■ Information Technology Engineers Examination

Information Security Management Examination (Level 2) Syllabus

— Details of Knowledge Required for the Information Technology Engineers Examination —

Version 1.1

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Corporate names or product names used in this syllabus are trademarks or registered trademarks of each company or organization.
® and TM are not used in the syllabus.

■ Introduction

The syllabus (subtitled as “details of the knowledge and skills required for the Information Technology Engineers Examination”) for the Information Security Management Examination, in which “the scope of exam questions”[1)] is described in more detail and the breadth and depth of the knowledge and skills required for Level 2 of the security management area are organized and clarified, has been defined and then published here.

It is expected that this syllabus will be used effectively as learning guidelines for examinees who aim to pass the examination, and also as instructional guidelines in the educational process within companies and schools.

Please note that the detailed information in this syllabus might be added, changed, or deleted, based on technology trends and other factors.

■ Configuration of the Syllabus

As shown in the figure1, this syllabus describes the “Required Knowledge” in the first half, and the "Required Skills” in the latter half.

The chapter on “Required Knowledge” shows the specific contents according to the major, middle and minor categories of the “scope of the morning questions on the Information Security Management Examination.”

The chapter on “Required Skills” shows the specific contents for each item of the “scope of the afternoon questions on the Information Security Management Examination.”

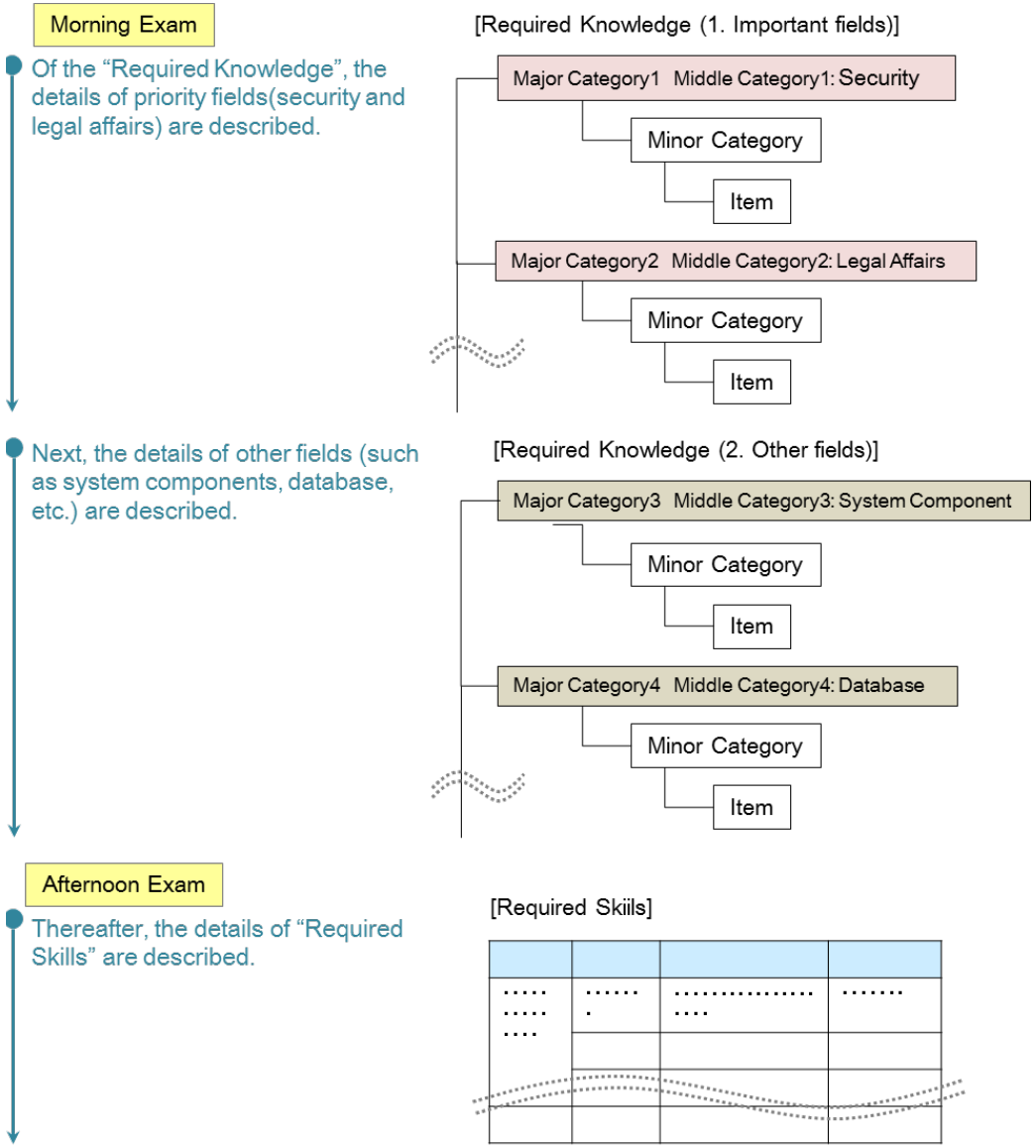

Figure 1 Configuration of the syllabus

Note[1)] "Outline of IT Engineers Examination 7. Scope of the examination (http://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.html , the original in Japanese)"

[Required Knowledge (1. Important Fields)]

Major Category 1: Technology Element　Middle Category 1: Security

Minor category		Item	Sample terms
1	Information security	Purpose and concept of information security	concept of information security, confidentiality, integrity, availability, authenticity, accountability, non-repudiation, reliability, OECD Security Guidelines (Guidelines for the Security of Information Systems and Networks)
		Importance of information security	improvement in corporate reputation based on the height of the level of information security, threat to business continuity due to accidents related to information systems, cyber space, information assets, threats, vulnerabilities
		Threat	**[Types of threats]** physical threats (accident, disaster, fault, destruction, theft, unauthorized intrusion, etc.), technical threats (unauthorized access, eavesdropping, spoofing, alteration, error, cracking, etc.), man-made threats (operational error, loss, damage, peep, unauthorized use, social engineering, etc.), cyber-attack, information leakage, intent, negligence, mistake, fraudulent behavior, sabotage, DoS attack, rumor, flaming, SPAM e-mail, file sharing software **[Malware / malicious programs]** computer virus, macro virus, worm, bot (botnet, remote operated virus), Trojan horse, spyware, ransomware, key logger, rootkit, backdoor, fake anti-virus software
		Vulnerability	bug, security hole, man-made vulnerability
		Fraud mechanism	fraud triangle (opportunity, motivation, rationalization), situational crime prevention
		Types of attackers	script kiddie, bot herder, insider, person who takes delight in people's reaction to his crimes, swindler, person who performs a deliberate crime
		Motive of attack	money capture, hacktivism, cyber-terrorism
		Cyber-attack method	• password cracking (round-robin attack (brute force attack), dictionary attack, etc.), password list-base attack • cross-site scripting, cross-site request forgeries, clickjacking, drive by download, SQL injection, directory traversal • Man-in-the-middle attack, third-party relay, IP spoofing, cache poisoning, session hijack, replay attack • DoS (Denial of Service) attack, DDoS attack, mail bomb • targeted attack (APT (Advanced Persistent Threats), watering hole attack, etc.) • phishing (one-click fraud, SMiShing, etc.), zero-day attack
		Information security technology (cryptography)	CRYPTREC cyphers list, cryptography (encryption key), decryption (decryption key), decoding, symmetric cryptography (common key), public key cryptography (public key, private key)), AES (Advanced Encryption Standard), RSA (Rivest, Shamir, Adleman), S/MIME (Secure MIME), PGP (Pretty Good Privacy), hybrid encryption, hash function (SHA-256, etc.), key management, disk encryption, file encryption, compromise
		Information security technology (authentication technique)	digital signature (signature key, verification key), timestamp (time authentication), message authentication, MAC (Message Authentication Code), challenge-response authentication
		Information security technology (user authentication)	login (user ID and password), access management, IC card, PIN code, one time password, multi-factor authentication, single sign-on, CAPTCHA, password reminder, password management tool

Minor category		Item	Sample terms
		Information security technology (biometric authentication technique)	vein authentication, iris authentication, voice authentication, face authentication, retina authentication, signature authentication, false rejection rate, false acceptance rate
		Information security technology (public key infrastructure)	PKI (Public Key Infrastructure), digital certificate (public key certificate), root certificate, server certificate, client certificate, CRL (Certificate Revocation List)
2	Information security management	Information security management	management of information based on the information security policy, information, information assets, physical assets, software assets, human assets (people, and their qualifications, skills, and experience), intangible assets, service, risk management (JIS Q 31000), monitoring, information security events, information security incidents
		Risk analysis and evaluation (Information asset review / Classification)	information assets review, classification and management by importance of information assets, information assets ledger
		Risk analysis and evaluation (Risk type)	loss of property, loss of responsibility, loss of net earnings, human cost, operational risk, supply chain risk, risk involved in usage of external service, risk involved in distribution of information by SNS, moral hazard, estimated annual loss, scoring method, cost factor
		Risk analysis and evaluation (Information security risk assessment)	risk standards (risk acceptance standard, standard for implementing information security risk assessment), risk level, risk matrix, risk owner, risk source, risk assessment process (risk identification, risk analysis, risk evaluation), risk avoidance, risk appetite, qualitative risk analysis technique, quantitative risk analysis technique
		Risk analysis and evaluation (Information security risk measures)	risk control, risk hedge, risk financing, computerization insurance, risk avoidance, risk sharing (risk transfer, risk distribution), risk retention, risk aggregation, residual risk, risk response plan, risk directory, risk communication
		Information security continuity	emergency category, emergency response plan (contingency plan), recovery plan, disaster recovery, failure recovery, backup measures, investigation method of damage status
		Information security regulations (Company regulations including information security policy)	organizational operation according to the information security policy, information security policy, information security purpose, information security measures criteria, information management regulations, security control regulations, documentation control regulations, regulations on measures to be taken against computer virus infection, regulations on measures against accidents, information security education regulations, privacy policy (personal information protection policy), employment agreement, office regulations, penal provisions, outward explanation regulations, regulations for exceptions, regulations for updating rules, procedure for approving regulations
		Information security management system (ISMS)	ISMS scope, leadership, planning, operation, performance evaluation (internal audit, management review, etc.), improvement (non-conformity and corrective action, continual improvement), purpose of management, management plan (information security incident management, information security education and training, compliance with legal and contractual requirements, etc.), effectiveness, ISMS conformity assessment system, ISMS certification, JIS Q 27001(ISO/IEC 27001), JIS Q 27002 (ISO/IEC 27002), information security governance (ISO/IEC 27014)
		Information security organizations/institutions	information security committee, information security-related organizations (CSIRT, SOC (Security Operation Center)), Cybersecurity Strategic Headquarters, NISC (National center of Incident readiness and Strategy for Cybersecurity), IPA Security Center, JPCERT/CC, unauthorized computer access notification system, computer virus notification system, notification system of vulnerability-related information of software, Information Security Early Warning Partnership, JVN (Japan Vulnerability Notes), suggestions for recurrence prevention, educational activities concerning information security, white hacker

Minor category		Item	Sample terms
3	Security technology evaluation	Security evaluation	PCI DSS, CVSS (Common Vulnerability Scoring System), vulnerability inspection, penetration test
4	Information security measures	Human security measures	Guidelines for the Prevention of Internal Improprieties in Organizations, raising of information security awareness (education, training, material distribution, media utilization), password management, user access management (account management, privileged access right management, need-to-know (least privilege), etc.), log management, monitoring
		Technical security measures	**[Types of technical security measures]** anti-cracking measures, measures against unauthorized access, measures against malware and malicious programs (installation of anti-virus software, update of virus definition file, etc.), outlet measures, inlet measures, defense in depth, privatization, access control, vulnerability management (OS update, application of vulnerability correction program, etc.), network monitoring, assignment of network access rights, intrusion detection, intrusion prevention, DMZ (demilitarized zone), quarantine network, e-mail / web security (measures against spam, SPF, URL filtering, content filtering), security of personal digital assistance (cell phone, smartphone, tablet terminal, etc.), wireless LAN security (WPA (Wi-Fi Protected Access) / encryption of wireless LAN by WPA2, SSID (Service Set IDentifier), SSID stealth, etc.), cloud service security, digital watermarking, digital forensics (preservation of evidence, etc.) **[Security products / services]** anti-virus software, DLP (Data Loss Prevention), SIEM (Security Information and Event Management), firewall, WAF (Web Application Firewall), IDS (Intrusion Detection System), IPS (Intrusion Prevention System), UTM (Unified Threat Management), SSL accelerator, MDM (Mobile Device Management)
		Physical security measures	RASIS (Reliability, Availability, Serviceability, Integrity, Security), RAS technology, quakeproof and fireproof facilities, UPS, dual-redundancy technology, mirroring, monitoring camera, locking control, entrance and exit control, clear desk / clear screen, remote backup, USB key
5	Security implementation technology	Secure protocol	IPsec, TLS, SSL, SSH
		Network security	packet filtering, MAC address (Media Access Control address) filtering, authentication server, VLAN (Virtual LAN), VPN (Virtual Private Network), security monitoring, honey pot, reverse proxy
		Database security	database encryption, database access control, database backup, logging
		Application security	security measures for web systems, secure programming, measures against buffer overflow, measures against cross-site scripting, measures against SQL injection

Major Category 2: Corporate and Legal Affairs　Middle Category 2: Legal Affairs

	Minor category	Item	Sample terms
1	Intellectual property rights	Intellectual property rights	Copyright Act (copyright, infringement of rights, protected object), cancel of copy guard
		Unfair Competition Prevention Act	trade secrets, illicit obtainment of a domain name
2	Laws on security	Basic Act on Cybersecurity	Basic Act on Cybersecurity
		Act on the Prohibition of Unauthorized Computer Access	access control function, unauthorized access, act that helps unauthorized accesses
		Act on the Protection of Personal Information	Guidelines on Personal Information Protection, Guidelines for proper handling of Specific Personal Information, Order for Enforcement of the My Number Act (Order for Enforcement of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedure), JIS Q 15001, privacy mark, OECD Privacy Guidelines (Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data), PIA (Privacy Impact Assessment), privacy framework, opt-in, opt-out, provision to a third party, anonymity method (sampling, k-anonymity)
		Criminal law	crime on electromagnetic records of unauthorized commands (penalty on computer virus creation), crime on computer fraud, crime on obstruction of business by damaging a computer, crime on unauthorized creation and use of electromagnetic records, crime on unauthorized creation of electromagnetic records of payment cards
		Other laws on security	Act on Electric Signatures and Certification Business (accredited certification business operator, electronic certificate), Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders, Act on the Regulation of Transmission of Specified Electronic Mail
		Standards concerning information security	articles in Penal Code concerning computer crime prevention, Standards for Measures Against Computer Viruses, Standards for Measures Against Unauthorized Access to Computers, Standards for Handling Fragility-related Information in Software or the like, Management Standards for Information Security Measures for the Central Government Computer Systems, smartphone safety enhancement strategy, social media guidelines (SNS usage policy)
3	Laws on labor and transaction	Laws on labor (Labor Standards Act)	office regulations
		Laws on labor (Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers)	laborer, dispatch destination, dispatch source, dispatch agreement, employment agreement, providing instructions
		Contracts associated with transactions between businesses	time and material contract, contract for work, software license agreement (volume license agreement, copyleft), software development agreement (model contract for software development outsourcing, information system/model transaction contract)
4	Other laws, guidelines, and engineer ethics	Other laws, guidelines, and engineer ethics	other laws (Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, e-Document Law (electromagnetic records), Law Concerning Preservation of National Tax Records in Electronic Form), compliance, information ethics and engineer ethics
5	Standardization	Standards and standardization organizations	JIS (Japanese Industrial Standards), IS (International Standards), ISO (International Organization for Standardization), role of associated organizations such as IEEE, de jure standard, de facto standard

[Required Knowledge (2. Other Fields)]

Major Category 3: Computer System　Middle Category 3: System Component

Minor category		Item	Sample terms
1	System configuration	System processing mode / usage type	centralized processing, distributed processing, interactive processing, usage types (batch processing, real-time processing)
		System configuration	functional allocation, redundant configuration, load distribution, dual system, duplex system, cluster, primary system (currently used system), secondary system (backup system), client/server system (client, server), thin client, web system (web browser, web server), peer to peer, cloud computing, SaaS, PaaS, IaaS, DaaS
		Storage configuration	RAID, NAS, SAN
		Reliability design	fault tolerant, fail-safe, foolproof, human error, UPS
2	System evaluation indexes	Performance characteristics and evaluation of a system	system performance indices (response time, throughput)
		Reliability characteristics and evaluation of a system	reliability indices and reliability calculation (MTBF, MTTR, availability)
		Cost efficiency evaluation of a system	initial cost, operational cost (running cost)

Major Category 4: Technology Element　Middle Category 4: Database

Minor category		Item	Sample terms
1	Database architecture	Database	types and characteristics of databases (relational database)
		Database management system	database management system and its functions (maintenance function, data security protection function)
2	Database design	Data analysis	elimination of data duplication, data dictionary
3	Data manipulation	Data manipulation	database language (SQL)
4	Transaction processing	Transaction processing	exclusive control, failure recovery (method of backup in preparation for a failure, generation management, full backup, differential backup, incremental backup)
5	Database application	Application of databases	data warehouse, metadata, big data

Major Category 4: Technology Element　Middle Category 5: Network

Minor category		Item	Sample terms
1	Network architecture	Role of communications network	network society, information society, ICT (Information and Communication Technology)
		Types and characteristics of networks	LAN (wired LAN, wireless LAN), WAN, services provided by telecommunications carrier, Internet connection service, Internet service provider
		Internet technology	TCP/IP, server, client, routing, global IP address, private IP address, domain, DNS, RADIUS
2	Data communication and control	Transmission methods and lines	packet switching, public line, leased line, FTTH
		Network connection	connection within LAN, connection between LANs, LAN-WAN connection, switching hub, router, Layer-2 (L2) switch, Layer-3 (L3) switch, bridge, gateway, wireless LAN access point, proxy server

Minor category		Item	Sample terms
3	Communications protocols	Protocols and interfaces (network layer, transport layer)	IP address, subnet address, subnet mask, MAC address, routing, IPv4, IPv6, port number
		Protocols and interfaces (application layer)	HTTP, HTTPS (HTTP over TLS), SMTP, POP3, IMAP, FTP
4	Network management	Network operations management (fault management)	operation statistics, fault isolation, fault cause identification, recovery action
5	Network application	Internet (e-mail)	mail server, mail client (mail software), relay method, broadcast mail, mailing list, mailbox, cc, bcc, MIME
		Internet (web)	web browser, markup languages (HTML, XML), hyperlink, web application software, cookie, domain name, URL
		Internet (file transfer)	FTP server, FTP client, upload, download, online storage
		Intranet / Extranet	VPN (Virtual Private Network), private IP address, EC (Electronic Commerce), EDI (Electronic Data Interchange)
		Communication services	leased line service, circuit switching service, packet switching service, Internet service, IP telephone, mobile communication, mobile communication standard (LTE, etc.), tethering, wide-area Ethernet, IP-VPN, Internet VPN, VoIP (Voice over Internet Protocol), best effort

Major Category 5: Project Management　Middle Category 6: Project Management

Minor category		Item	Sample terms
1	Project management	Project management	PDCA management cycle, project, project management, project environment, project frameworks, project self-management (change management, problem discovery, problem reporting, measures planning, documentation)
2	Project integration management	Project integration management	project integration management, understanding and management of an overall project
3	Project stakeholder management	Project stakeholder management	project stakeholder management, stakeholder
4	Project scope management	Project scope management	project scope management, WBS, activity, baseline
5	Project resources management	Project resources management	project resources management and its processes (project team management), staff (project manager, project member, project management team), PMO (Project Management Office), device, equipment, material, software, hardware, external human resources management
6	Project time management	Project time management	project time management and its processes (ordering of activities, estimation of activity period, schedule creation), activity list, PERT (Program Evaluation and Review Technique)
7	Project cost management	Project cost management	project cost management, cost baseline, cost of resources
8	Project risk management	Project risk management	project risk management and its processes (risk identification, risk evaluation, response to risk, risk control), risk
9	Project quality management	Project quality management	project quality management, failure report

Minor category		Item	Sample terms
10	Project procurement management	Project procurement management	project procurement management and its processes (procurement planning, supplier selection, procurement management), buyer, supplier, utilization method of external resources
11	Project communications management	Project communications management	project communications management, communication, typical information distribution methods (push, pull, feedback, e-mail, voicemail, video conference, paper)

Major Category 6: Service Management　Middle Category 7: Service Management

Minor category		Item	Sample terms
1	Service management	SLA	SLA (Service Level Agreement), customer satisfaction, service time, response time, service and process performance
2	Service design and transition	Service design and transition	service acceptance criteria, service design document, non-functional requirements, transition, operational service level agreement, activity and system transition, transition planning, transition rehearsal, transition judgment, notification of transition, transition evaluation, operational test, acceptance test, handover of operations
3	Service management process	Service level management	service level management, service target, review, service improvement plan, service catalog
		Service reporting	service reporting, performance with respect to service target, trend information
		Service continuation and availability management	service continuation and availability management, service continuation planning, RTO, RPO, recovery (failure recovery, disaster recovery), cold standby, hot standby, availability, reliability, maintainability
		Capacity management	capacity management, monitoring, management index (CPU utilization, memory utilization, file usage volume, network utilization, etc.), threshold
		Supplier management	supplier management, supplier, agreement, internal group, OLA (Operational Level Agreement)
		Management of incidents and service requests	management of incidents and service requests, incident, extent of impact, service request, escalation, workaround, serious incident, near miss
		Problem management, configuration management, change control, release and deployment management	problem management (problem, known error, root cause, preventive action, trend analysis), configuration management (asset management), change management (change management, impact on service as a result of change), release and deployment management (association between configuration management and change management)
4	Service operation	Service operation	system operations management, operation (system monitoring, operation, status notification, work instructions, operation log), service desk (inquiries from the user)
5	Facility management	Facility management	facility management, building/office management, equipment management (power supply, air conditioning equipment, etc.), UPS, security cable wire

Major Category 6: Service Management　Middle Category 8: System Audit

Minor category		Item	Sample terms
1	System audit	Purpose and procedure of system audits	purpose of system audits, reliability, security, efficiency, effectiveness, audit tasks, system auditability (log, trace), system audit quality evaluation
		Information security audit	Information Security Audit Standards, Information Security Management Standards
		Compliance audit	action guideline, ethic, transparency, findings of infringement of rights, finding of problems in the working environment
2	Internal control	Internal control	separation of job duties, mutual checks (separation of work), setup of implementation rules, establishment of a check system, role played by IT in internal control, risk evaluation and treatment, control activities, information and communications, monitoring, response to IT, IT control (IT overall control, IT operation processing control), IT governance
		Evaluation and improvement of compliance	continuous evaluation of the status of compliance with standards and internal/external codes of conduct, arrangement of internal control, CSA (Control Self Assessment)

Major Category 7: System Strategy　Middle Category 9: System Strategy

Minor category		Item	Sample terms
1	Information systems strategy	Development of information systems strategy	information computerization committee, computerization promotion system
2	Business process	Business process improvement and problem solving	workflow system, BPR (Business Process Reengineering), process viewpoint, effective utilization of IT, improvement in business efficiency through information system utilization, system utilization for communication, SNS (Social Networking Service), use of e-mail for work
3	Solution business	Types of solution services	cloud service, SaaS, PaaS, IaaS, ASP
4	System utilization promotion and evaluation	System utilization promotion	information literacy, data utilization, effective utilization of IT (including IoT, big data, AI, etc.), popularization and awareness raising
		Evaluation and verification of information system utilization	ROI (Return on Investment) analysis of information system, evaluation and verification of system utilization, understanding of work details and existence of change in the workflow, understanding and evaluation of the operation status of information system, improvement of information system
		Information system disposal	system life cycle, data erasing

Major Category 7: System Strategy　Middle Category 10: System Planning

Minor category		Item	Sample terms
1	Computerization planning	Considerations in computerization planning (risk analysis of information systems installation)	risk analysis targets, occurrence frequency/effect/bounds of a risk, details and amount of damage according to the type of risk, measures against risks (risk avoidance, loss prevention, loss reduction, risk transfer, risk retention, etc.), loss of property, loss of responsibility, net operating income loss, human loss, risk measurement
2	Requirements definition	Requirements analysis	identification of requirements, analysis of requirements, steps for requirements analysis (user needs study, analysis of investigation details, current state analysis, definition of problems/issues, requirements specification)
		Requirements definition	purpose of requirements definition, definition of requirements (operational requirements definition, business processing procedure, functional requirements definition, non-functional requirements definition, security requirements, information/data requirements)
3	Procurement planning and implementation	Procurement and procurement planning	use of external resources (system integrator, SI service provider, outsourcing), management of system assets and software assets (license management, configuration management)
		Procurement implementation (procurement methods)	typical procurement methods, RFI (Request For Information)
		Procurement implementation (request for proposal)	RFP (Request For Proposal), RFQ (Request For Quotation), scope of procurement, system model, service requirements, target schedule, contract conditions, vendor management requirements, vendor project organization requirements, evaluation of the techniques and track record of the vendor, proposal and quotation
		Procurement implementation (vendor selection)	proposal evaluation criteria, requirements conformance, breakdown of expenses, schedule by process, final delivery deadline
		Procurement implementation (conclusion of a contract)	receiving system, cost, receiving time, role allocation of ordering party and vendor company, model contract for software development outsourcing, information system/model transaction contract, intellectual property right license agreement

Major Category 8: Corporate and Legal Affairs　Middle Category 11: Legal Affairs

Minor category		Item	Sample terms
1	Management and organization theory	Business management (business management / management organization)	PDCA, CEO (Chief Executive Officer), CIO (Chief Information Officer), CISO (Chief Information Security Officer), CPO (Chief Privacy Officer)
		Business management (human resources management / behavioral science)	case study, e-Learning, leadership, communication
		Business management (risk management)	BCP (Business Continuity Plan), BCM (Business Continuity Management), BIA (Business Impact Analysis)
		Computer literacy	computer literacy
2	OR and IE	Inspection techniques and quality control techniques	sampling, simulation, seven QC tools, new seven QC tools
		Analysis of business operation and operational planning	data mining, brainstorming, Delphi method, decision tree
3	Accounting and financial affairs	Corporate activities and accounting	fixed cost, variable cost, cost, profit, gross profit, operating profit, variable cost ratio, break-even point, depreciation, lease, rental
		Financial statements	balance sheet, cash flow statement, assets (net assets, current assets, fixed assets, deferred assets, tangible assets, intangible assets), liability (current liability, fixed liability), current ratio

[Required Skills]

In ‘Required skills’ column below, “to *do something*” refers to performing some parts of the activities independently.

Major item	Minor item	Required skills	Sample terms
I Items concerning planning of information security management and information security requirements			
1 Planning of Information Assets Management	1-1 Identification of information assets and clarification of value	To understand the necessity, methods, and procedures of identifying the information assets used in the department (such as the information system, data, documents, facility, personnel, etc.), to understand the necessity, methods, and procedures of clarifying their values (importance) from the three aspects of confidentiality, integrity, and availability, and to clarify the value through close investigation of documents and hearing.	information assets, value (importance), three characteristics (confidentiality, integrity, availability)
	1-2 Clarification of management responsibility and permissible range of usage	To understand the role of the person responsible for management of information assets, and to examine the management policy and management system of information assets in the department. Also, to understand the necessity, methods, and procedures of acceptance and confirmation of information assets, clarification of the permissible range of usage, and change and disposal management on the basis of policies decided by the organization and department, and to consider and propose rules of them by himself/herself.	information assets acceptance, change management, usage management, disposal management, management system
	1-3 Creation of information assets ledger	To understand the necessity, methods, and procedures of creating an information assets ledger, and to create the information assets ledger.	information assets ledger, inventory-taking of assets
2 Information Security Risk Assessment and Risk Response	2-1 Identification, analysis, and evaluation of risks	To understand concepts and techniques of analyzing threats, vulnerabilities, and values of information assets used the department from the aspects of physical, technical, and human factors, and estimating the size of the risk by understanding the frequency of occurrence and the result of occurrence of the event quantitatively and qualitatively, and to perform evaluation on the basis of the risk acceptance standard decided by the organization. Also, to identify new risks accompanying the occurrence of new types of threats, changes in the information system, and changes in the organization, and to evaluate them in the same way.	threat, vulnerability, cyberattacks (targeted attack, zero-day attack, etc.) value of assets, physical factors, technical factors, human factors, ease of occurrence of an event, consequences (extent of damage), risk acceptance standard
	2-2 Consideration of measures against risks	To understand the concept, necessity, methods, and procedures of risk response for all identified, analyzed, and evaluated risks based on each of the categories of physical, human (administrative), and technical measures, and to consider measures against risks. Also to identify the current implementation status of the considered measures. To understand the size of risks, cost required for implementing the measures against risks, and the concepts, methods, and procedures of the action to be taken against the risks that remain even after taking measures, and to consider the priority of measures against risks (including the view of whether or not the risks are tolerable).	measures against risks, physical measures, human (administrative) measures, technical measures, residual risks

Major item	Minor item	Required skills	Sample terms
	2-3 Development of a risk response plan	To understand the purpose of creating a risk response plan and the content to be specified (such as the implementation items, resources, responsible persons, scheduled time of completion, and evaluation method of implementation results) on the basis of the priority of the considered measures against risks and to develop the risk response plan.	risk control, risk hedge, risk financing, computerization insurance, risk avoidance, risk sharing (risk transfer, risk diversification), risk retention, risk aggregation, risk response plan
3 Presentation of Information Security Requirements Concerning Information Assets	3-1 Physical and environmental security	To understand the concept and mechanism of physical and environmental security for protecting the information assets, thereby to consider the method of entrance and exit control for offices, method of carry-in and carry-out control of information assets, method of physical protection of the network, and scope of intended objects (including mobile devices) for which information security needs to be maintained, and to compile the requirements on the basis of the risk response plan.	entrance and exit control method, carry-in and carry-out control, network, mobile device
	3-2 Technical and operational security concerning the information system of the department	To understand the concept and mechanism of technical and operational security for protecting the information assets, and to compile the requirements on the basis of the risk response plan while receiving the technical support from the information system department. The requirements include the items described below: • Business requirements concerning access control, user access management, user responsibility • Information security requirements concerning the information system developed and acquired in the department, information security in the development and support process, and handling of test data, etc. • Procedures and responsibility of operation Also, if necessary, to compile and propose the requirements for the information system to be used by the department among the information systems owned by the information system department, in the same manner.	access control, business requirements, user access management, information security requirements, development and support process, acceptance test, test data
4 Presentation of Information Security Requirements for Continual Assurance of Information Security	4-1 Presentation of Information Security Requirements for Continual Assurance of Information Security	To understand the information security requirements necessary for continuously ensuring information security of the department at the time of occurrence of a failure or disaster, and to confirm that the requirements have been incorporated into the business continuity plan. Also to propose improvements (incorporating the requirements in the plan, specifying additional procedures, and documenting them) in case the requirements are excessive or insufficient.	failure, disaster, business continuity management, information security continuity

Major item	Minor item	Required skills	Sample terms
II Items concerning operation and continual improvement of information security management			
5 Management of Information Assets	5-1 Maintenance and management of the information assets ledger	To understand the content to be described in the information assets ledger, and the necessity and procedures of maintenance and management of the ledger, thereby to appropriately reflect the acceptance, deployment, change in the administrator, change in the configuration, transfer to another department, and disposal of the information assets in accordance with the internal regulations of the organization including the information security policy (hereinafter, "the information security regulations"), and the rules specified by the department, and to perform maintenance and management of the information assets ledger.	information security policy, acceptance of information assets, deployment, change in administrator, change in configuration, transfer to another department, disposal
	5-2 Management of media	To understand the methods and procedures of management of portable media (carrying in/out to/from the office in the department, and disposing of) necessary for preventing the occurrence of an information security incident (hereinafter, "incident"), and to provide advice for enabling the members of the department to appropriately implement the predetermined procedures.	carry in/out media, disposal, portable media (USB memory, DVD, hard disk, etc.)
	5-3 Recording of usage status	To understand the necessity, methods, and procedures of managing the information assets, thereby to identify the usage status of the target assets and track their deployment, administrator, and change in configuration, and to record the usage status of the information assets.	deployment of information assets, administrator, change in configuration
6 Assurance of Information Security during Use of the Information System of the Department	6-1 Protection from malware	To understand the types of malware and the purpose and mechanism of protection of information assets from malware, to deepen the understanding of the members of the department regarding anti-malware and anti-virus software, and to promote compliance with information security regulations.	malware, computer virus, Trojan horse, worm, anti-virus software
	6-2 Backup	To understand the concept, methods, and procedures of backup for preventing loss of important data, to deepen the understanding of the members of the department regarding the importance of backup, and to promote implementation of backup in accordance with the information security regulations.	backup (acquisition cycle, storage location), restore
	6-3 Acquisition and monitoring of logs	To understand the types of logs related to the information system, such as the system log, system error log, alarm record, usage status log, etc., and the purpose of acquiring the logs, and to monitor information security accidents and information security violations such as unauthorized intrusions on the basis of the relevant records and periodic analysis.	log monitoring, log record, log analysis, storage method
	6-4 Maintenance of information security during transfer of information	To understand the concept and mechanism of maintenance of information security during information transfer, and to perform management of checking the content of the information transferred by the member of the department, controlling the referable websites, and controlling of carrying in/out devices in accordance with information security regulations and the functions provided by the information system.	e-mail, file, referable websites, carry in/out devices
	6-5 Vulnerability management	To understand the concept, necessity, methods, and procedures of vulnerability management, and to obtain patch information on the basis of the usage status of the information system of the department, and to promote patch application on the basis of the patch application criteria specified by the organization.	vulnerability management, patch management, patch application standard

Major item	Minor item	Required skills	Sample terms
	6-6 User access management	To understand the concept, necessity, methods, and procedures of management of access to the information system, offices, and other information assets, and to periodically ensure that the access rights assigned to the department members are set appropriately by reflecting changes in the relevant duty and personnel changes including employment and retirement.	authentication method, password, password strength, change cycle, change method, biometric authentication, IC card, token, access right
	6-7 Inspection of operational status	To understand the necessity, methods, and procedures of inspection of the operational status of the information system in the department, and to confirm that information security is assured in accordance with the information security regulations. Also, to report to and consult the superior when an inappropriate item is detected, and to take actions appropriately.	information security policy, monitoring, measurement, analysis, evaluation, vulnerability inspection, intrusion inspection
7 Assurance of Information Security during Outsourcing of Business	7-1 Investigation of information security at the outsourcing contractor's end	To understand the necessity, methods, and procedures of investigation of information security at the outsourcing contractor's end, and to check beforehand the differences in the information security requirements demanded of the outsourcing contractor, such as the information handling rules, and the actual conditions at the outsourcing contractor's end in cooperation with the person in charge of the contract. Also, if corrections are needed on the basis of the results of prior check of the actual conditions at the outsourcing contractor's end, and to make adjustments with the outsourcing contractor in cooperation with the person in charge of the contract, including the method, time period, and costs for the measures to be taken. And to check that information security is assured at the time of the start and during the update of outsourcing in cooperation with the person in charge of the contract.	outsourcing contractor management, information handling rules, information security requirements
	7-2 Implementation of information security management at the outsourcing contractor's end	To understand the necessity, methods, and procedures of performing information security management at the outsourcing contractor's end, and to perform explanation of information security requirements relevant to the outsourced task to the responsible person of the outsourcing contract and elimination of the discrepancies with the content of the contract in cooperation with the person in charge of the contract. To check the implementation status of fraud prevention and protection of confidentiality after the conclusion of the contract in cooperation with the person in charge of the contract. If there are discrepancies between the actual conditions of the outsourced task and the contents of the contract, to perform the clarification of the reasons and solutions for the discrepancies and the corrective measures in cooperation with the person in charge of the contract.	outsourcing contractor management, prevention of unauthorized acts and protection of confidentiality, confidentiality agreement
	7-3 End of outsourcing	To understand the concept of the measures that need to be taken when outsourcing finishes, and to provide instructions of performing of collection or disposal of the material and data presented to the outsourcing contractor, and to check the results in cooperation with the person in charge of the contract.	receiving inspection, disposal, system life cycle, data erasing

Major item	Minor item	Required skills	Sample terms
		To compile the status of collection or disposal of the material and data from the outsourcing contractor, and to report it to the superior.	
8 Management of Information Security Incident	8-1 Detection	To understand the methods and procedures for detecting an information security incident, and to detect an incident from among the information security events.	information security event, information security incident, incident response
	8-2 Initial processing	To understand the concept, methods, and procedures of the initial processing of an information security incident, and to perform the items described below: • Contacting the superiors and the relevant departments when an incident is detected, and seeking instructions • Considering the priority of the measures to be taken in view of the size and scope of the impact of the accident upon receiving the instruction as described above, and proposing and implementing measures to avoid expansion of damage • Recording the initial processing for the accident, and reporting the status	information security incident, incident response, accident
	8-3 Analysis and recovery	To understand the concept, methods, and procedures of analysis and recovery of an information security incident, and to perform the items described below: • Investigating the status and scope of harm caused by the accident in cooperation with the information system department, and evaluating the damage and impact • Identifying the cause of the accident on the basis of the security information, various types of information on the accident, operation records collected in the department, and access records	operation record, access record, isolation of the cause
	8-4 Proposal and implementation of preventive measures against recurrence	To understand the concept of prevention of recurrence of information security incidents, and to consider permanent preventive measures against recurrence so that the same accident may not occur again.	recurrence prevention, revision of business procedures
	8-5 Collection of evidence	To understand the concept, methods, and procedures of collection of evidence of the information security incident, and to identify, collect, acquire, and maintain information that could be used as evidence in accordance with predetermined procedures.	evidence, digital forensics
9 Improvement in Awareness of Information Security	9-1 Education and training on information security	To understand the importance of raising awareness about information security, and education and training necessary for raising awareness, and to perform the items described below: • Considering and proposing an education and training plan for understanding the information security policy, the organizational policy and procedure for the duties, and issues and impacts of information security • Supporting the education and training provided by the organization to the departments	information security policy, information security awareness, education and training plan, education material, evaluation of result
	9-2 Advice on information security	To understand the methods and procedures of advice on information security, and to offer advice to the members of the department for performing operation while maintaining the information security.	FAQ, knowledge

Major item	Minor item	Required skills	Sample terms
	9-3 Prevention of information leakage due to internal fraud	To understand the concept of prevention of information leakage due to internal fraud, and to take each of the measures, namely deterrence, prevention, and detection, in accordance with the guidelines on prevention of internal fraud stipulated by the organization.	education and training plan, guidelines on prevention of internal fraud, fraud triangle (opportunity, motivation, rationalization), situational crime prevention
10 Maintaining Compliance	10-1 Guidance to compliance	To understand the concept of maintaining compliance (guidance to compliance), and to perform the items described below: • Notifying the target laws, standards, norms, and information security regulations to the relevant persons, and working toward their general awareness in accordance with the annual education plan stipulated by the organization so that thorough compliance of the related laws, standards, norms, and information security regulations may be ensured • Implementing recurrent transmission (recurrent education) so that awareness about compliance may be established	information security policy, compliance, laws, standards, information ethics regulations
	10-2 Evaluation and improvement of compliance status	To understand the concept of maintaining compliance (evaluation and improvement of compliance status), and to perform the items described below: • Responding to the inspection and evaluation of the compliance status of the laws, standards, norms, and information security regulations, conducted periodically by one's own department or the business operations audit department • Cooperating with the information security audit conducted by a third party (including external parties), arranging the necessary documents, and responding to interviews • Compiling and implementing the measures necessary for improvement as an activity plan based on the findings of the audit department	information security audit, internal audit, self-inspection, findings in the audit
11 Continual Improvement of Information Security Management	11-1 Arrangement and analysis of problems	To understand the concept of continual improvement of information security management (arrangement and analysis of problems), and to perform the items described below: • Arranging the problems that could occur during the operation of information security (such as repulsion by a user, successive appearance of persons violating information security as a result of unrealistic rules, etc.), extracting the relevant parts of the information security regulations, and confirming appropriateness of the current regulations • Extracting the relevant parts of the information security regulations, and confirming appropriateness of the current regulations upon introduction of a new information security technology or a new information system • Confirming that information security is assured when an information system is used	information security policy, analysis of business operations, review techniques, brainstorming

Major item	Minor item	Required skills	Sample terms
	11-2 Revision of information security regulations	To understand the necessity and processes of continual improvement of information security management, and to implement revision of information security regulations, if there is a necessity of revision	PDCA cycle, reform of regulations
12 Collection and Evaluation of Trends and Case Examples concerning Information Security	12-1 Collection and evaluation of trends and case examples concerning information security	To understand the necessity and means of collection and evaluation of trends and case examples concerning information security, and to perform the items described below: • Collecting the security information provided by the information security organizations and product vendors, and evaluating the urgency and necessity of measures to be taken by the organization • Collecting information on the latest threats and accidents from the information security organizations, vendors, and other companies • Collecting the latest security information, information security technical information, and examples of information security accidents from reports, academic journals, and commercial magazines, analyzing and evaluating the information, and considering the necessity and cost effectiveness of its application to the information system • Collecting information such as establishment and amendment/abolishment of laws and standards concerning information security, changes in the conventional wisdom, and new issues regarding compliance	information security organizations (NISC, JPCERT/CC, IPA), case study, group learning, seminar

■ Information Security Management Examination (Level 2)
Syllabus (Version 1.1)

Information-technology Promotion Agency, Japan
IT Human Resources Development Headquarters, Japan
Information-Technology Engineers Examination Center (JITEC)
15th Floor, Bunkyo Green Court, 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/

Sep. 2016