Information Technology Engineers Skill Standards

Information Systems Security Administrator

Contents

The original document in Japanese was prepared on March 29, 2001 and updated on September 28, 2001

Central Academy of Information Technology

Japan Information Processing Development Corporation

1. Overview

1.1 Background of developing the "Information Technology Engineers Skill Standards"

At present, great hopes are placed on information technology as the sources of industry regeneration and new economic growth. This is because the roles of IT have been expanded from the tools for manufacturing cost reduction and service speedup to those for effective collaboration among enterprises and the creation of new industries. From now on, the rise or fall of an enterprise will be determined by quality of computerization investment. It is therefore an urgent matter to bring up engineers who construct advanced information systems and those who utilize them.

In view of this, the Central Academy of Information Technology has repeated a study on how to bring up, evaluate, and select good engineers who can show their practical ability on actual jobs. As a conclusion, the academy decided to establish the "information technology engineers skill standards" centering on the criteria to determine whether the required jobs can be performed adequately or not.

1.2 Significance and objective of developing the "Information Technology Engineers Skill Standards"

The results of surveys that the Central Academy of Information Technology has conducted on information technology engineers have suggested an important issue to be solved in the industrial world and by educational institutions such as schools. The issue is the establishment of the guidelines that clearly define what the industrial and educational worlds are expecting to get. While these guidelines need to define the level of knowledge, skills and capability to be equipped with by IT personnel (engineers) who do the actual jobs in the industrial world, they need to define the models of IT engineers who can be accepted internationally, and the ways how schools and other educational institutions should conduct education training on the basis of these models. One example of the guidelines is the "Skill Standard for IT Engineers" developed by the Northwest Center for Emerging Technologies (NWCET) as part of the establishment of "Skill Standards" by the US Department of Labor.

The "Information Technology Engineers Skill Standards" have been developed as a tool that solves the issue mentioned above, and apply to all the sections of the information technology engineers examinations as criteria to evaluate the skills of engineers who have been brought up. The application of this skill standard is significant for the industrial world in "recruiting human resources with the guaranteed ability to do actual jobs." For educational institutions such as schools, this is significant for "understanding and confirming the knowledge, ability, and the achievement levels of the engineers required by enterprises." For government agencies, this is significant for "grasping the technical level of the entire industrial world."

1.3 Configuration of the "Information Technology Engineers Skill Standards"

The "Information Technology Engineers Skill Standards" is a tool that provides information about knowledge and skill needed to do jobs such as building, operational control, usage and evaluation of IT system in organizations such as corporations. It also provides indicators to determine the outcome of jobs. "Information Technology Engineers Examinations: Overview of the New System" and "Information Technology Engineers Examinations: Scope of Examinations" describe knowledge, technology (technical knowledge), and ability that information technology engineers need to have, and performance indicators (listed in 1), 2), and 3) below). The established skill standards describe these points more specifically by consulting actual jobs.

1) Roles and jobs
2) Expected technical levels
3) Scopes of examinations: examination in the morning and that in the afternoon
   (The above information can be downloaded to access http://www.jitec.jipdec.or.jp/.)

The "Information Technology Engineers Skill Standards" consists of three kinds of technical information described below. In this standard, individual skill standards are established for each examinees classified according to examination categories.

(1) Key activities

This chapter describes jobs that are keys unique to each examination categories. It describes the "roles and jobs" in 1) above more specifically.

(2) Skill criteria

This chapter describes what knowledge and skill should be used to do the key activities in (1) above, and also describe performance indicators to determine what outcome should be obtained. It describes "expected technical levels" in 2) above more specifically.

(3) Body of knowledge

This chapter systematically describes common knowledge independent of examination categories and knowledge needed to do the key activities in (1) above. This chapter also covers the "scopes of examinations" in 3) above.

1.4 Image of an "Information Systems Security Administrator" and Skill Standards

These skill standards have been prepared by applying the framework of the information technology engineers skill standards, which have been introduced until now, to "Information Systems Security Administrator."

(1) Image of applicable persons

For information systems, Information Systems Security Administrators engage in information systems security requirements definition, implementation, operation, analysis, and review corresponding to the information systems life cycle consisting of requirements definition, planning, construction, and operation. In these basic jobs, they are required to have the ability to plan and implement the measures to maintain information system security and evaluate the results from the physical, human, and technical points of view.

(2) Skill standards

The skill standards below apply to Information Systems Security Administrators.

1) IT common body of knowledge
2) Information Systems Security Administrator
   - Key activities, skill standards, practical body of knowledge, and core body of knowledge

2. Key Activities

Key activities in the information assets and information systems that form a part of the foundation of business activities refer to procedural items of work for the protection of information assets and information systems, which is the basic job area for information systems security administrator. In this skill standard, the above job area is called an "information systems security management process."

As shown in Figure 2-1, jobs in the information systems security management process are broken down into seven basic "activities."

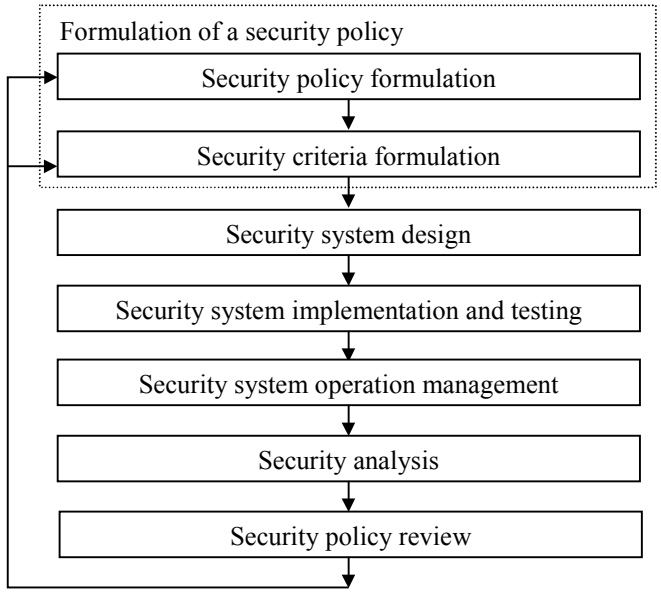

Fig. 2-1 Information systems security management process

Each activity is further broken down into detailed jobs called "tasks." These skill standards present the information system security management process in the following format:

Activity	Task	Job outline
1. Act 1	1-1 Task 1	x x x x x x x x x x x x x x
	1-2 Task 2	x x x x x x x x x x x x
	1-3 Task 3	x x x x x x x x x x
2. Act 2	2-1 Task 1	x x x x x x x x x x x
	2-2 Task 2	x x x x x x x x x x x x x
	2-3 Task 3	x x x x x x x x x x x x x x x
	2-4 Task 4	x x x x x x x x x x x x

Information systems security administrators mainly take charge of the activities of "Security policy formulation," "Security criteria formulation," "Security system design," "Security system implementation and testing," "Security system operation management," "Security analysis," and "Security policy review" as shown in Figure 2-1. In these processes, they fulfill their roles through such jobs as "the formulation of a security policy," "the selection and installation of security products," and "user education."

[Information system security management process]

Activity	Task	Job outline
1. Security policy formulation	1-1 Evaluate information assets	Organize the information assets (such as information systems, data, personnel, and documents) presented by each department of the enterprise, and clarify their values (importance and criticality) from the viewpoint of security through interviews and other means.
	1-2 Recognize threats	Extensively collect, analyze, and organize information on threats to modern society.
	1-3 Identify risks	Identify the risks posed by threats to the enterprise's information assets, and analyze the causes of the risks.
	1-4 Organize and survey measures	Organize physical, human, and technical measures against each of the risks analyzed. Survey the degrees to which those measures are implemented at present.
	1-5 Evaluate risks	For each of the risks analyzed, estimate the probability of its occurrence and evaluate it qualitatively and quantitatively. Rank the risks in terms of priority of countermeasures by considering the damage arising from the actualization of each risk, the costs of reducing the risk, and the risks remaining after countermeasures have been taken.
	1-6 Formulate a security policy	On the basis of the results of risk evaluation, formulate the enterprise's security policy. The main points of the policy will include the objectives, scope, and achievement levels of security measures; the matters to be observed by responsible persons, business managers, and employees; and a system of carrying out information system security activities.
2. Security criteria formulation	2-1 Make security regulations for general business activities	From the viewpoint of security in general business activities, formulate regulations concerning employee activities, regulations for the management of internal documents, regulations concerning security education, and regulations concerning the explanations to be made externally in case of an emergency.
	2-2 Make security regulations for information systems	From the viewpoint of security in the enterprise's information systems, formulate regulations for the management of network server, client, and data operations, regulations for the management of Internet use, regulations for system management operations, regulations for the management of security in the system development process, and regulations concerning the security measures (security architecture) applicable to the objects of development.

Activity	Task	Job outline
3. Security system design	3-1 Control authentication and authority	Determine the user authentication method, the procedures through which the owners of information assets authorize users' access to the assets, the method of examining whether the scope of users' access is appropriate, and the method of users' actually accessing information assets.
	3-2 Control physical security	To guarantee the integrity and availability of information assets as a whole, determine the method of managing buildings, the method of controlling entries and exits, the method of protecting physical network foundation, and the physical equipment to ensure security so that the operations required to maintain security can be performed. (Or give advice to this effect.)
	3-3 Control logical security	To guarantee the integrity and availability of information assets as a whole, determine the appropriateness of an inter-network filtering method and of physical equipment and inter-network segment access policies. If necessary, give advice to those concerned. Also ensure that (or give advice so that) appropriate operations can be performed to maintain security.
	3-4 Ensure reliability of data on network foundation	To guarantee the consistency and availability of the data flowing over the network foundation, determine safety measures to prevent packet tampering and other attacks over the network.
	3-5 Maintain data security	On the basis of the results of risk evaluation, determine such measures as the restriction of access to data on an individual basis, the mechanism of recording access to data, the mechanism of reducing operation errors, and the method of data encryption.
	3-6 Create security operation procedures	Determine procedures for backup, emergency measures, and so forth. Determine the scope of security monitoring and the method of storing information on the results of security monitoring. Obtain the organization's approval of security operations and communicate them to users.
	3-7 Enlighten users and plan education and training	To improve users' security consciousness, conduct appropriate enlightening education with respect to security problems, their ripple effects, and problems caused by a technique of social engineering. Also establish security education and training plans.

Social engineering: Techniques for coaxing information by taking unfair advantage of human psychology or misunderstanding

Activity	Task	Job outline
4. Security system implementation and testing	4-1 Select and install security products	Identify the components of the enterprise's information systems and network, and select and install security products for each component.
	4-2 Develop security systems	If there are no appropriate security products to implement security system design requirements, develop own software as needed.
	4-3 Check security implementation	To find security problems and vulnerable parts with respect to the environmental settings of installed products or developed functions, actually make attacks on the system, server, or network, and check whether security is maintained according to design requirements.
5. Security system operation management	5-1 Implement security operation procedures	Review the operation procedures implementing security system design results, review from the aspect of operation, and feed back any problems found. If no problems are found, implement these operation procedures.
	5-2 Monitor and record system operations	Within the scope of the security monitoring items determined in security system design, monitor and record the status of use of the system and traffic patterns.
	5-3 Maintain systems	Collect the security information provided by a security institution (CERET/CC) and security product vendors, and apply the patches provided by vendors to the system in accordance with urgency and the organization's need.
	5-4 Educate users	Give users basic education and training at regular intervals. For education and training, hire outside consultants and others as appropriate.
	5-5 Educate security engineers	Hiring outside consultants and others as appropriate, give security engineers practical specialized education at regular intervals.

Activity	Task	Job outline
6. Security analysis	6-1 Detect accidents	Detect illegal intrusion and security breaches by analyzing system logs, system error logs, alarm records, and traffic patterns and by checking system consistency.
	6-2 Initial handling of accidents	In accordance with the emergency regulations, communicate and explain an accident, determine the order of priority of the steps to be taken, prevent the spread of damage, and preserve the evidences.
	6-3 Analyze accidents	Survey the conditions and scope of the damage caused by an accident, and assess subsequent damage and effects. Identify the cause of the accident by collecting security information, other information on the accident, operation records, access records, and so forth.
	6-4 Recovery from accidents	Study and implement the measures to prevent recurrences of an accident, and recover the system from the accident. Reconfigure the system as needed.
	6-5 Implement measures to prevent recurrences	Study and implement the permanent measures to prevent the occurrence of similar accidents. Reconfigure the system as needed.
	6-6 Evaluate security	Collect information on the latest threats and accidents; perform inspections regularly by making intrusions, traffic attacks, etc., which simulate typical security accidents; and evaluate the vulnerability of the system and the status of observance of the security policy.

Activity	Task	Job outline
7. Security review	7-1 Collect and evaluate technical information	Collect, analyze, and evaluate the latest security information, security technology information, and cases of security accidents, and consider the need of their application to information systems and their cost effectiveness.
	7-2 Sort out and analyze operation problems	Sort out possible security operation problems (such as opposition from users, unrealistic rules, and a succession of violators); identify the points where they are related with the security policy and security criteria; and review the policy and standards as necessary.
	7-3 Sort out and analyze technical problems	By installing new security technology, identify the points which are related with the security policy and security criteria, and review the policy and criteria as necessary.
	7-4 Sort out and analyze new risks	Sorting out new risks from new threats, identify the points which are related with the security policy and security criteria, and review the policy and criteria as necessary.
	7-5 Update the security policy	When a third party performs an information system security audit, prepare necessary documents and be available for an interview. Review the security policy in response to new risks, matters pointed out, and improvement recommendations. Also, proceed to the reconstruction of security system design, implementation, operation, and management.

3. Skill Criteria

The skill criteria correspond to tools (tables) that provide indicators to check the status of achievement of the information systems security management process described in the key activities. With these criteria, it is determined whether information systems security administrator have promoted a series of jobs successfully according to proper sequence and by using proper techniques, proper knowledge, and proper skill.

The skill criteria provide indicators to indicate what outcome needs to be obtained ("performance indicators") as a result of job execution for each "task" of each of the seven activities. They also provide the knowledge ("required knowledge") and skill ("required skill") required to do the jobs.

[Information Systems Security Administrator Skill Criteria]

1. Security policy formulation				
No.	**Task**	**Performance indicators**	**Required knowledge**	**Required skill**
1-1	Evaluate information assets	• The enterprise's information assets (information systems, data, personnel, and documents) have been identified through interviews with top management, the information strategy executive, the information system security executive, senior managers of operating departments, senior managers of the information system department, and planning people. • The information assets sorted out have been evaluated for their importance and criticality, and organized from the three aspects of security, integrity, and availability. • The information assets sorted out and evaluated have been explained to top management, the information system security executive, and planning people, and their approval has been obtained.	• Knowledge about information collection techniques, procedures, and implementation • Related laws and regulations (such as the Law for Prevention of Unfair Competition, copyrights, and patent rights) • Knowledge about the enterprise's information assets • Knowledge about the enterprise's information systems and network structure • Knowledge about information asset evaluation and measuring techniques • Knowledge about documentation	• Ability to set the targets and scope of a survey • Ability to notice details of the enterprise's information assets • Ability to analyze the in-house flow of information assets • Ability to sort out information assets in a rational way • Ability to make presentations to top management, the information system security executive, and planning people • Ability to negotiate in the enterprise over the evaluated information assets
1-2	Recognize threats	• Survey information is accurate and complete. • Information sources and requests have been grasped using appropriate methodology. • Information about existing threats has been collected comprehensively. • Collected information is classified into such categories as information tampering, information leakage, waste of resources, illegal use of resources, and human errors.	• Knowledge about information collection techniques, procedures, and implementation • Knowledge about incidents and accidents involving information assets • Knowledge about risk evaluation • Knowledge about technologies and operations in general systems and networks • Knowledge about system and network architectures, hardware, and software	• Ability to set the targets and scope of a survey • Ability to notice details of incidents and accidents in information systems in society • Ability to collect information continually • Ability to grasp threats in a rational way

1-3	Identify risks	• Existing risks have been identified for the information assets evaluated. • The plans where risks may occur and their timings have been sorted out. • The causes of risks have been classified into physical, technical, and human causes.	• Knowledge about the types and causes of risks • Knowledge about information assets • Knowledge about the enterprise's system and network structures • Knowledge about system and network architectures, hardware, and software	• Ability to notice details of risks to the enterprise's information assets and their causes • Ability to sort out information assets and risks by associating them in a rational way
1-4	Sort out measures and investigate status	• Measures have been determined to deal with the identified risks. • The extent of implementation of the measures in the present circumstances has been investigated and clarified.	• Knowledge about measures against risks • Knowledge about system and network architectures, hardware, and software • Knowledge about information collection techniques, procedures, and implementation	• Ability to notice details of risks to the enterprise's information assets and their causes • Ability to sort out risks and measures in a rational way • Ability to set the targets and scope of an investigation • Ability to analyze investigation results
1-5	Evaluate risks	• The probability of occurrence of the risks sorted out has been clarified. • The amount of damage at the occurrence of each risk has been calculated. • For each risk, measures to reduce it have been worked out and the costs of the measures have been calculated. • For each risk, the balance between the amount of damage when each risk becomes actual and the costs of measures is considered. • Remaining risks have been evaluated. • Ranks have been assigned to individual risk measures.	• Knowledge about empirical data on the probability of occurrence of risks • Common knowledge about probability and statistics on the occurrence of risks • Knowledge about the calculation of the costs of security measures	• Ability to calculate and evaluate the damage resulting from the loss of information assets (lost value of assets, costs of cause investigation and recovery, and costs of explaining the case to society) • Ability to notice details of incidents and accidents in information systems in society • Ability to collect information continually

1-6	Formulate a security policy	• The enterprise's management policy shows its approach to security measures. • The security policy is documented in such a way as not to depend on individual technologies. • The security policy describes the objectives of security measures, the scope of application, levels of achievement, policy on criteria of measures, matters to be observed by the responsible person for the information system security executive, managers, and employees, implementation organization or system, operation, penalties, disclosure, and reviews. • The security policy has been explained to top management, the information system security executive, and planning people, and their approval has been obtained.	• Knowledge about the management policy • Knowledge about documentation • Knowledge about the method of formulating a security policy	• Flexible ability to go back during the policy formulation to the preceding process which ranges from information asset evaluation to risk evaluation • Ability to describe the security policy in the business level language • Ability to write compositions stressing the continuity of security measures • Ability to make presentations to top management, the information system security executive, and planning people

2. Security criteria formulation

No.	Task	Performance indicators	Required knowledge	Required skill
2-1	Make security regulations for general business activities	• The criteria cover all measures organized in security policy formulation. • The criteria have been explained to top management, the information system security executive, and planning people, and their approval has been obtained. • In line with the measures organized in risk analysis, the following criteria have been drawn up: (1) Employment contract/ job regulations (2) Security/document/information management regulations (3) Regulations for security education (4) Penal provisions (5) Regulations for external explanations (6) Exceptional regulations (7) Regulations for updating rules	• Knowledge about the security policy • Knowledge about standards of security criteria • Knowledge about laws, regulations, ordinances, and legal procedures • Knowledge about employment contracts • Knowledge about job regulations • Knowledge about confidentiality agreements • Knowledge about the protection of privacy • Knowledge about crisis management • Knowledge about the leakage of confidential information • Knowledge about confidential information management procedures • Knowledge about cases of security incidents and accidents • Knowledge about security-related outside education services • Knowledge about press releases • Knowledge about the creation and update of standards • Knowledge about document management and document alteration procedures	• Ability to notice details in drawing up criteria • Ability to make presentations to top management, the information system security executive, and planning people • Ability to negotiate in the enterprise over the criteria drawn up • Ability to continually collect cases of security incidents and accidents • Ability to enforce the criteria flexibly

2-2	Make security regulations for information systems	• The criteria cover all measures organized in security policy formulation. • The criteria have been explained to top management, the information system security executive, and planning people, and their approval has been obtained. • In line with the measures organized in risk analysis, the following criteria have been drawn up: (1) Regulations for the use of the Internet (2) Regulations for the installation and management of a public server for the Internet (3) Regulations for the installation and management of in-house servers and clients (4) Regulations for the installation and management of remote access points (5) Applications installation regulations (6) Data management regulations (7) Regulations for the implementation of antivirus measures (8) Regulations for emergency actions (9) Security audit regulations (10) Information systems administrator regulations (11) System development regulations	• Knowledge about the security policy • Knowledge about standards of security criteria • Knowledge about services, trends, and crimes and accidents over the Internet • Knowledge about Internet connection technology and security tools • Knowledge about network topology • Knowledge about firewalls • Knowledge about the installation and operation of servers • Knowledge about the installation and operation of remote access servers • Knowledge about the software license system concerning applications • Knowledge about the leakage of confidential information • Knowledge about encryption technology • Knowledge about networks, hardware, and software • Knowledge about social engineering • Knowledge about computer viruses • Knowledge about antivirus software • Knowledge about crisis management • Knowledge about press releases • Knowledge about the detection of accidents • Knowledge about security audits • Knowledge about job regulations • Knowledge about system operation and management • Knowledge about system development procedures • Knowledge about outsourcing agreements	• Ability to notice details in drawing up criteria • Ability to make presentations to top management, the information system security executive, and planning people and to persuade them • Ability to negotiate in the enterprise over the criteria drawn up • Ability to continually collect information on services and trends over the Internet • Ability to continually collect cases of security incidents and accidents • Ability to analyze measures from cases of incidents and accidents

3. Security system design

No.	Task	Performance indicators	Required knowledge	Required skill
3-1	Control authentication and privilege	• To realize the security criteria, the system has been designed as follows: (1) Passwords are designed in such a way that character strings that cannot be easily guessed correctly will be selected. (2) The use of biometrics and digital signature technology has been considered. (3) Unnecessarily redundant confirmation is not performed for authentication, and the granting of access right is designed to be easy to use. (4) Privilege is controlled in such a way that even if illegal users break a part of the authentication, they cannot access the other parts. (5) The system is designed in such a way that authorized users' actions are recorded so that illegal access to the system and data can be easily detected.	• Knowledge about password technology • Knowledge about authentication technology • Knowledge about the technical mechanism of biometrics • Knowledge about digital signature technology • Knowledge about operating systems • Knowledge about networks, hardware, software, and databases	• Ability to derive system requirements concerning authentication and privilege from security criteria • Ability to build authentication and privilege granting systems, maintaining consistent relations between them. • Ability to assemble security technologies, including authentication, encryption, and digital signature technologies, into a single system from a unified viewpoint. • Ability to propose systematization by combining biometric, digital signature, and other technologies

3-2	Control physical security	• To realize the security criteria, the system has been designed as follows: (1) Physical media suitable for preventing signal leaks have been selected. (2) The network topology that can minimize damage that may arise from accidental network disconnections. (3) Physical isolation has been made sure of. (4) Decisions have been made on the placement of physical equipment, and on safety devices for human accesses and in-use environment.	• Knowledge about wiretapping from communication cables • Knowledge about network topologies • Knowledge about network hardware and software • Knowledge about security products	• Ability to derive system requirements concerning the security of physical equipment from security criteria • Ability to apply appropriate physical security in accordance with the evaluation of information assets performed in risk analysis • Ability to integrate the system in such a way that important information assets can be physically isolated • Ability to visit affiliated organizations and to discuss with and persuade people there to realize physical security
3-3	Control logical security	• To realize the security criteria, the system has been designed as follows: (1) Network design has been understood, and problems and solutions have been studied from the viewpoint of security. (2) Network requirements, such as access control, have been clarified so that authenticated users can access appropriate information assets.	• Knowledge about network architectures • Knowledge about network topologies • Knowledge about the principles of filtering • Basic knowledge about TCP/IP • Knowledge about routing	• Ability to derive system requirements concerning logical security from security criteria • Ability to apply security technology to system design • Ability to understand network design • Ability to derive network design requirements from security system design requirements

3-4	Ensure reliability of data on network foundation	• To realize the security criteria, the system has been designed as follows: (1) Decisions have been made on the placement of firewalls, the control of traffic flow, and the traffics to be admitted or rejected. (2) With respect to network services, the services and protocols to be supported have been selected, and a security mechanism has been designed. (3) The system has been designed in such a way that important traffic for the operation of network foundation (update of routing information) will be carried out through authentication. (4) The system has a built-in mechanism that enables backup of important data and retransmits data that failed to reach the destination.	• Knowledge about firewalls • Knowledge about network architectures • Knowledge about network services • Knowledge about routing technology • Knowledge about the TCP protocol • Knowledge about network attacks	• Ability to derive system requirements concerning data consistency from security criteria • Ability to apply security technology to system design • Ability to determine appropriate traffic control in accordance with the system importance found in risk analysis • Ability to collect information on the filtering of network services provided by CERT/CC and vendors and to incorporate it into the system
3-5	Data security protection	• To realize the security criteria, the system has been designed as follows: (1) The system has been designed in such a way that the data which the risk analysis found to cause the most damage if abused will be encrypted. (2) The system has been designed in such a way that decryption will be performed only when the data is referred to. (3) The system has been designed in such a way that encryption keys will be adequately managed.	• Knowledge about encryption technology • Knowledge about the operation of cryptosystems • Knowledge about the method of managing encryption keys	• Ability to derive system requirements concerning the maintenance of data confidentiality from security criteria • Ability to apply security technology to system design • Ability to determine the data that needs to be encrypted • Ability to create a encryption key management system

3-6	Create security operation procedures	• To realize the security criteria, appropriate operations and operation procedures have been worked out as shown below, reflecting users' opinions, and have been approved by the organization: (1) Backup and restoring procedures (2) Procedures for storing the software and data backed up (3) Procedures for carrying outside the organization's computers and important data (4) Determination of the scope of data to be collected for security monitoring (5) Procedures for the storage and management of security monitoring data (6) Preparation to protect privacy with respect to the audit data including personal information	• Knowledge about documentation management • Knowledge about storage media • Knowledge about backup tools • Knowledge about the leakage of confidential information • Knowledge about security audits • Knowledge about the protection of privacy • Knowledge about the way of cooperating in the investigation of security incidents	• Ability to derive system requirements concerning backup from security criteria • Ability to draw up complete backup procedures • Ability to determine the scope of data to detect security incidents and accidents • Ability to determine the method of storing backup data and security monitoring data • Ability to draw up procedures, from security criteria, that will apply to the scenes of actually implementing security • Ability to negotiate in the enterprise over the operations and procedures drawn up
3-7	Enlighten users and plan education and training	• To realize the security criteria, the following items have been implemented: (1) Top management's understanding has been obtained for continual security education. (2) Enlightening education has been conducted to enhance security consciousness. (3) Education and training plans have been drawn up to provide continual security education for managers and employees.	• Knowledge about risks to information assets • Knowledge about in-house rules and penalties • Knowledge about new fields of security in general	• Ability to convince top management of the importance of providing continual security education • Ability to formulate education plans with due consideration to users' convenience

4. Security system implementation and testing

No.	Task	Performance indicators	Required knowledge	Required skill
4-1	Select and introduce security products	• Security products suitable for the components of an enterprise network have been selected and installed • Cost effectiveness--the costs of installing products vs. the amount of damage when a risk becomes actual-- is considered. • The operation of necessary functions has been confirmed. • The need of conforming to international standards has been confirmed.	• Knowledge about enterprise network configurations • Knowledge about the functions of security products • Knowledge about ISO15408	• Ability to select security products that can realize a security system • Ability to select security products with appropriate cost effectiveness
4-2	Develop security systems	• It has been fully checked whether there are applicable security products. • Cost effectiveness--the costs of development vs. the amount of damage when a risk becomes actual-- is considered. • The operation of necessary functions has been confirmed.	• Knowledge about the functions of security products • Knowledge about computer system architectures • Knowledge about network system architectures • Knowledge about software development	• Ability to clarify security function requirements • Ability to check whether the developed system meets the security function requirements or not • Ability to understand the OS level processing of computers and network systems
4-3	Check security implementation	• The latest information has been obtained on security holes, security recommendations, and patches. • Intrusion tests have been conducted, by actually performing attacks. • Intrusion tests reflect the latest information on security. • If any security hole is found, measures to deal with it are promptly taken, and permanent measures for the future are studied.	• Knowledge about security holes • Knowledge about security recommendations • Knowledge about tools to verify security functions or to check for security holes • Knowledge about computer system and network system architectures • Knowledge about network attacks	• Ability to continuously collect information on security and security holes • Ability to perform network attacks • Ability to build credibility in the enterprise

5. Security system operation management				
No.	**Task**	**Performance indicators**	**Required knowledge**	**Required skill**
5-1	Implement security operation procedures	• The system has been operated in accordance with the security policy (including the security criteria), performing its functions. • Any problems occurring in the implementation of procedures are recorded.	• Knowledge about security implementation procedures to observe the security policy • Knowledge about exceptions to security implementation procedures	• Ability to have users strictly conform to the implementation procedures without omissions • Ability to discover techniques to circumvent the security implementation procedures and frustrate the techniques
5-2	Monitor and record system operations	• The objects to be monitored and the monitoring method have been clarified. • The traffic determined in security system design has been monitored and recorded. • Recorded data is stored and is available for analysis. • If any security breach is found, it is dealt with in accordance with predetermined procedures.	• Knowledge about security implementation procedures • Knowledge about security monitoring tools	• Ability to find or predict serious attacks from trivial records • Ability to discover security holes and security breaches by using security monitoring tools (including the ability to manage the people who perform inspections using the tools) • Ability to promptly deal with security breaches
5-3	Maintain systems	• The latest information has been obtained on security holes, security recommendations, and patches.	• Knowledge about security holes	• Ability to select the patching information necessary for the network
5-4	Educate users	• The functions prescribed in the education plan have been performed. • User education has been performed continually and at appropriate times.	• Knowledge about security incidents and accidents • Knowledge about risks to information assets • Knowledge about in-house rules and penalties	• Ability to explain security incidents and accidents in an easy-to-understand manner • Ability to persuade users • Ability to make presentations • Ability to communicate with the managers of user departments
5-5	Educate security engineers	• The functions prescribed in the education plan have been performed. • Security engineer education has been performed continually and at appropriate times. • The results of education have been utilized in security operation management.	• Knowledge about outside security services • Knowledge about security incidents and accidents • Knowledge about network attacks	• Ability to have people acquire new technical information • Ability to analyze the causes of security incidents and accidents • Ability to have people apply the techniques they have acquired to security system operation management

6. Security analysis				
No.	**Task**	**Performance indicators**	**Required knowledge**	**Required skill**
6-1	Detect accidents	• Normal system operations have been grasped. • Log files have been checked at regular intervals. • System consistency has been checked at regular intervals. • Automatic tools are used effectively to detect illegal intrusions.	• Knowledge about network attacks. • Knowledge about intrusion detecting techniques. • Knowledge about system access logs. • Knowledge about systems or other automatic tools to detect illegal intrusion • Knowledge about the contents of outside monitoring services	• Ability to monitor continuously • Ability to find or predict serious attacks from trivial records • Ability to warn security violators without sacrificing human relations
6-2	Initially handle accidents	• Procedures for the initial handling of accidents are documented. • Contacts with the persons responsible for information systems and with the related departments have been made as required by procedures. • Actions to be taken are prioritized. • Actions to prevent the spread of damage are taken in accordance with their priority. • Initial handling is documented and reported.	• Knowledge about an in-house communication structure and responsibility structure • Knowledge about the announcement of accidents • Knowledge about the security policy • Knowledge about the results of analysis and the importance of information assets • Knowledge about computer systems and network systems • Knowledge about system operation	• Ability to perform initial handling calmly • Ability to determine the priority of handling on the basis of the importance of information assets • Ability to report facts accurately without mixing them with speculations • Ability to carry out appropriate handling, contacting CERT/IPA and others
6-3	Analyze accidents	• An accident analysis system has been established. • The scope of damage has been identified. • The latest information has been obtained on security holes, security recommendations, and patches. • The causes of accidents have been identified.	• Knowledge about network attacks • Knowledge about computer systems and network systems • Knowledge about security-related incidents and accidents • Knowledge about the analysis of security monitoring data • Knowledge about the procedures for pursuing the causes of accidents	• Ability to carefully investigate and analyze network attacks • Ability to report the causes of accidents, contacting CERT/IPA and others, and to objectively analyze the accidents • Ability to keep a detailed record of accidents

6-4	Recovery from accidents	• Recovery from an accident has been carried out promptly, and the system has been reconfigured as necessary. • A detailed record of recovery has been documented. • Recovery has been communicated to the information system managers and users. • Security has been reviewed after recovery.	• Knowledge about security hole information, security recommendations, and patch information • Knowledge about the enterprise's system configuration • Knowledge about backup procedures and restoring procedures	• Ability to judge the urgency of an accident and determine and take action for early recovery in a short time • Ability to accurately record and report facts
6-5	Implement measures to prevent recurrences	• Measures have been determined and carried out to prevent recurrences, and the system has been reconfigured as necessary. • Security has been reviewed after the determination of measures to prevent recurrences.	• Knowledge about security hole information, security recommendations, and patch information • Knowledge about the enterprise's system construction	• Ability to select and carry out appropriate measures in consideration of the cause of an accident • Ability to accurately record and report facts
6-6	Evaluate security	• The status of observance of the security policy has been evaluated by performing intrusion tests. • Intrusion tests have been performed from time to time. • If intrusion tests find inadequacy, corrective measures are taken promptly. • Security evaluation information has been used in the review of security.	• Knowledge about security hole information, security recommendations, and patch information • Knowledge about security test items • Knowledge about outside testing services • Knowledge about network attacks	• Ability to take prompt action to deal with any security hole found • Ability to continually implement security measures • Ability to build credibility in the enterprise • Ability to use various attacking tools

7. Security review				
No.	**Task**	**Performance indicators**	**Required knowledge**	**Required skill**
7-1	Collect and evaluate technical information	• The latest information has been obtained on security holes, security recommendations, and patches. • Information on the latest security technology has been collected, and its applicability to in-house systems has been evaluated.	• Knowledge about security-related incidents and accidents • Knowledge about security technology • Knowledge about the enterprise's system configuration and network configuration • Knowledge about vendor information	• Ability to collect information on security technology • Ability to select the security hole information and the security technology related to the enterprise's systems and networks
7-2	Sort out and analyze operation problems	• Problems in the implementation of the policy have been collected and sorted out through user questionnaires and interviews. • The standards frequently violated have been identified and sorted out. • The problems sorted out have been analyzed from the viewpoint of amending the security policy, and the policy has been reviewed. • The impact of the implementation of measures to prevent recurrences of accidents on the security policy has been analyzed, and the policy has been reviewed.	• Knowledge about information collection techniques, procedures, and implementation • Knowledge about the enterprise's system and network configurations • Knowledge about the enterprise's system and network operations	• Ability to set the targets and scope of a survey • Ability to analyze problems in the system operation and network operation policies and criteria on the basis of the results of questionnaires sorted out • Ability to review the security policy in response to the analysis of problems • Ability to report to top management on what managerial actions should be taken in response to the analysis of problems
7-3	Sort out and analyze technical problems	• The parts of the security policy to be affected by the development of new technology have been identified and sorted out. • The parts of the security policy to be affected have been identified from the results of evaluation of security analysis and sorted out. • The problems sorted out have been analyzed from the viewpoint of amending the security policy, and the policy has been reviewed.	• Knowledge about security • Knowledge about the enterprise's system configuration and network configuration	• Ability to sort out security information • Ability to analyze problems in the security policy and criteria on the basis of the technical information sorted out • Ability to review the security policy in response to the analysis of problems • Ability to report to top management on what managerial actions should be taken in response to the analysis of problems

7-4	Sort out and analyze new risks	• New risks have been collected and sorted out. • The parts of the security policy to be affected by new risks have been identified and sorted out. • The problems sorted out have been analyzed from the viewpoint of amending the security policy, and the policy has been reviewed.	• Knowledge about security incidents and accidents • Knowledge about security technology • Knowledge about the enterprise's system configuration and network configuration	• Ability to collect and sort out information on security incidents and accidents • Ability to identify the causes of security incidents and accidents from actual cases and analyze the measures to deal with them • Ability to analyze problems in the security policy and criteria on the basis of the technical information sorted out • Ability to review the security policy in response to the analysis of problems
7-5	Update the security policy	• A system to update the security policy has been established. • With respect to amendments to the security policy, risk analysis has been performed again based on the results of analysis and the policy has been updated. • Amendments to the security policy have been approved by top management, the information system security executive, and planning people. • The security policy has been reviewed continually.	• Knowledge about the procedures for amending the security policy • Knowledge about the security policy • Knowledge about the method of drawing up a security policy and security criteria	• Ability to scrutinize the security policy from time to time

4. Body of Knowledge

In the body of knowledge for information systems security administrators, the knowledge which is needed to perform the activities described in "2. Key Activities" successfully and to solve various problems is divided into groups according to technical and problem-solving themes, and is classified in a hierarchical structure. Here, the various problems may include the diversification and complication of needs, increasing cost of operation management, and measures to cope with emerging new technologies.

The body of knowledge which information systems security administrator must have consists of the following two kinds:

1) IT common body of knowledge
2) Information systems security administrators' practical body of knowledge and core body of knowledge

The "IT common body of knowledge" in 1) is not limited to information systems security administrators, but it is necessary for examinees of all examination categories. It is therefore provided in a separate volume. For details, refer to the "Information Technology Engineers Skill Standards: IT Common Body of Knowledge."

By consulting "Information Technology Engineers Examinations: Scope of Examinations," we can know that information systems security administrators are tested for knowledge at the following technical levels in the six fields of the IT common body of knowledge:

"II. Computer system (Level II)"
"III. System development and operation (Level I)"
"IV. Network technology (Level II)"
"VI. Security (Level III)"
"VII. Standardization (Level III)"
"VIII. Computerization and management (Level II)"
"IX. Audit (Level II)"

In 2) practical body of knowledge and core body of knowledge for information systems security administrators, the part corresponding to the practical body of knowledge summarizes the knowledge on "A. Threats to enterprise systems and the social environment," "B. Security policy formulation," "C. Security system design and implementation," and "D. Security operation management and evaluation." The knowledge on A is required for problem solving. Information systems security administrators should show their competence most in fields B, C, and D. The part corresponding to the IT common body of knowledge pursues knowledge more deeply with respect to the body of knowledge organized in the "IT common body of knowledge."

[Information systems security administrator practical body of knowledge and core body of knowledge]

Knowledge field	Major classification	Intermediate classification	Minor classification
A. Threats to enterprise systems and the social environment			
	1 Motives for threats		
		1.1 Types of attackers	
			1.1.1 Beginners (script kiddies) 1.1.2 Amateurs 1.1.3 Professionals 1.1.4 Insiders 1.1.5 Terrorists 1.1.6 Political antagonists
		1.2 Motives for attacks	
			1.2.1 Ignorance and carelessness 1.2.2 Mischief 1.2.3 Exhibitionism 1.2.4 Revenge 1.2.5 Money 1.2.6 Terrorism and war
	2 Types of threats		
		2.1 System vulnerability	
			2.1.1 Vulnerability of protocols (TCP, ICMP, UDP, NNTP, HTTP, SMTP, FTP, NFS/NIS, DNS, TFTP, whois, finger) 2.1.2 Vulnerability of the product systems (WWW browsers, mail systems, buffer overflow, automatic execution by scripts) 2.1.3 Vulnerability of the development systems (vulnerability of development systems and tools) 2.1.4 Vulnerability of system settings (server and firewall settings) 2.1.5 Vulnerability of system operation (management of user IDs and passwords) 2.1.6 Vulnerability to social engineering (leakage of information through phone calls and paper trash) 2.1.7 Vulnerability to physical access (illegal intrusion taking advantage of inadequate guard) 2.1.8 Vulnerability due to development techniques (failure to remove a back door after debugging)

		2.2 Types of attacks	
			2.2.1 Illegal access 2.2.2 Wiretapping 2.2.3 Disguising 2.2.4 Denial of service (stepping stone attack, distributed service denial) 2.2.5 Computer viruses (Trojan Horse, back door) 2.2.6 Attacks using social engineering 2.2.7 Security management tools (automatic collection of information on security holes and vulnerability)
	3 Social environment		
		3.1 Laws and regulations concerned	
			3.1.1 Copyright law 3.1.2 Illegal Access Prevention Law 3.1.3 Act for Protection of Individuals' Information 3.1.4 Unfair Competition Prevention Law
		3.2 International standards and national guidelines	
			3.2.1 ISO15408 3.2.2 ISO17799 (BS7799) 3.2.3 Information Security Policy Guidelines (July 18, 2000) 3.2.4 ISO13333

Knowledge field	Major classification	Intermediate classification	Minor classification
B. Security policy formulation			
	1 Security policy formulation		
		1.1 Evaluate information assets	
			1.1.1 Methods of identifying information assets (information systems, network systems, data, documentation, personnel) 1.1.2 Methods of evaluating information assets (importance in terms of confidentiality, integrity, and availability; criticality and riskiness)
		1.2 Recognize threats	
			1.2.1 Current state of threats (people, things, events, and disasters causing damage to information assets) 1.2.2 Current state of vulnerability (weaknesses in information systems abused by threats)
		1.3 Identify risks	
			1.3.1 Locations of risks (servers, clients, networks, routers, software, development tools, and storage media) 1.3.2 Times of risks becoming actual (working hours, off-hours, national or shop holidays, emergencies, and occasions of making external explanations) 1.3.3 Causes of risks (physical, technical, and human factors)
		1.4 Organize measures	
			1.4.1 Preventive measures 1.4.2 Emergency measures 1.4.3 Measures against disasters 1.4.4 Protective measures 1.4.5 Maintenance measures 1.4.6 Detection and analysis of intrusion
		1.5 Evaluate risks	
			1.5.1 Quantitative risk evaluation methods 1.5.2 Qualitative risk evaluation methods 1.5.3 Costs of risk measures 1.5.4 Allowance for risks
		1.6 Formulate a security policy	
			1.6.1 Policy template 1.6.2 Policy formulation methods 1.6.3 Policy approval procedures

	2 Security criteria formulation		
		2.1 Make security regulations for general business activities	
			2.1.1 Employment contract/ job regulations
			2.1.2 Security, document, and information management regulations
			2.1.3 Regulations for security education (regulations for the continual implementation of security education)
			2.1.4 Penal provisions (regulations for the punishment of security breaches, such as handing offenders over to the police for a penal offense and bringing a civil action against damages)
			2.1.5 Regulations for external explanations (regulations concerning the cases of making external explanations and officials to make explanations)
			2.1.6 Exceptional regulations (regulations for admitting of exceptions)
			2.1.7 Regulations for updating rules (regulations concerning the timing of updating rules and updating procedures)
			2.1.8 Procedures for the approval of regulations

		2.2 Make security regulations for information systems	2.2.1 Regulations for the use of the Internet (regulations for accessing the Internet from inside the enterprise, using mail, etc.) 2.2.2 Regulations for the installation and management of an open server for the Internet (regulations concerning the criteria for installing servers for connection to the Internet and operation management) 2.2.3 Regulations for the installation and management of in-house servers and clients (regulations concerning the criteria for installing in-house servers and clients and operation management) 2.2.4 Regulations for the installation and management of remote access points (regulations concerning the criteria for installing access points for remote access to the enterprise from outside and operation management and use) 2.2.5 Applications installation regulations (regulations for the installation of applications on networked machines and for their use) 2.2.6 Data management regulations (regulations for data access control and data life cycle management) 2.2.7 Regulations for the implementation of antivirus measures (regulations concerning antivirus measures for machines exchanging data with the outside) 2.2.8 Regulations for emergency actions (regulations for emergency actions to deal with accidents) 2.2.9 Security audit regulations (regulations concerning security checks, security monitoring, and security audits) 2.2.10 Information systems administrator regulations (regulations concerning the jobs of information systems administrators) 2.2.11 System development regulations (regulations for checking whether or not security requirements are met in the design and implementation stages) 2.2.12 Procedures for the approval of regulations

Knowledge field	Major classification	Intermediate classification	Minor classification
C. Security system design and implementation			
	1 Security system design		
		1.1 Control authentication and privilege	
			1.1.1 Safe passwords (S/Key passwords, one-time passwords) 1.1.2 Authentication mechanisms (PPP, TACACS+, RADIUS, Kerberos, DCE, FORTEZZA) 1.1.3 Other authentication technologies (biometrics [fingerprint, iris, etc.] and digital signature)
		1.2 Control physical security	
			1.2.1 Physical media (twisted pairs, optical fibers, wireless) 1.2.2 Network topologies (bus type, star type, ring type) 1.2.3 Locations of physical equipment (network equipment, servers, clients, and mobile devices) 1.2.4 Physical access (wiring paths, and boxes to contain servers and network equipment) 1.2.5 Physical equipment operating environment (buildings, computer rooms, telecommunications machine rooms, entry/exit control devices, cargo entries/exits, etc.)
		1.3 Control logical security	
			1.3.1 Sub-networks (network segmentation and concealment of the inside) 1.3.2 Filtering 1.3.3 Routing 1.3.4 Virtual LAN
		1.4 Ensure reliability of data on network foundation	
			1.4.1 Connection with outside networks (firewalls, NAT, proxy servers, IP masquerade) 1.4.2 Server locations (DMZ) 1.4.3 Network services (firewall service) 1.4.4 Protection against attacks (illegal access, spoofing attacks, attacks on open services, such as DOS attacks)

		1.5 Protect data security	
			1.5.1 Cryptosystems (symmetric key cryptosystem, public key cryptosystem, elliptic curve cryptosystem) 1.5.2 Encryption technologies and their application (DES, RSA, SSL, PKI, certification authority, IPSEC) 1.5.3 Digital signature (X. 509) 1.5.4 Encrypted mail (PGP, S/MIME) 1.5.5 Prevention of illegal reproduction (digital watermarking)
		1.6 Create security operation procedures	
			1.6.1 Backup/restoring methods (verification by actual recovery from backup) 1.6.2 Monitoring data (objects of monitoring, scope of monitoring, and storage of data) 1.6.3 Privacy protection methods 1.6.4 Operation procedures (granting of passwords, deletion, recovery, temporary suspension, etc.)
		1.7 Enlighten users and plan education and training	
			1.7.1 Enlightening education 1.7.2 Technical education (technical aspect) 1.7.3 Effects of continuous education
	2 Security system implementation and testing		
		2.1 Select and introduce security products	
			2.1.1 Components of enterprise networks (in-house networks, Internet access, dial access) 2.1.2 Security products 2.1.3 Cost effectiveness
		2.2 Develop security systems	
			2.2.1 Cost effectiveness
		2.3 Confirm security implementation	
			2.3.1 Intrusion testing services 2.3.2 Attacking tools 2.3.3 Security information (CERT/CC, JPCERT/CC, IPA)

Knowledge field	Major classification	Intermediate classification	Minor classification
D. Security operation management and evaluation			
	1 Security system operation management		
		1.1 Implement security operation procedures	
			1.1.1 Implementation record
			1.1.2 Dealing with violators
		1.2 Monitor and record system operations	
			1.2.1 Security monitoring system
			1.2.2 Intrusion monitoring services
		1.3 Maintain systems	
			1.3.1 Security hole information
			1.3.2 Patch information
			1.3.3 Secure server services
		1.4 Educate users	
			1.4.1 Enlightening education
			1.4.2 Basic education
			1.4.3 Advanced security education (response to electronic authentication foundation)
		1.5 Educate security engineers	
			1.5.1 Training
			1.5.2 Outside education services
	2 Security analysis		
		2.1 Detect accidents	
			2.1.1 Log files
			2.1.2 System consistency
			2.1.3 Intrusion detection systems
			2.1.4 Intrusion monitoring services
		2.2 Initial handling of accidents	
			2.2.1 Emergency action manual
			2.2.2 Priority order of actions
			2.2.3 Measures to prevent the spread of damage
			2.2.4 Timing of preserving evidence
		2.3 Analyze accidents	
			2.3.1 Methods of investigating damage (checking network equipment settings and checking transaction logs)
			2.3.2 Methods of investigating the causes of accidents

		2.4 Recovery from accidents	
			2.4.1 Recovery action 2.4.2 System reconfiguration 2.4.3 Accident record
		2.5 Implement measures to prevent recurrences	
			2.5.1 Measures to prevent recurrences 2.5.2 Rebuilding the system
		2.6 Evaluate security	
			2.6.1 Intrusion testing services 2.6.2 Security enhancement measures
	3 Security review		
		3.1 Collect and evaluate technical information	
			3.1.1 Technical information 3.1.2 Evaluation criteria
		3.2 Sort out and analyze operation problems	
			3.2.1 Information from user questionnaires and hearings 3.2.2 Status of security breaches 3.2.3 Problem analysis methods
		3.3 Sort out and analyze technical problems	
			3.3.1 Problem analysis methods
		3.4 Sort out and analyze new risks	
			3.4.1 Security recommendations 3.4.2 Problem analysis methods
		3.5 Update the security policy	
			3.5.1 Update approval procedures 3.5.2 Involvement of top management

Information Technology Engineers Skill Standards
Information Systems Security Administrator **Original version in Japanese published on March 29, 2001**

Publisher Central Academy of Information Technology
Japan Information Processing Development Corporation
19th Floor, Time 24 Building, 2-45 Aomi, Koto-ku, Tokyo 135-8073, Japan
Tel +81 3 5531 0171 (key number)
Fax +81 3 5531 0170
URL http://www.cait.jipdec.or.jp

© March 29, 2001 Japan Information Processing Development Corporation