security responsibilities, responsibility of default, the expiration date, he sign of responsible-person and others;

i) Inspect the credit review record and check whether it records the review content, review result and so on and check whether the review time is consistent with the review cycle.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Staff leave-post

Evaluation items

a) Develop relevant management codes to strictly regulate the leave-post process of staff and to timely terminate all access authority of staff who left their jobs;

b) Retrieve all kinds of identity documents, keys, badges, etc. as well as hardware and software provided by the agency;

c) Handle strict transfer procedures and the staff at key posts can leave their jogs after undertaking the confidentiality obligations after transfer and ensure that the password of information technology system being in charge of staff who left their jobs must be changed.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, human-resource staff, staff leave-post requirements documents, confidentiality undertaking documents, confidential personnel management practices, and implementation records.

The implementation of evaluation

a) Interview the security officer and inquire whether all access authority of staff who left their jobs have been timely terminated and whether all kinds of identity documents,

keys, badges, etc. as well as hardware and software provided by the agency have been retrieved.

b) Interview the human-resource staff and inquire what the transfer procedures are, whether the transfer of staff at key posts is done according to relevant management methods of confidential-staff and whether that the transferred staff can leave in the period of breaking away from the secret after undertaking relevant confidentiality obligations is required;

c) Inspect the staff leave-post requirements documents and inquire the transfer procedure and post-leave requirements have been specified in them;

d) Inspect whether there are records of returning identity documents, equipment and others;

e) Inspect the confidentiality undertaking documents and check whether there is a signature of the transfer staff in them;

f) Inspect the relevant management methods of confidential-staff and check whether the requirements for confidential-staff, transfer procedure of confidential-staff and other relevant contents have been described,

g) Inspect the implementation records of transferring staff at key posts and check whether the records are consistent with the management methods.

Result judgment

a) If a) ~ g) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Staff assessment (G4)

Evaluation content

a) Regularly assess the security skills and security awareness to staff at each post;

b) Do a overall and strict security review and skill assess to staff at key posts;

c) Establish confidentiality system and regularly or irregularly inspect or assess the implementation of confidentiality system;

d) Record and save the assessment result.

Evaluation mode

Interview and inspect.

Evaluation objects

Security officer, human-resource staff and staff assessment records.

Implementation of evaluation

a) Interview the security officer and inquire whether there is a person who regularly assess the security skills and security knowledge of staff at each post;

b) Interview the human-resource staff and inquire the assessment situation of staff at each post, how long the assessment cycle, what the assessment contents are and inquire the security review situation of staff, whether the reviewed staff include the staff at all posts, what the review contents are (such as operation behavior, social relationship, social activity and so on and whether the review is overall;

c) Interview the human-resource staff and inquire what the punishment measures for staff who violates the security strategy and provisions are;

d) Inspect the assessment records and check whether the recorded assessed staff include the staff at each post, whether the assessment contents include the security knowledge, security measures and others and check whether the record data is consistent with the assessment date.

Result judgment

a) If the interviewed personnel in b) under the implementation of evaluation stated that the review content include social relationship, social activities, operation behavior and other aspects, this item is positive;

b) If the statement of interviewed staff in c) under the implementation of evaluation is consistent with the description in the document, this item is positive;

c) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

4) Security awareness education and training (G4)

Evaluation items

a) Give written provisions to regular security education and training and develop different training plan for different posts;

b) Carry out security awareness education, post skill training and relevant security technical training to all kinds of staff to popularize basic knowledge of information security, to regulate the post operation and to improve safety skills;

c) Carry out at least one time of information security training to information security management staff each year; (F4)

d) Give written provisions to security responsibilities and disciplinary measures and inform the relevant personnel of them and punish those who violates the security strategy and provisions.

e) Record, file and save the situation and result of security education and training.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, security guards, system administrators, network administrators, database administrators, training programs and training records.

The implementation of evaluation

a) Inspect whether security education and training programs have been developed and whether the security education and training has been done to staff at each post according to the plan;

b) Inspect the relevant systems and disciplinary records of security responsibilities and disciplinary measures.

c) Inspect the document of security education and training program and check whether there are training programs for different posts; check whether the program determined the training purpose, training methods, training objects, training contents, training time, training location and so on and whether the training content includes base knowledge of information security, post operation procedure and so on;

d) Inspect whether there are records about security education and training, check whether the records have description of training staff, training content, training results and others and check whether the records are consistent with the training program.

Result judgment

a) If the interviewed personnel in b) under the implementation of evaluation can clearly state the inquired content and the statement of security responsibilities, disciplinary measures and post operation procedures are consistent with water described in the document, this item is positive;

b) If a) ~ d) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

5) External personnel access management (G4)

Evaluation content

a) Agencies designate responsible departments to take responsible for the authorization and approval of external personnel access related to non-secret-involved computer systems and networks and special personnel to accompany and supervise the access after approval and register and file it; (F4)

b) Establish access control mechanisms and authentication mechanism for computer systems and internet resources of financial institutions allowing external staff to access and list the list of off users and their authority and the activities of them shall be monitored; (F4)

c) All organizations and individuals obtaining the access authorization of external personnel shall sign security confidentiality agreements with financial institutions and shall strictly observe relevant provisions and operation procedures of financial institutions and they are not allowed to add, delete, modify and check data and not allowed to copy and leak any information of the financial institution. (F4)

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, security manger, security responsibility contract or confidentiality agreement, third party access management documents, access approval document and registration records.

Implementation of evaluation

a) Interview the security officer and inquire what measures having been taken for the access of the third party (such as the staff providing service to system and maintaining the system software and hardware, business cooperation partners, evaluators, etc.) are and whether that the third shall sign a security responsibility contract or confidentiality agreement with the agency before access is required.

b) Interview the security manger and inquire whether what measures having been taken for the access to important areas (such as visiting the host room, important servers or equipment, confidentiality documents and so on) by the third party are, whether there is written approval of relevant responsible-person, whether the whole process is accompanied or supervised by a special person and whether it has been recorded and filed and managed;

c) Inspect the security responsibility contract or confidentiality agreement and check whether they include the scope of confidentiality, duty of confidentiality, responsibility of default, the expiration date, the sign of responsible-person and others;

d) Inspect the third party access management document and check whether that what staff is included in the third party is clear, check the scope (area, system, equipment, information and other contents) that the third party is allowed to access, the condition whether the third party can access (the important areas requiring written application and approval for visit) and access control of the third party (being accompanied or supervised by a special person in the whole process) and the condition whether the third party can leave and so on;

e) Inspect the approval documents for the access of the third party to important areas and check whether there is a written application for the access of the third party to important areas and whether there are approval signatures of the approver for the access and so on;

f) Inspect the registration record of the access of the third party to important areas and check whether the records have described the entering time, leaving time, visited area, visited equipment or information and the accompanier and other information about the access of the third party to important areas.

Result judgment

a) If a) ~ f) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

The main evaluation object of personnel security management are relevant documents and working records of 5 control points, staff recruitment, staff leave-post, staff assessment, security awareness education and training and external personnel access management and the specified contents are shown in Annex A.3.2.3.

7.1.3.2.4 System construction management

1) System-level (G4)

Evaluation items

a) Be clear about the boundary and security protection class of information system;

b) Describe and determine the method and reason for regarding the information system as some security protection class in writing.

c) Organize relevant agency and related technical experts to demonstrate and validate the rationality and correctness of the classification result of information system.

d) Ensure that relevant agency have approved the classification result of the information system.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, documents about system partitioning, documents about system-level, documents about expert’s demonstration and documentation about system attributes.

Implementation of evaluation

a) Interview security officers and inquire whether the method of dividing the information

system and the method of determining the security protection class of the information system comply with the guidance of the classification guidelines and whether they has been clearly described; whether the method of determining the security protection class of the information system comply with the guidance of the classification guidelines and whether relevant agency and security technical experts have been organized to demonstrate and verify the classification result and whether the classification result has been approved by relevant agency (such as superior competent agency);

b) Inspect the documents about system partitioning and inspect whether the document has been clearly described the method and reason for the system partitioning;

c) Inspect the documents about system-level and inspect whether the document has clearly gave the security protection class of the information system, whether it has clearly described the method and reason for regarding the information system as some security protection class and whether it has gave the SxAyGz value of the security protection measure composition; inspect whether the classification result has the seal of approval from relevant agency;

d) Inspect the documents about expert's demonstration and inspect whether there are experts having comments on the classification results;

e) Inspect the documentation about system attribute and inspect whether the documentation is clear about the mission, services, networks, hardware, software, data, border, personnel and so on about the system.

Result judgment

a) If there is no superior competent agency in the a) under the implementation of evaluation and the security officer has approved it, then this information system satisfies the requirements of evaluation items of this unit.

b) If b) ~ e) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

2) Design of security program (G4)

Evaluation items

a) Appoint and authorize a special agency to do overall planning to the security construction of the information system and to develop short-term and long-term security construction plans;

b) Use the resources of the information system of the supervising authority or the regional construction projects that has affected the resources and configuration of information system of other supervising authorities and the engineering construction scheme shall be audited and approved by the business and technology departments of the supervising authority;

c) Select basic security measures according to the security protection class of the system and complement and adjust the security measures according to the result of risk analysis;

d) Uniformly consider the overall security strategy, the security technology framework, security management strategy, the overall construction planning, security needs analysis and detailed design program of the security protection system according to the classification of the information system and form the supporting document;

e) Organize relevant agency and security technology experts to demonstrate and audit the rationality and correctness of overall security strategy, security technology framework, security management strategy, the overall construction planning, the security needs analysis, detailed design program and other related documents and shall obtain the approval before official implementation;

f) Regularly adjust and amend the overall security strategy, security technology framework, security management strategy, the overall construction planning, security needs analysis, the detailed design program and relevant supporting documents according to the result of the class-evaluation and security evaluation.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, responsible-person for system construction, documents about the overall security strategy, security technology framework, documents about the security management strategy, the overall construction plan, detailed design program, documentation about expert's demonstration and maintenance records.

Implementation of evaluation

a) Interview the security officer and inquire whether the special department of authority has been do overall plan to the security construction of the information system and what the responsible department/ person responsible is;

b) Interview the responsible-person for the system construction and inquire whether there are short-term and long-term security construction plans and whether the basic security safety measures have been selected according to the security level of the system and whether the security measures have been complemented and adjusted according to the results of risk analysis and what the adjustments are;

c) Interview the responsible-person for system construction and inquire whether the overall security system, security technology framework, security management strategy, the overall construction planning and detailed design program haven been uniformly considered according to the classification of the information system;

d) Interview the responsible-person for system construction and inquire whether relevant agency and relevant technical experts have been organized to demonstrate and audit the overall security strategy, security technology framework, security management strategy and relevant supporting documents and whether those have been approved by the management department.

e) Interview the responsible-person for system construction and inquire whether the overall security strategy, security technology framework, security management strategy, the overall construction planning, detailed design program and relevant supporting documents have been regularly adjusted and amended according to the result of security evaluation and security assessment and inquire the time of the maintenance cycle;

f) Inspect the plan of the security construction of the system and inspect whether the documents have clear short-term security construction planning and long-term security construction planning about the system;

g) Inspect the overall security strategy, security technology framework, security management strategy, the overall construction planning, the detailed design program and other supporting documents of the system and inspect whether whose documents have been approved by the institute's management.

h) Inspect the documents about expert's demonstration and inspect whether relevant agency and security technology experts have comments on the overall security strategy, security technology framework, security management strategy, the overall construction planning, the security needs analysis, detailed design program and other related documents;

i) Inspect whether there are maintenance records or revised version of the overall security strategy, security technology framework, security management strategy, the overall construction planning, detailed design program and other related documents and whether the record date is consistent with the maintenance cycle.

Result judgment

a) If a) ~ i) in evaluation implementation are positive, then this information system satisfies the requirements of evaluation items of this unit.

3) Product procurement

Evaluation items

a) Ensure that the purchasing and use of security products comply with relevant national provisions;

b) Ensure the purchasing and use of password products meet the requirements of state password department;

c) Appoint or authorize a special department to be responsible for product purchasing and the purchasing of the equipment shall adhere to the principle of open, fair and imparity and shall adopt the tender, invitation and other forms to complete it.

d) If agencies purchase information security ensuring products about scan and detection, they shall report it to the science-technology department for approval and record; (F4)

e) Do pre-selection tests to products and determine the scope of candidate products and regularly audit and update the list of candidate products;

f) Commission professional evaluation organizations to carry out the special tests to products forming important parts;

j) The information security ensuring products about scan and detection are limited to be used by the information security management person of this agency; (F4)

h) Regularly inspect information of relevant log and report about the each kind of information security ensuring products and summarize and analyze them. If there is a big problem, shall immediately take corrective actions and report it according to specified programs; (F4)

i) Regularly back up and archive log and reports generated by each kind of information security ensuring products for at least six months; (F4)

j) Timely upgrade and maintain information security ensuring products. Information security ensuring products that have exceeded the service life or cannot be used any longer shall be treated according to the fixed asset retirement approval procedure; (F4)

k) Configure information security ensuring products in local.

Evaluation modes

Interview and inspect.

Evaluation objects

Security officer, responsible-person for system construction, product purchasing management system, result record of the product selection evaluation and list of updated candidate products.

Implementation of evaluation

a) Interview the security officer and inquire whether there is a special department being responsible for the product purchasing and what the department is;

b) Interview the responsible-person for the system construction and inquire the purchasing situation about6 the information security ensuring products, whether the scope of the candidate products has been determined by carrying out selection test

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			access control system and other important equipment.		
4	Lightning prevention	a) Buildings with computer room shall be equipped with lighting prevention equipment.	Interview the responsible-person for physical security and inquire what lighting prevention measures having been taken are, whether the building with computer room is equipped with lighting prevention equipment and whether the lighting prevention equipment have passed the acceptance or the technical detection of relevant national departments.		
		b) The computer room shall be equipped with AC power grounding cable.	Interview the responsible-person for physical security and inquire whether the grounding of computer system in the computer room is set with AC power grounding cable and check whether the computer room design/acceptance document is in consistent with the actual situation.		
5	Fire prevention	a) The computer room shall be equipped with gas fire fighting equipment and automatic fire alarm systems with little effect on computer equipment.	Interview the responsible-person for physical security and inquire what fire fighting measures having been taken are; check whether the fire fighting equipment are placed in place and whether the service life of them is qualified.		
		b) The channel settings, decorative materials, equipment and cables and others in the computer room shall meet fire safety requirements and shall pass the fire inspection and acceptance. (F2)	Whether the computer room is set with more than two fire escape channels and whether the un-obstruction can be ensured to the channel from sub-areas of the computer room to each fire escape channel to facilitate the escape of personnel and whether the channel of		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			the room is equipped with t significant fire signs.		
6	Water and moisture prevention	a) Water pipes shall not pass through the roof of the computer room, but they pass through the floor, protection and prevention measures shall be taken.	Interview the responsible-person for physical security and inquire whether the computer room is installed with upper and lower water pipes, whether the water pipe is installed to prevent from passing through the roof if there is installed water pipe and whether protection measures have been taken if the installed water pipe passes through the raised floor.		
		b) Take measures to prevent water from passing through windows and roof of the computer room and from penetrating the wall.	Inspect whether the computer room is equipped with windows open outside and whether necessary rain prevention measures have been taken for windows if there are such windows; whether there are no leakage, infiltration and damp phenomenon to the roof, wall and others and whether there is no obvious threat of leaks and damp in the computer room and its environment.		
		c) Take measures to prevent condensation of water vapor and transfer and penetration of underground water in the computer room.	Inspect whether the computer room is equipped with dehumidifier and whether it can works normally, whether measures have been taken to prevent transfer and penetration of underground water of the computer room and whether the situation is consistent with humidity record of the computer room.		
7	Static electricity prevention	a) Take necessary grounded anti-static measures for key equipment.	Interview the responsible-person for physical security and inquire whether there are static electricity problems or failure events caused by		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			static electricity, what effective anti-static measures having been taken are, whether necessary grounded anti-static measures have been taken for key equipment; inspect the computer room design/acceptance document and check whether the described content is in line with the actual situation.		
8	Temperature and humidity control	a) Set temperature and humidity automatic adjustment facilities to limit the temperature and humidity changes in the computer room within the range permitted by the operation of equipment.	Inspect whether the temperature and humidity automatic adjustment facilities can work normally.		
9	Power supply	a) Set voltage regulators and over-voltage protection devices on the power supply line in the computer room.	Interview the responsible-person for physical security and inquire whether there was been voltage instability phenomenon, whether voltage regulator and over-voltage protection device have been set on the power supply line of computer system; inspect whether the voltage regulator and over-voltage protection device on the power supply line of computer system work normally and check whether the supply voltage is normal.		
		b) Provide short-term backup power supply and the backup power supply measures (such as batteries, generators, etc.) can provide more than one hour of operating time.	Interview the responsible-person for physical security and inquire whether short-term backup power supply equipment (such as UPS) are set, whether the supply time meet the minimum power supply requirements of the system; check whether the short-term		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			backup power supply equipment works normally.		
		c) UPS power supply shall be provided for important area and vital equipment of the computer room separately. (F2)	Inspect whether UPS power supply is provided for important area and vital equipment of the computer room separately.		
10	Electromagnetic protection	a) Power lines and communication cables shall be isolated to prevent mutual interference	Inspect the wiring of the computer room and check whether power lines and communication cables are isolated.		

A.1.1.2 Network security checklist

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
1	Structure security	a) Ensure that business processing capabilities of key internet equipment have redundant space to meet the business needs in peak time.	Interview the internet manager and inquire the processing capacity of border equipment of the information system and main internet equipment meet the current business peak traffic situation, and inquire what means having been used to monitor and control the operation situation of main internet equipment are.		
		b) Ensure that the bandwidth part accessing internet and core internet can meet the business needs in peak time.	Interview the internet manager and inquire whether each part of bandwidth meet the business needs in peak time. If the cannot meet the needs, require to do bandwidth on main internet equipment. If there is internet management system or traffic monitoring system, view whether bandwidth usage statements of the internet and core internet reaches or exceeds the processing capacity record.		
		c) Draw network topology structure figure being consistent with the current operation situation.	Inspect whether the network topology structure figure is consistent with the current operation		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			situation.		
		d) Divide different subnets or network segments according to the working duties of various departments, importance of various departments, the importance of information involved and other factors and assign address section for each subnet and internet section according to the principle of facilitating management and control; the production network Internet and office internet shall be isolated effectively.	1. Inspect the internet design/ acceptance document and check whether different subnets or internet sections are divided according to he working duties of various departments, importance of various departments, the importance of information involved and other factors, 2. Log on to core switch “show vlan brief” to check vlan division, “show int vlan X” to check the situation of a specific vlan in detail.		
2	Access control	a) Deploy access control equipment at the border of internet and start the access control function.	a) Carry out a interview and determine what equipment are border access control equipment.		
		b) Can provide the ability to allow / deny access clearly according to the data stream of session state information and control the granularity to be network section level.	1. View whether the client has done arp binding to important internet section and the host, 2. Log on to the switch “show run” to view whether static arp binding, port and mac binding measures have been taken to important internet section and the host, 3. Whether the firewall and agency service and other means have been taken to prevent arp spoofing.		
		c) Determine to permit or deny that the user do resource access to the controlled system according to the access allowance rule between the user and the system and control the granularity to be single user.	Log on to the internet equipment, “show run” to view whether the access control lists accurate to host.		
		d) Limit the quantity of user who has dial-up access.	Log on to the internet equipment “show run | b vty” to view whether the user quantity of vty has been limited.		
3	Security audit	a) Make log and record to the running status, network traffic, user behavior and others of the	Log on to the internet equipment, 1. to “show snmp” to view whether		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
		internet equipment in the internet system.	snmp has been configured to record the running state of internet equipment; to show logging, 2. to “show ip netflow export” to view whether network traffic logs have been configured; 3. to “show aaa meth accounting” to view whether user behavior record has been configured.		
		b) Audit records shall include the date and time of the event, user, type of event, whether the event is successful and other information related to audit, which shall be saved for at least one month.	Log on to the log server or AAA server and view whether the record includes the date and time of the event, user, type of event, whether the event is successful and other information related to audit and whether the save time is at least one month.		
4	Border integrity check	a) Be able to check the behavior connecting with external network privately without permission in the internal internet done by the internal user.	Log on to the illegal external-access service network monitoring and management server in the business network; view whether there is computer with illegal external-access client accessing the internet and whether location and block have been done if there is such as computer.		
5	Intrusion prevention	a) Monitor the following attack behaviors at the internet border: port scan, brute force attacks, trojan backdoor attacks, denial service attacks, buffer overflows, IP fragment attacks and worm attacks and so on.	View whether relevant measures have been taken to internet attacks at the internet border and core business internet section.		
6	Internet equipment protection	a) Do identity authentication to the user logging on to the internet equipment.	Whether AAA authentication or other authentications have been done to internet equipment. If there is authentication, log on to the AAA server and view whether the user matches the identity and		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			limits of authority of the administrator.		
		b) Limit the logging address of the administrator of the internet equipment.	Log on to the internet equipment “show run” to view whether corresponding acl has been used on the internet equipment to limit the log of the administrator; 2. log on to AAA server and view whether the administrator address has been limited.		
		c) The mark of the user of the internet equipment is unique.	Interview the internet equipment manger and inquire the mark of each internet equipment user.		
		d) The identity authentication information shall have the feature that it is not easy to be fraudulent and the there shall be requirements to the complexity of the password and the password shall be changed periodically.	Interview the internet manger and inquire water the strategy of the password of internet equipment is.		
		e) Be equipped with capacity of treating log failure, can take measures, like ending the session, limiting illegal logins and automatically exit.	Use a wrong password to log on to the internet equipment for many times and observe whether the session ends, whether illegal logins are limited and observe whether the login will be exited by the system if the operation does not done for a long time after login.		
		f) When carry out remote management to the internet equipment, it shall take necessary measures to prevent the authentication information from being eavesdropped in the internet transmission process.	Log on to the internet equipment remotely and view whether the 22 port SSH method or other encryption methods have been adopted.		
		g) Back up the configuration document of the internet equipment each month and timely do backup if there is a change.	Interview the internet manger and inquire who the configuration document of the internet equipment is backed up.		
		h) Regularly inspect the running situation of the internet equipment. (F2)	View the inspect record and check whether he running situation of the internet equipment has been regularly inspected.		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
		i) Sort out the service port coming with the internet equipment system, turn off unnecessary system service ports and establish corresponding examination and approval system for the open of ports. (F2)	Evaluate the internet equipment and check whether unnecessary equipment services have been turned off and check the examination and approval system document.		
		j) Regularly inspect the version information of software of the internet equipment. (F2)	View the checklist and check whether the version information of software of the internet equipment has been regularly inspected.		
		k) Establish clock synchronization mechanism for internet equipment. (F2)	Inspect the setting situation of the clock of the internet equipment.		
		l) Regularly inspect and lock or revoke redundant user accounts in the internet equipment.	1. Log on to the internet equipment, “show run | b user to view whether the set accounts correspond to the administrators one by one, 2. if there is internet log server or AA server, view whether there are relevant operation records at the period the administrator corresponds in disguised form.		

A.1.1.3 Host security checklist

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
1	Identity authentication	a) Do identity identification and authentication to users logging on to the operation system and database system.	Interview the system administrator/ database administrator and inquire what measures having been taken to achieve identity identification and authentication are and what identity authentication measures and what handling measures having been provided by the system are.		
		b) The management user identity of operation system and database system shall have the feature that they are not easy to be fraudulent and the static	Inspect the operation system of main servers and management system of main database systems and view whether identity		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
		password of key systems shall consists of more than six bits with letters, numbers, symbols and others and the password shall be changed regularly.	authentication measures have been provided (such as user name, password and so on), whether the identity authentication information have the feature that they are not easy to be fraudulent, for example, the password is long enough, complex enough (for example, the specified character shall consist of upper and lower case letters, numbers and special characters), have enough life cycle and enough replace requirements of new password and old password (such as specifying the replaced character quantity) or it uses token to facilitate the memory of password.		
		c) Start the capacity of processing log failure, can take measures, like ending the session, limiting illegal logins and automatic exit.	Inspect the operation system of main servers and management system of main database systems and view capacity of processing login failure is equipped, whether the limit value is set for illegal logins, whether the authentication session is ended or the account is closed temporarily when the login exceeds the limit value; view whether automatic exit is set for the for the condition where the login exceeds the set limit time; check whether authentication warning information is set.		
		d) Take necessary measures when conduct remote management to servers through internet to prevent the authentication information from being eavesdropped in the internet transmission process.	Inspect the operation system of main servers and view whether identity identification, authentication, and corresponding encryption have been done to servers		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			or terminate equipment connected with the operation system of servers by the system.		
		e) Assign different user names to different users of the operation system and database to ensure the unique of user name.	Evaluate the operation system of main servers and management system of main database, add one new user and the identity of the user is the identity of the original user (such as user name or UID) and check whether it will succeed.		
2	Assess control	Start the access control function and control the resource access of the user according to security strategy.	Inspect the security strategy of the server operation system and database management system and check whether that the main body has specified the control access to the object (such as the access control to the document or system equipment, catalog, acl access control lists and so on) with identity provisions of user and/or user group is clear, whether the covering range includes the main bodies (such as users) and objects (such as document and database list and so on) directly related to the information security and the operation between bodies and objects (such as read, write, or execute).		
		b) Separate the limits of authority of privileged users of operation system and database system.	Inspect the operation system for main servers and database management system and check whether mutual restraint (for example, the system administrator, security officer and others cannot audit logs, the security auditor cannot mange audit logs of important events,		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			descriptions.		
5	Confidentiality of communications	a) The application system shall use password technology to do session initialization verification before the communicating parties establish a connection.	1) Inquire the security officer and check whether the technologies have been taken to do before the communicating connection is established. 2) Inspect the design/acceptance document and check whether there are descriptions of confidentiality of communications and whether there are descriptions that the password technology is used to do session initialization verification if there are descriptions of confidentiality of communications.		
		b) Encrypt sensitive information characters in the communication process.	1) Inquire the security officer and check whether confidentiality measures have been taken to sensitive information characters in the application system in the communication process and what the measure specifically are. 2) Inspect the design/acceptance document and check whether there are descriptions of confidentiality of communications and whether there are descriptions of confidentiality of communications to sensitive information characters in the communication process if there are descriptions of confidentiality of communications.		
6	Software fault-toler	a) Provide the function of validating the effectiveness of	1) Interview the administrator and inquire		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
	ance	data to ensure that format or length of data input through man-machine interface or communication interface meet the requirements set by the system.	whether there are measures ensuring the software fault-tolerance capability and what measures having been taken are. 2) Input different data (such as the data whose format or length meet the requirements set by the system or data whose format or length dose not meet the requirements set by the system at the application terminal, including login ID and authentication data, and other operation data and see the reaction of the system.		
		b) The application system shall be able to continue to provide parts of functions to ensue those necessary measures can be taken when a fault occurs.	Interview the system administrator and check whether that the system can continue to provide service function when a fault occurs is ensured.		
		c) Be able to effectively shield system error messages and do not directly feedback error massages produced by the system to the customer. (F2)	Inspect whether measures shielding system error messages have been taken to prevent that error massages produced by the system will be directly feedback to the customer.		
7	Resource control	a) For application systems with sessions or short connects, when one side of the communication in the application system does not response within a period, the other side shall be able to automatically end the session.	1) Inquire whether the business system have measures controlling resource and what those measures are specifically. 2) Log on to the application system server and check whether the system property has set a connection timeout limit.		
		b) Be able to limit the maximum number of concurrent session connection of the system.	1) Inquire the administrator and view the maximum number of concurrent session connections the system can support and whether there is a limitation to it. 2) Log on to the		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			application system server and check whether the system has set parameters to limit the maximum number of concurrent session connections.		
		c) The application system with sessions shall be able to limit the multiple concurrent session of one single account.	1) Inquire the administrator to know the number of concurrent session that one single account can initiate and whether there are limits to it. 20 Log on to the application system server and check whether the system has limited the multiple concurrent session of one single account. 3) Connect the system with many concurrent sessions exceeding the specified number of it of one single account and test whether it is successful.		

A.1.1.5 Data security checklist

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
1	Integrity of data	a) Be able to detect that the integrity of system management data, authentication information and critical business data are damaged during the transmission process.	1) Inquire the security officer and check whether there are measures ensuring the integrity of system authentication information and critical business data in the transmission process and what those measures are specifically. 2) Inspect the application system and check whether the function is equipped to detect/ verify whether authentication information and critical business data are damaged during the transmission process.		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
2	Confidentiality of data	a) Use encryption or other protective measures to achieve the confidentiality of the data storage of authentication information.	1) Inquire the security officer and check whether encryption or other protective measures have been taken to achieve the confidentiality of the data storage to the authentication information and sensitive users' data. 2) Inspect the application system design/acceptance document and check whether there are descriptions that encryption or other protective measures have been taken to achieve the confidentiality of the data storage to the authentication information and sensitive users' data. 3) Inspect the application system and check whether encryption or other effective protective measures have been taken to achieve the confidentiality of the data storage to the authentication information and critical business data.		
3	Backup and recovery	a) Be able to do backup and recovery to important information.	1) Interview the internet manager and inquire whether the internet equipment in the information system has provided the function of selecting and backing up important information for users; whether hardware redundancy has been provided to important network equipment, communication lines and servers; 2) Interview the system administrator and inquire whether the operation system in the information system has provided the function of selecting and		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			backing up important information for users; 3) Interview the database manager and inquire whether the database management system in the information system has provided the function of selecting and backing up important information for users; 4) Inspect the design/ acceptance document of important application system and check whether there are descriptions that the application system has provided the function of selecting and backing up important information for users.		
		b) Provide hardware redundancy of critical network equipment, communication lines and data processing systems to ensure the availability of the system.	1) Inspect the operation systems, internet equipment, database management systems and critical application systems and check whether the function of selecting and backing up important information is equipped and whether the configuration is correct. 2) Inspect whether hardware redundancy of critical network equipment, communication lines and data processing systems have been provided.		

A.1.2 Management checklist

A.1.2.1 Security management system

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
1	Management system	a) Develop the overall policy and security strategy of information security, describing the overall object, scope, principle and security framework of the structure security work.	Inspect the overall policy and security strategy of information security and check whether the document has clearly described the overall object, scope, principle		

SN	Category	Evaluation requirements	Evaluation methods	Conclusion records	Compliance
			and security framework of the structure security work.		
		b) Establish security management system to important management content in the security management activities.	Inspect each item of security management system and check whether it covers the system construction, renovation, upgrading, operation and maintenance and other aspects.		
		c) Establish operation procedures to daily management and operation implemented by the security officer and the operator.	Inspect whether there are operation procedures to important management and operation, such as system maintenance manual, user operation procedure and so on.		
2	Development and release	a) The science-technology department of the financial institution headquarter is responsible for the development of security management system applicable to the whole range of the institution and science-technology departments of all branches are responsible for the security management system applicable within jurisdiction.	Interview the security officer and inquire what departments and personnel being responsible for the development of security management system are and what the personnel participating in it are.		
		b) Organize relevant personnel to do demonstration and validation to developed security management system.	Interview the security officer and inquire the development procedure of developing security management system, whether demonstration and validation to developed security management system has been done; check the management system review record and check whether there are review opinions of relevant personnel.		
		c) Release the security management system to relevant personnel in some way.	Inspect whether the release process of security management system is official and effective and whether the system has been released		

Bibliography

[1] *Standardization Law of the People's Republic of China* (the 1988 No.11 Chairman Decree of the PRC), Standing Committee of the National People's Congress

[2] GB/T 1.1-2000 Standardization Guide Part 1: The structure and preparation of standard rules

[3] GB/T 10112-1999 Terminology work - Principles and methods

[4] GB/T 16785-1997 Terminology work - Harmonization of concepts and terms

[5] GB/T 20001.1-2001 Rules for drafting standards - Part 1: Terminology

[6] GB/T 22240-2008 Information security technology – Classification guide for classified protection of information system security

[7] GB/T 25070-2010 Information security technology protect the security of information systems level design technical requirements

[8] JR/T 0060 Securities and futures industry - Baseline for classified protection of information system

[9] JR/T 0067 Securities and futures industry - Testing and evaluation requirement for classified protection of information system

_____ END _____

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

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