Registered Information Security Specialist Examination

(Level 4)

Syllabus

— Details of Knowledge and Skills —

Version 1.0

IPA

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Major category	Minor category	Outline	Required knowledge	Required skills
1 Vulnerability and Threat Analyses of an Information System	1-1 Evaluation of information assets	Analyze the development target system, organize information assets (system, data, human resource, document, etc.) to be included in risk identification, and clarify the value of the information assets from the viewpoint of information security (confidentiality, integrity, availability, and effect on system operation) through detailed document reviews and interviews etc..	• Techniques, procedures, and practices for information collection • Related laws (Act on the Prohibition of Unauthorized Computer Access, Act on Regulation of Transmission of Specified Electronic Mail, Act on the Protection of Personal Information, Act on Electronic Signatures and Certification Business, Basic Act on Cybersecurity, etc.), standards, guidelines, etc. • Organizational IT assets • Organizational information systems and network configurations • Evaluation and quantification techniques for IT assets • Documentation	• Defining the aim and scope of the research • Paying attention to the details of organizational IT assets • Understanding the flow of IT assets within the organization • Rationally organizing IT assets
	1-2 Identification of risks (detection of vulnerabilities and threats)	For the development target system, analyze information with regard to risk factors (vulnerabilities, threats, etc.) to information assets, and identify risks that may potentially have a serious impact on the system and risks that cause indefinite losses.	• Techniques, procedures, and practices for information collection • Incidents and accidents involving IT assets • Factors and evaluation of risks • Architectures, technology and operations, hardware, and software of information systems and networks • IT assets • New platform (cloud, virtualization, mobile, embedded systems, web technology)	• Estimating and evaluating an amount of loss of IT assets (including values of lost assets, cost for investigating the cause, cost for restoration, and cost for social explanation) • Defining the aim and scope of the research • Thoroughly listing risks related to organizational IT assets • Rationally organizing the association between IT assets and risks • Collecting information continuously • Rationally identifying vulnerabilities and threats • Rationally identifying risk factors (vulnerabilities and threats) in the new platform
	1-3 Calculation of risks	Calculate the degree of each risk by quantitatively and qualitatively calculating the probability of occurrence of each risk as well as the scale of the influence upon occurrence.	• Empirical data on the probability of risk occurrence • Probabilities and statistics • Calculation of security measure costs	• Estimating and evaluating an amount of loss of IT assets (including values of lost assets, cost for investigating the cause, cost for restoration, and cost for social explanation) • Defining the aim and scope of the research • Collecting information continuously

Major category	Minor category	Outline	Required knowledge	Required skills
	1-4 Evaluation of risks	Create a risk acceptance standard[1)] for determining whether additional countermeasures are required for each of the identified risks. Then, evaluate the calculated degree of risk against the risk acceptance standard, and clarify and prioritize the risks that require additional countermeasures.	• Security measure costs • Risk acceptance standard	• Creating a risk acceptance standard • Prioritizing countermeasures
	1-5 Selection of countermeasures against risks	Risk countermeasures include risk avoidance, risk transfer, risk optimization, and risk retention. Depending on the type of risk, develop and combine appropriate countermeasures in accordance with the organization's information security policy. Also consider control means for abnormal situations such as emergencies and disasters.	• Risk countermeasures • Architectures, hardware, software, and operations of information systems and networks • Techniques, procedures, and practices for information collection	• Thoroughly listing risks related to organizational IT assets • Rationally organizing risks and countermeasures • Analyzing the research results

Major category	Minor category	Outline	Required knowledge	Required skills
2 Defining of Security Requirements	2-1 Collection and analysis of information for defining the security requirements	Clarify the security requirements by analyzing demands based on the organization's information security policy, problems with the current system, and new demands. While doing so, select a scope of research, conduct a research, summarize the research result, summarize the need for security measures, summarize prerequisites and restrictions, summarize the general business flow, and investigate solutions and scope of computerization.	• Business contents and terms • Information collection methods • Business analysis techniques • Modeling techniques • System engineering • Hardware • Software • Networking: • Protocols • Topologies • Routing • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) countermeasures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • Information security economics • Trends of IT (including IoT, big data, AI, etc.)	• Practicing techniques and procedures for information collection • Determining the goal and scope of research • Clarifying demands and restrictions • Modeling and analyzing business operations • Categorizing needs, prerequisites, and restrictions for computerization • Analyzing application systems • Assessing whether an information system can solve a problem • Accurately identifying security problems • Analyzing network architectures • Collecting cases, accidents, and technology trends with respect to security, and analyzing the degrees of influence

Major category	Minor category	Outline	Required knowledge	Required skills
	2-2 Designing of the security architecture	Design an entire structure of the related hardware, software, network, and operations management as a security architecture to implement the security requirements of the development target system.	• Hardware (including virtualization technology) • Software (including cloud technology) • Networking: • Protocols • Topologies • Routing • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) countermeasures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • ISO/IEC 15408 (JIS X 5070) • Reliability design • Documentation of implementation methods and requirements • Security-related standardization	• Proposing a single information system that integrates security technologies for cryptography, authentication, digital signature, and the like from a consistent perspective • Deriving hardware/software-related security requirements from the information security measures criteria • Applying appropriate physical security measures according to the results of an IT asset evaluation conducted during risk analysis • Integrating the information system to allow physical isolation of important IT assets • Deriving network design requirements from the security system design requirements • Selecting security products for implementing security systems • Selecting appropriate security products, with consideration for cost-effectiveness

Major category	Minor category	Outline	Required knowledge	Required skills
	2-3 Defining of the security requirements	Define the security requirements for the development target system according to problems with the development target system and new demands, focusing on countermeasures for high-priority risks identified through analysis of vulnerabilities and threats. For example, if the development target system is a network system, deployment of security measures, such as firewalls and intrusion detection devices, may be required. If the development target system is a business application, security requirements such as a user authentication feature or an access control feature based on privilege definitions may be included.	• Functions and operation of information systems • Development processes and development technologies • Software quality requirements • Quality assurance • Security technologies • Software testing • Development environments for middleware, tools, programming languages, etc. • Cost estimation • Databases • Networks • Operations management • Construction purpose of information systems • Basic functions of information systems • Prototyping of information systems • Techniques for information system tests • Migration of information systems • Operations and maintenance of information systems	• Correlating system requirements with security requirements • Deriving system requirements for authentication and privileges from the information security measures criteria • Logically defining security requirements while maintaining the consistency of relationships between authentication and privileges • Translating user demands into security requirements • Identifying contradictory demands and presenting comprehensive solutions • Applying effective technologies to fulfill requirements • Analyzing the importance of data • Analyzing the correctness and consistency of information • Selecting efficient testing techniques • Designing effective prototypes
	2-4 Preparation of the security requirements definition document	Define the following items with respect to security measures for implementing the determined security requirements and document them for presentation as the security requirements definition documents: • Aim and scope of security measures • Security functions and performances • Demands for business operations, the organization, and users Investigate the creation of requirements for the hardware, software, network, and operations management as necessary.	• System development environments and system operational environments • Matters and notes to be included in the system requirements definition document	• Describing priority matters explicitly

Major category	Minor category	Outline	Required knowledge	Required skills
	2-5 Evaluation and review of the security requirements definition document	Together with the system designers, review the security requirements definition document from the perspective of consistency with users' demands on the development target system, feasibility of system design, testing plans, feasibility of operations and maintenance, and compliance with the organization's information security policy.	• How to proceed with review • System development environments and system operational environments • Matters and notes to be included in the system requirements definition document	• Selecting communication methods appropriate for the system requirements definition review • Appropriately evaluating opposing opinions • Clarifying problems and finding solutions

Major category	Minor category	Outline	Required knowledge	Required skills
3 Design of Security Functions	3-1 Determination and evaluation of the security function method	Investigate implementation methods for security functions of each of hardware, software, network, and operations management as part of the architecture for fulfilling the security requirements. Document the methods into the security implementation method specifications by collaborating with the system designers to review the document from the perspective of consistency with user needs on the development target system, feasibility of system design, testing plans, and feasibility of operations and maintenance. Finally, integrate the specifications into the specifications for the entire system as the design specifications for security implementation method.	• Hardware • Software • Networking: • Protocols • Topologies • Routing • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) countermeasures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • System architecture design concepts and technologies • System architecture design document contents • Operations and maintenance • Review methods (peer review, walk-through review, inspection, etc.) • Performance prediction • Testing techniques	• Documenting the system architecture accurately • Evaluating each computerization plan candidate and explaining them to persons concerned • Identifying core requirements for the system architecture • Selecting technologies with consideration for cost-effectiveness • Allocating system requirements in accordance with a consistent criteria • Interpreting system requirements and associating them with the system architecture • Analyzing and constructing the logical consistency of an information system • Understanding and resolving the core of problems • Documenting software requirements accurately • Clarifying the conditions of use for software • Understanding user demands accurately and reflecting them on the system • Understanding business operations • Understanding requirements for business operations • Simulating operations and maintenance • Analyzing threats and selecting countermeasures • Summarizing the required network configuration • Interpreting system requirements and system design, and associating them with software requirements

Major category	Minor category	Outline	Required knowledge	Required skills
	3-2 Design of security implementation	Design functions required to realize the security requirements definitions for each of the following: hardware, software, network, and operations management. Also prepare a work plan for security implementation, and review it in collaboration with other system designers.	• Software design techniques • Available platforms • Structured designs • Object-oriented design techniques • Information system configurations • Algorithms • Software detailed design • Accurate documentation of program logics • CASE tools and integrated development environment • Programming languages • Review methods (peer review, walk-through review, inspection, etc.)	• Understanding the contents of the system specifications and partitioning the subsystems into components • Designing consistent interfaces between components • Achieving the required quality • Realizing a structure with expandability, versatility, reliability, etc. • Designing software components in accordance with the system specifications • Organizing matters to be discussed and summarizing them into detailed specifications • Selecting the most appropriate design technique • Selecting a development environment most appropriate for the information system
	3-3 Preparation of the security implementation test specifications	Based on the test requirements, prepare component test specifications and unit test specifications for the software, and connection test specifications for the network, etc.	• Designing of unit test specifications • Test tools • Development processes • Operational environments • Programming languages • Implementation environments	• Preparing a unit test plan • Preparing a component test plan • Preparing a system test plan
4 Implementation and Test of Security Functions	4-1 Implementation of security functions	Implement security functions for each of the following: hardware, software, network, and operations management. Secure programming techniques are required for software implementation. For network implementation, investigate deployment of security measures, such as firewalls, intrusion detection systems, authentication VLAN, and quarantine network.	• Code development methodologies • SQL programming • Program quality factors such as readability, efficiency, and ease of maintenance • Selection of programming languages suitable for the development of the target application system • Reuse of existing components • Object-oriented design techniques • Review methods (peer review, walk-through review, inspection, etc.) • Secure programming (programming languages, web application development, software vulnerability countermeasure technologies, etc.) • Network protocols, topology, routing, and network hardware	• Clarifying the programming guideline according to the detailed specifications • Documenting processing details concisely • Creating and comparatively evaluating alternative codes for a complicated and difficult logic • Understanding the organization and hierarchy of information systems • Implementing the required software quality • Realizing a program structure with expandability, versatility, reliability, etc.

Major category	Minor category	Outline	Required knowledge	Required skills
	4-2 Support for system tests	Conduct unit and component tests for the security functions to be developed, and support the system test. Also conduct vulnerability and security penetration testing for the development target system.	• Unit test procedures • Component test procedures • System requirements test procedures • System test procedures • Techniques for confirming that software is implemented as defined in the specifications • Techniques for confirming that an information system is implemented as defined in the specifications • Iterative test processes • Error analysis and resolution processes • Attack techniques and vulnerabilities used to perform security penetration testing • Knowledge for security evaluation testing (white box, black box, penetration test, malware analysis, etc.)	• Identifying, resolving, and correcting malfunctions and failures • Investigating, analyzing, and proposing solutions for situations • Understanding the architecture and hierarchy of information systems • Systematically organizing processes and results, and documenting them as detailed evidence • Devising alternative plans when user requirements are not satisfied due to technical or system defects • Planning and executing all security penetration testing
	4-3 Updating of related documents	Update the user manual and other system documents (external specifications, internal specifications, functional specifications, etc.) for security functions implemented in the past. Also reflect the update results on the organization's information security policy as necessary.	• Writing user manuals • Writing system documents • Document update procedures • Operations of information systems	• Explicitly explaining how and why the user manual was modified • Appropriately reflecting changes to the design or implementation of the information system on the existing system documentation
5 Migrating Security Functions to the Production Environment	5-1 Support for migrating the development target system to the production environment	Support the preparation of the migration plan and the migration of the development target system in accordance with the organization's information security policy.	• Understanding information security policies • Existing systems of the user • Software installation • Concurrent operations with existing systems	• Understanding the information security policy • Planning software migration with minimum influence on existing business operations for users • Supporting users upon start-up
	5-2 Support for development target system's acceptance inspection	Support the acceptance review and acceptance inspection of the development target system by the outsourcer.	• Inspection of results of system tests and system requirements tests • Acceptance review • Acceptance inspection	• Providing acceptance support required by the users

Major category	Minor category	Outline	Required knowledge	Required skills
	5-3 Education, training, and support for operators	For the developed security functions, develop and support the education and training program for the system operators.	• Software operation required by operators • External security diagnostic services • Security incidents and accidents • Network attacks • System log and access log	• Planning education, training, and support in accordance with the operation capability of the operators • Providing education, training, and support to the operators • Analyzing the causes of security incidents and accidents • Analyzing the system log and access log • Applying learned techniques to the operations management of security systems
	5-4 System user support	Define the scope of user support and propose specific support items. Place particular weight on planning and conducting education and training for the users, and on establishing and supporting the help desk. Record the support activity, clarify issues, and implement solutions for them.	• Security incidents and accidents • Risks for IT assets • Company regulations and security policy • Documentation and archiving • Security tools • OS, application systems, and network systems used by the users • Network configurations required by the users • Information collection methods • Technology information, expertise, and reference materials related to user demands	• Institutionalizing and documenting expertise and results accumulated through business practices • Describing maintenance procedures as an overview • Recognizing, analyzing, and providing solution to fulfill needs • Concisely and explicitly describing the contents of education and training • Evaluating user capabilities and setting appropriate education goals • Preparing environments for education and training • Instructing and advising users in accordance with their comprehension and technical level
6 Information Security Review	6-1 Security review of the development target system	For each technology method and protocol adopted by the development target system, verify their safety and reliability from the perspective of information security, confirm their conformance with the organization's information security policy, and provide feedback to the review requesters.	• Hardware • Software • Networking: • Protocols • Topologies • Routing • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware,	• Accurately understanding the details of the system architecture • Evaluating each computerization plan candidate • Identifying core requirements for the system architecture • Selecting technologies with considerations for cost-effectiveness • Interpreting system requirements and associating them with the system architecture • Analyzing and constructing the logical consistency of an information system • Understanding and resolving the essence

Major category	Minor category	Outline	Required knowledge	Required skills
			bot, worm, malicious adware, crack tool, etc.) countermeasures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • Review methods • Feedback	of problems • Collecting information on a new attack technique and evaluating the degree of influence

Major category	Minor category	Outline	Required knowledge	Required skills
7 Security Management Support for Operation of an Information System	7-1 Support for establishment of the security management structure	Support the establishment of the security management structure and management rules for system operations, based on the organization’s information security policy. Also, support the information security manager in establishing and executing technical protective measures against security penetrations. Further, support the preparation of a security education plan for the users.	• Security requirements • Contingency plans and business continuity plans • Potential risks • Security intrusion cases • Security measure technologies and implementation cases • Cost of security measure techniques • Hardware • Software • Networking: • Protocols • Topologies • Routing • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) measures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • Supply chain risk • Information security education • User security management • Security management in system development (offshore development environment)	• Identifying possible security intrusion within the organization • Understanding the organization’s information security policy, as well as security integrated into the information system • Calculating the cost-effectiveness of security measures • Supporting the planning of physical security measures, technical security measures, and management security measures

Major category	Minor category	Outline	Required knowledge	Required skills
	7-2 Support for security intrusion monitoring and situational analyses	Collect and analyze security intrusion monitoring information, and report to the information security manager. Attach security information, such as “new type of computer virus” and “security measure case studies” to the report.	• Types and characteristics of security intrusion • Security intrusion detection technologies • Past security intrusion cases • Implementation of security intrusion countermeasures • Monitoring of information system usage • Vulnerability check tools • Exceptions in operational procedures • Communication and responsibility structures of organizations • Disclosure of accidents • Information security policies • Risk analysis results and importance of IT assets • Information systems and network systems • System operations • Analysis of security monitoring data • Accident cause investigation procedures • Digital forensics	• Distinguishing signs of security intrusion • Discovering or predicting serious attacks from subtle traces • Determining whether a sign of security intrusion will actually result in a security intrusion • Determining the severity of a security intrusion • Determining the influence of a security intrusion on the business • Discovering and preventing abuse of loopholes in operational procedures • Promptly discovering security violations • Analyzing the system log and access log
	7-3 Support for confirmation of the security strength	Support periodical analysis and evaluation of security strength through vulnerability tests and security penetration tests. If any issue is found, plan measures for strength improvement.	• Security attack tools • Vulnerability • Security recommendations • Security function verification or vulnerability check tools • Information system and network system architectures • Network attacks	• Collecting vulnerability information and security information continuously • Practicing network attacks • Confirming the security strength using various attack tools • Promptly taking measures against discovered vulnerabilities

Major category	Minor category	Outline	Required knowledge	Required skills
	7-4 Support for security intrusion countermeasures	Provide technical support to find security intrusion, such as unauthorized intrusion, through analysis of the system log, system error log, alarm records, and traffic patterns, as well as system integrity checks. Investigate the situation and scope of damage due to security intrusion, and evaluate the amount of loss. Collect security information and various information related to intrusions, system log, access log, etc. to support the identification of the cause of the breach. Investigate and propose a permanent prevention measure to prevent reoccurrence of similar security intrusion. Support reconstruction of the system as required.	• Network architectures, topologies, hardware, and software • Monitoring procedures • Intrusion detection tools • Response to security intrusion • Vulnerability and security patches • Malware	• Taking appropriate measures against security intrusion • Utilizing network monitoring tools and intrusion detection tools • Utilizing vaccination tools • Selecting appropriate measures based on the causes of an accident • Determining the urgency and recovery plan for an accident quickly • Taking adequate initial action • Determining the priority of action to be taken depending on the importance of each IT asset • Contacting JPCERT/CC or IPA to take appropriate action • Recording and reporting facts correctly
	7-5 Support for security evaluation	Collect the latest information related to threats, vulnerabilities, and intrusion, and evaluate the system’s vulnerability and conformance to the information security policy.	• Vulnerability information, security recommendations, and security patch information • Security test items • External security diagnostic services • System audits (for security)	• Thoroughly collecting information concerning threats, vulnerabilities, and intrusion • Judging the quality of external services

Major category	Minor category	Outline	Required knowledge	Required skills
8 Management of a Development Project[2)]	8-1 Management of development lifecycles	At each stage of the information system's lifecycle, including planning, requirements definition, development and procurement, and operations and maintenance, take effective security measures to maintain the security of the development project. Measures include the following: identification and categorization of effects due to loss of confidentiality, integrity, and availability during development; investigation of requirements from the viewpoint of information security policy for the development target system; investigation of costs; development of an information security maintenance plan (configuration management, emergency response, education, risk assessment, etc.); development of a detailed management plan; evaluation of information security (evaluation of the effectiveness of the management plan); continuous monitoring; disposal of storage media, disposal of hardware and software; etc.	• Risk factors • Cost calculation for security measures • Risk management • Leakage of confidential information • Business continuity management • Management procedures for confidential information • Hardware • Software • Networks • Operations management • Databases • Security: • Password and account management • Cryptography technology, authentication technology, digital signature technology, and PKI • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) countermeasures • Application security measures • Database security measures • Network security measures • System security measures • Physical security measures • Log management • Access control • Privilege minimization • Attack techniques (spoofing, tapping, falsification, SQL injection, cross site scripting, DoS/DDoS attacks, phishing, social engineering, targeted attack, ransomware, etc.) • Document control • Backup tools • Risk assessment • Education plans • Configuration management • Emergency countermeasures • Disposal of storage media	• Estimating and evaluating an amount of loss of IT assets (including values of lost assets, cost for investigating the cause, cost for restoration, and cost for social explanation) • Determining the storage method for backup data and security monitoring data • Creating procedures for use in the actual operations of the security system based on the information security measures criteria • Rationally organizing risks and countermeasures

Major category	Minor category	Outline	Required knowledge	Required skills
	8-2 Handling of security violations	Monitor and record system usage, system log, access log, alarms, and traffic patterns under the system environment used for the development project, and detect security violations.	• Preparation of emergency response manuals • Failure recovery plans and recovery measures • Collection of vulnerability information • Security intrusion reporting agencies • Digital forensics • Unauthorized access countermeasures • Incident handling • Malware (computer virus, spyware, bot, worm, malicious adware, crack tool, etc.) countermeasures	• Discovering or predicting serious attacks from subtle traces • Appropriately warning security violators • Giving priorities to actions based on the significance of IT assets • Recording the details of an accident • Determining the urgency and recovery plan for an accident in a short time • Promptly taking measures against a discovered vulnerability • Carefully investigating and analyzing network attack situations
	8-3 Application of security patches	Support application of security patches for hardware, firmware, and software (in particular, OS, antivirus software, virus signature files, etc.) used in the development project.	• Vulnerability information disclosing agencies • Security patch application procedures • Backups and restorations • Firmware update techniques • Hardware and software license agreements • Hardware and software vendor support	• Selecting required patch information for hardware, software, and networks • Applying patches (including firmware update in hardware) without causing a fault
	8-4 Control of system documents	Control documents created and used in the project to prevent leakage of confidential development information and customer data (including personal data), etc.	• Review procedures • Digitization of paper files • Access control • Clear desk and clear screen • Document control • Configuration management • Storage media • Backup tools • Leakage of confidential information	• Creating backup procedures • Determining the storage method for backup data • Documenting and informing users of the management rules
	8-5 People management	Take deterrent, prevention, detection, and recovery measures to prevent fraudulent conducts by project members. Clarify and acknowledge the responsibility of each member for information security. Provide appropriate information security education to prevent fraudulent conducts.	• Security education • People management techniques • Employment agreements • Office regulations • Nondisclosure agreements • Privacy policy and personal data protection • External security education services	• Promoting conformity to the rules • Precisely and concisely describing the contents of education and training • Evaluating the educational and training needs and user capabilities, and setting appropriate education goals • Appropriately assigning security responsibilities • Detecting and identifying fraudulent conducts

Major category	Minor category	Outline	Required knowledge	Required skills
9 Support for Information Security Management	9-1 Support for development of the information security policy	Provide technical support for evaluation of information assets, recognition of threats, identification of risks, summarization and investigation of countermeasures, and evaluation of risks, with respect to development or revision of the organization's information security policy.	• Organization's information security policy • Organization's management strategy and business strategy • Organization's information security management system • Business continuity management • Internal control	• Embodying the business strategy and business plan in an information security policy • Analyzing the issues of information security activities from the viewpoint of business continuity
	9-2 Support for development of information security measures criteria	Provide technical support to create information security rules for organization's general activities, in order to support development or revision of the organization's basic information security measures criteria.	• Information security policy • Information security measures criteria • Organizational rule system • Laws, regulations, or guidelines and legal procedures • Employment agreements • Office regulations • Nondisclosure agreements • Privacy policy and personal data protection • Risk management • Leakage of confidential information • Business continuity management • Management procedures for confidential information • Actual security incidents and accidents • Preparation and updating of standards • Document control and document modification procedures	• Appropriately supporting the preparation of standards on measures • Continuously collecting information concerning actual security incidents and accidents • Continuously collecting laws, regulations, guidelines, rules, and standards with respect to information security

Major category	Minor category	Outline	Required knowledge	Required skills
	9-3 Support for review of information security	Provide technical support on information security review through collection and evaluation of technology information, summarization and analysis of operational issues, summarization and analysis of technical issues, and summarization and analysis of new risks, with respect to organization’s information security.	• Security incidents and accidents • Vendor information and security research agency information • Techniques, procedures, and practices for information collection • Information systems, network configurations, and operations of organizations	• Collecting information concerning security technologies • Evaluating and selecting vulnerability information and security technologies related to the information system and network • Creating a questionnaire form for operations on information security, and making a questionnaire survey • Analyzing issues with the information security policy (guidelines and standards) in the operations of the system and network based on the summarized results of the questionnaire survey • Supporting information security policy revisions for addressing the analyzed issues • Supporting preparation of reports on management decisions required for addressing the analyzed issues

Notes [1] A risk acceptance standard is a criteria used as a reference for evaluating the importance of a risk. It includes factors, such as costs involved, legal requirements, socioeconomic and environmental aspects, and priority amongst persons concerned and assessments.

[2] In addition to the tasks listed above, management of a development project also includes security management support tasks for information system operations.

■ Registered Information Security Specialist Examination (Level 4) Syllabus (Version 1.0)

Information-technology Promotion Agency, Japan
IT Human Resources Development Headquarters,
Japan Information-Technology Engineers Examination Center (JITEC)
15th Floor, Bunkyo Green Court Center Office, 2-28-8, Hon-Komagome,
Bunkyo-ku, Tokyo 113-6591 Japan
Tel: 03-5978-7600 (main switchboard)   Fax: 03-5978-7610
Website: http://www.jitec.ipa.go.jp/

2016-10