

■ Information Technology Engineers Examination —————

Information Technology Service Manager Examination

(Level 4)

Syllabus

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

Version 4.1

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.

Major category	Minor category	Outline	Required knowledge	Required skills
1 Service Management	1-1 Service Management	<p>Service providers implement service management in order to fulfill service requirements, direct activities for the design, transition, delivery and improvement of services, and control resources and risks.</p> <p>(1) Service requirements Clearly set out the needs of customers and service users as well as those of the service provider as service requirements.</p> <p>(2) Service management system Implement a service management system, an integrated process approach, direct and control service management activities.</p> <p>(3) Risk management Monitor and control the status of service provision, and evaluate and manage the risks relating to a service.</p>	<p>The following regarding service management:</p> <ul style="list-style-type: none"> • Service • Service components • Service management • Management system • SMS (Service management system) • Service requirements • Service quality • Service life cycle • Stages of service life cycle (strategy, design, transition, operation, continuous improvement) • Customers • Service providers • SLA (Service Level Agreement) • Risk management • Risk assessment • JIS Q 20000 series (ISO/IEC 20000) • ITIL • Trends in information technology (including IoT, big data, AI, etc.) 	<ul style="list-style-type: none"> • Implementing efficient and effective service management • Investigating impact on service management systems in the stages of the service life cycle. • Performing risk management and risk assessment concerning the achievement of service management objectives • Identifying customer expectations for a service, and communicating continuously • Leading a team to achieve its objectives for the maintenance and improvement of service quality
	1-2 Establishment and improvement of service management	<p>Apply the PDCA (Plan-Do-Check-Act) methodology to service management systems.</p> <p>(1) Creation of implementation plan Create, implement, and maintain a plan for service management.</p> <p>(2) Implementation and operation Implement and operate a service management system for the planning, transition, delivery, and improvement of services.</p> <p>(3) Monitoring and reviews Monitor, measure, and review the service management system and services.</p> <p>(4) Creation and management of an improvement plan Take actions to continuously improve the performance of the service management system and services.</p>	<p>The following regarding the establishment and improvement of service management:</p> <ul style="list-style-type: none"> • Process approach • Processes, procedures • PDCA • Process capability levels (process maturity levels) • Process assessment • Gap analysis • CSF (Critical Success Factor) • KPI (Key Performance Indicator) • SMART • Continuous improvement • Service and process performance • JIS Q 9001 (Quality management systems – Requirements) 	<ul style="list-style-type: none"> • Planning and constructing the service management system • Measuring and explaining the results of executing service management processes • Performing assessments of process capability levels • Planning and implementing the improvement of service management processes • Monitoring, measuring, analyzing, and reporting the performance of services and processes • Managing projects

Major category	Minor category	Outline	Required knowledge	Required skills
2 Service design and transition	2-1 Planning of new or changed services	Create a service plan for a new service or service change as defined in a change management policy, which is proposed to meet operational needs or improve the effectiveness of a service. <ul style="list-style-type: none"> Identify service requirements Create a plan to meet the identified service requirements. 	The following concerning service planning: <ul style="list-style-type: none"> Service acceptance criteria Change management policy Closure of a service Service pipeline Service portfolio 	<ul style="list-style-type: none"> Identifying service requirements, and creating a service plan Investigating the organizational structure during design, development, and transition Communicating with stakeholders
	2-2 Design and development of new or changed services	Design and develop new or changed services <ul style="list-style-type: none"> Make specific service requirements, and document design. Develop a service on the basis of a documented design. 	The following regarding service design and development: <ul style="list-style-type: none"> Design and development Service design document 	<ul style="list-style-type: none"> Making specific requirements concerning quality of service that must be achieved, such as a service level or service reliability, and creating a design document. Investigating organizational impact, such as the organizational structure during service operations, which is caused by the delivery of a service
	2-3 Transition of new or changed services	Plan and implement transition of new or changed services. <ul style="list-style-type: none"> Use an acceptance test environment to implement a test prior to deployment to an operational environment. Conduct verification on the basis of service acceptance criteria. Deploy an approved new service or service change to an operational environment. Report the achieved results to customers and stakeholders in comparison with the expected results proposed at the planning stage after transition is completed. 	The following regarding service transition: <ul style="list-style-type: none"> Transition Operational service level agreements Transition of operations and systems Transition planning Transition rehearsals Transition decisions Transition notification Transition evaluation Operational tests Acceptance tests Handover of operations Acceptance of application systems Acceptance of services Release and deployment management 	<ul style="list-style-type: none"> Planning and implementing a service transition plan Investigating whether service requirements and the design have been fulfilled on the basis of service acceptance criteria Creating and implementing an acceptance test plan, and evaluating the results Reporting the level of achievement of results
3 Service management processes	3-1 Service delivery processes	(1) Service level management Perform the following to define, agree, record, and manage levels of service: <ul style="list-style-type: none"> Agree to an SLA (the scope of services and the service level targets) with parties concerned. Maintain the SLA with regular reviews. Monitor and record service levels Identify causes behind a non-conformance, and commence corrective action and preventive action. 	Service level management <ul style="list-style-type: none"> Service level Service targets Non-conformance Corrective action Service improvement plans Service catalogs Review of SLA 	<ul style="list-style-type: none"> Negotiating SLAs with customers, and obtaining agreement Regularly monitoring and maintaining service level management processes and SLAs Identifying causes for non-conformance to service levels and opportunities for improvement Creating and maintaining service catalogs
		(2) Service reporting	The following regarding service reporting: <ul style="list-style-type: none"> Performance Workload 	<ul style="list-style-type: none"> Regularly creating, reviewing, and evaluating reports on service and operation performance and achievements

Major category	Minor category	Outline	Required knowledge	Required skills
		Produce agreed, timely, reliable, accurate reports for informed decision making and effective communication.	<ul style="list-style-type: none"> Trend information 	<ul style="list-style-type: none"> Analyzing reports, and identifying and prioritizing actions for improvement Implementing reviews of service provision with concerned persons in order to build a consensus with stakeholders in service provision regarding the direction of improvements
		<p>(3) Service continuity and availability management</p> <p>Perform the following to ensure that the service continuity requirements agreed with customers can be implemented in circumstances after a major loss of service due to a service failure or a disaster.</p> <ul style="list-style-type: none"> Develop a service continuity strategy. Develop a service continuity plan. Test the service continuity plan. Manage the service continuity plan. <p>Perform the following to ensure that the availability requirements agreed with customers can be implemented both under normal circumstances and after a severe service interruption.</p> <ul style="list-style-type: none"> Create, review, and maintain an availability plan. Measure and record the availability. Investigate unplanned non-availability, and take appropriate actions. Predict potential issues, and take preventive action. 	<p>The following regarding service continuity:</p> <ul style="list-style-type: none"> BCP (Business continuity plan)/ BCM (Business Continuity Management) BIA (Business impact analysis) Service continuity plans Commencement (of service continuity plans) Recovery Plan for dealing with unpredicted situations (contingency plan) RTO (Recovery Time Objective) RPO (Recovery Point Objective) RLO (Recovery Level Objective) Disaster recovery Preventive action Fall back Fail-soft Cold standby/hot standby/warm standby <p>The following regarding availability:</p> <ul style="list-style-type: none"> Availability Reliability Resilience Maintainability Response time MTBF MTTR FMEA (Failure Mode and Effects Analysis) FTA (Failure Tree Analysis) SFA (Service Failure Analysis) Fault tolerance 	<ul style="list-style-type: none"> Assessing and managing risks regarding service continuity Making and managing a service continuity plan Testing the service continuity plan in accordance with the business environment Creating a disaster recovery plan, and confirming the feasibility of a plan Analyzing the loss caused by the disruption or functional degradation of an information system Clarifying the importance and urgency levels of the recovery of business operations Deciding the scope of agreement for the permissible range until recovery, such as the decrease service quality level for the service recovery period Defining allowable recovery time and recovery priority considering importance and urgency of the business operations, extent of impact, consistency with other business operations, etc. Defining availability requirements Identifying the weak points of configuration that reduce availability Analyzing and assessing the various risks (e.g., vulnerability) of availability
		<p>(4) Budgeting and accounting for services</p> <p>Perform budgeting operations to plan and manage the budgeting for the cost of service provision. Perform: accounting as an accounting operation; apportioning indirect costs; allocating direct costs; etc. Efficiently manage financial conditions through these activities.</p>	<p>The following regarding budgeting and accounting for services</p> <ul style="list-style-type: none"> Financial management Budgeting operations Accounting operations Billing Apportionment 	<ul style="list-style-type: none"> Managing finances for services and service components Clarifying costs for each cost category and cost item Making and managing a budget

Major category	Minor category	Outline	Required knowledge	Required skills
		<ul style="list-style-type: none"> • Manage budgeting operations. • Manage accounting operations. • Apportion indirect costs, and allocate direct costs. 	<ul style="list-style-type: none"> • ROI • Costs • Direct costs • Indirect costs • Depreciation • TCO (Total cost of ownership) • Indirect person-hours 	<ul style="list-style-type: none"> • Determining the income and expenditure of services, and evaluating and reporting their profitability and validity
		<p>(5) Capacity management Perform the following to obtain and provide necessary capacity (e.g., data processing capability and storage space) in timely and cost-effective ways:</p> <ul style="list-style-type: none"> • Produce a capacity plan. • Model infrastructure along with current and expected future capabilities of such infrastructure. • Determine and analyze how much resources are utilized. • Monitor capacity. • Tune performance, and provide adequate capacity. 	<p>Capacity management:</p> <ul style="list-style-type: none"> • Demand • Capacity • Capacity planning • Monitoring • Thresholds • Business capacity management • Service capacity management • Component capacity management • Capacity database • Modeling and trend analysis 	<ul style="list-style-type: none"> • Performing business capacity management to quantify and manage business plans and needs as future service requirements • Performing service capacity management that supports service planning and resources to achieve service targets • Performing component capacity management to achieve the agreed targets for components • Creating a capacity plan on the basis of the performance and predicted requirements
		<p>(6) Management of Information Security Perform the following to effectively manage information security:</p> <ul style="list-style-type: none"> • Compile the direction of physical, operational, and technological measures to protect the security of information assets as an information security policy, and gain the approval of a manager with the appropriate privileges. • Implement and operate physical, operational, and technological measures for information security management. <ul style="list-style-type: none"> – Secure physical security such as entrance access control, protection from external threats, device installation, maintenance and safe disposal, and asset movement. – Implement network security measures such as firewalls and intrusion detection systems. – Implement measures against malware such as creating preventive measures against damage from malware, creating measures for the early discovery of malware infection, handling malware infection, and training users. 	<p>The following regarding information security management:</p> <ul style="list-style-type: none"> • Information security • Information security policy • Information assets • Threats • Vulnerabilities • Information security risk assessment • Risk analysis • Risk evaluation • Risk acceptance • Controlling physical entry and exit of rooms • Network security solutions (e.g., firewalls, intrusion detection systems) • Privileges • User access management • User authentication • User password management • Special privilege management • Access control • Log information protection • Information security incident 	<ul style="list-style-type: none"> • Introducing and enforcing security measures on the basis of a plan • Identifying information assets • Performing risk management for information security, and selecting appropriate management measures to reduce risk • Creating risk reduction measures • Performing assessments of residual risks • Implementing physical security measures • Implementing security measures for computers • Installing, operating, and managing network security products • Developing, implementing, and promoting the operation rules of measures against malware • Considering malware infection prevention and measures for its early detection • Implementing and operating anti-malware software • Developing, implementing, and promoting the rules of managing data

Major category	Minor category	Outline	Required knowledge	Required skills
		<ul style="list-style-type: none"> – Implement measures for data security such as data management standards, creating measures for the occurrence of a security problem, and implementing and operating preventive solutions against information leakage. • Implement periodic risk assessment in order to identify information security risks, and implement specific measures for management in order to prevent or reduce impact of the identified risks. • Handle information security incidents with a priority that is appropriate for the information security risk according to an incident or service request management process. 	<ul style="list-style-type: none"> • Malware • BYOD (security management) • Information security management standards (JIS Q 27000 family standards) • ISMS (Information Security Management System) 	<ul style="list-style-type: none"> • Implementing and operating solutions for preventing information leakage • Regularly inspecting and analyzing obtained log trails, and taking necessary measures • Appropriately handling an information security incident when it occurs
	3-2 Relationship processes	<p>(1) Business relationship management Perform the following activities in order to establish a relationship between a service provider and a customer.</p> <ul style="list-style-type: none"> • Manage customer relationship and customer satisfaction. • Communicate with customers. • Review service performance. • Handle complaints. • Measure, analyze, and review customer satisfaction levels. 	<p>The following regarding business relationship management:</p> <ul style="list-style-type: none"> • Users • Stakeholders • Customer satisfaction • Complaints 	<ul style="list-style-type: none"> • Managing customer relationship and customer satisfaction • Fulfilling responsibility to explain quality of service to a customer, and convincing a customer of the value of a service through communication • Reviewing and reporting service performance • Understanding how to investigate customer satisfaction, analyzing and evaluating the investigation results
		<p>(2) Supplier management Perform the following activities when a supplier is used by a provider to implement and operate service management processes.</p> <ul style="list-style-type: none"> • Reach agreement on contract documents between a service provider and a supplier and service levels. • Ensure proper management of sub-contracted suppliers who are contracted by lead suppliers. • Measure, monitor, and review supplier performance. 	<p>The following regarding supplier management:</p> <ul style="list-style-type: none"> • Governance • Supply chain (for service provision) • Suppliers • Lead suppliers • Sub-contracted suppliers • Contracts • Internal groups • OLA (Operational level agreements) • Cloud services such as SaaS, PaaS, IaaS, etc. (of utilization) 	<ul style="list-style-type: none"> • Governing processes effectively operated by suppliers • Negotiating to reach agreement on contract documents between a service provider and a supplier and service levels • Ensuring proper management of sub-contracted suppliers who are contracted by lead suppliers. • Gaining the cooperation of providers for maintenance and improvement of service quality • Measuring, monitoring, and reviewing supplier performance
	3-3 Resolution processes	<p>(1) Incident and service request management Establish and implement the following procedures to restore as swiftly as possible the</p>	<p>The following regarding incident and service request management:</p> <ul style="list-style-type: none"> • Incidents (unplanned interruptions to a service, reductions in the quality of a service or failures 	<ul style="list-style-type: none"> • Detecting incidents early, and organizing and recording measures for dealing with them • Conducting analysis for resolving incidents

Major category	Minor category	Outline	Required knowledge	Required skills
		<p>service agreed with a customer, or to respond to service requests.</p> <ul style="list-style-type: none"> Recording, allocation of priority, classification, escalation, resolution, and closure <p>Provide information continuously to customers about the progress of incidents and service requests.</p> <p>For serious incidents:</p> <ul style="list-style-type: none"> Reach agreement with a customer on definition. Classify and manage the incidents in accordance with a procedure. Notify top management about the incidents, and manage the incidents under the supervision of the person in charge. Review after recovery. 	<p>of configuration items that have not yet impacted a service)</p> <ul style="list-style-type: none"> Serious incidents Service requests (standard changes, requests for information, requests for guidance or requests for access to standard services, etc.) Impact Avoidance measures Escalation Recording Prioritizing Classifying Resolving Closing Recovery Resolution target time Incident models 	<ul style="list-style-type: none"> Leading a resolution team to perform and manage incident management processes Resolving incidents, and processing service requests Communicating effectively about serious incidents Evaluating incidents for possible security implications
		<p>(2) Problem management</p> <p>Perform the following to minimize disruption to the customers' business by proactive identification and analysis of the cause of incidents and by managing problems to closure:</p> <ul style="list-style-type: none"> Establish and implement a procedure of identification, recording, allocation of priority, classification, updating of records, escalation, resolution, and closure for problems. Take preventive action to reduce potential problems. Pass changes, which are required to correct the root cause of problems, to the change management process. Review and report the effectiveness of problem resolution. Accumulate the root cause, resolution measures, and avoidance measures of a resolved problem in order to be able to use these when an incident occurs. 	<p>The following regarding problem management:</p> <ul style="list-style-type: none"> Problems Known errors Root causes Preventive action Trend analysis Single point of failure Recording Prioritizing Classifying Escalation Resolving Closing 	<ul style="list-style-type: none"> Performing problem management: <ul style="list-style-type: none"> Analyzing and evaluating failure impacts Managing failure histories (known errors) Identifying failures, diagnosing causes, and recovering from failures, and developing workarounds Managing target date for resolution Resolving problems by using methods such as the KJ method, the KT method, the Seven Basic Tools of Quality, brainstorming, and the 5 Whys Analyzing problem trends, and investigating latent problems Communicating workarounds, permanent solutions, or progress of problems to persons concerned Evaluating and reporting the performance of problem management
	3-4 Control processes	<p>(1) Configuration management</p> <p>Perform the following to define and control the components of the service and infrastructure and to maintain accurate configuration information:</p> <ul style="list-style-type: none"> Plan and implement configuration management. 	<p>Configuration management:</p> <ul style="list-style-type: none"> CI (Configuration items) Storage of configuration items CMDB (Configuration management database) Configuration baseline Configuration identification 	<ul style="list-style-type: none"> Planning configuration management Designing and operating configuration management systems Building, maintaining, and managing configuration management databases

Major category	Minor category	Outline	Required knowledge	Required skills
		<ul style="list-style-type: none"> Identify and define configuration items. Accept and record approved identifiable configuration items. Explain and report the configuration status. Verify and audit the configuration. Maintain and manage a configuration management database. 	<ul style="list-style-type: none"> Versions Related change requests and problems Configuration audits Asset management SAM (Software asset management) Basic license JIS X 0164-1(Software asset management -- Part 1: Processes) 	<ul style="list-style-type: none"> Understanding and identifying the details of configuration items Performing and reporting on the version control and change management of configuration items Verifying and auditing that management information matches actual systems
		<p>(2) Change management Record, classify, assess, and approve requests for change in a controlled manner, perform a review of change implementation according to a schedule and a deployment and post-implementation review</p> <ul style="list-style-type: none"> Clearly define and document the scope of a change. Record requests for change, and appropriately classify them. Assess requests for changes for risk, impact, and business benefit. Reverse or remedy unsuccessful changes. Review post-change results Periodically analyze and assess change logs, and establish and maintain a basic policy and procedure for emergency changes. 	<p>Change management:</p> <ul style="list-style-type: none"> Changes RFC (Requests for change) Requests for change (emergency change, normal change, standard change) Recording requests for change Classifying (urgent, emergency, major, and minor) Assessment Accepting requests for change Change schedule Reversing Post-implementation review 	<ul style="list-style-type: none"> Accepting requests for changes Prioritizing requests for changes, and classifying them appropriately Perform assessment of impact and risk for services and customers, and permitting changes that are acceptable Managing change schedules Analyzing change records Improving change management processes
		<p>(3) Release and deployment management Perform the following for efficient deployment into an operational environment:</p> <ul style="list-style-type: none"> Make plans for release and deployment. Configure and test releases. Deploy a release to an operational environment. Link with change management. 	<p>The following regarding release and deployment</p> <ul style="list-style-type: none"> Releases Emergency releases Deployment Release and deployment plans Acceptance criteria for releases Building (of releases) Acceptance testing environments Operational environments Restoration (to correct failed releases) (Release) distribution (policy) 	<ul style="list-style-type: none"> Planning release and deployment Planning and deploying releases Transition to a production environment Measuring and analyzing the results of a release to determine whether it has been successful or not
4 Service operation	4-1 System operations management	<p>Perform the following to manage system operation appropriately:</p> <p>(1) Operation management</p> <ul style="list-style-type: none"> Create an operation plan for daily activities and planned activities. Create an operation plan for new applications. 	<p>The following regarding system operations management:</p> <ul style="list-style-type: none"> Managing operational resources (human resources such as personnel, and technological infrastructure resources such as hardware, software, data, and networks) Managing the operation of virtual machines 	<ul style="list-style-type: none"> Developing operation plans Designing operation methods for failures Developing failure measures (e.g., degraded operation) Based on allowable recovery time and recovery priorities, planning the methods and procedures of backups

Major category	Minor category	Outline	Required knowledge	Required skills
		<ul style="list-style-type: none"> Define management standards for the notification of important changes to operational status. <p>(2) Fault management</p> <ul style="list-style-type: none"> Create recovery and degraded operation plans to perform appropriate operation when a system fault occurs. Consider and operate high-availability systems on the basis of a policy for service continuity and availability management through technical measures such as providing redundancy for their devices. <p>(3) Operation methods during failures</p> <ul style="list-style-type: none"> Clarifying and verifying alternative processing procedures, recovery procedures, and organization up to recovery to speed up failure recovery and improve service continuity and availability <p>(4) Performance measurement</p> <ul style="list-style-type: none"> Performing measurement of performance on the basis of a capacity management policy 	<ul style="list-style-type: none"> Job management Data management User management Knowledge concerning information security management such as identity authentication, access control, privilege management, and trail management functions Basic knowledge concerning capacity management Knowledge concerning technologies and solutions that enable high availability Cold start, warm start 	<ul style="list-style-type: none"> Planning and implementing resolutions for capacity bottlenecks, and the efficient use of resources Performing information security management for operations Considering and operating high-availability systems with technical measures such as redundancy for their computers and communication devices Designing management standards for the notification of important changes to operational status Creating an operation plan for applications
	4-2 Operation	<p>Perform the following activities for appropriate operations:</p> <p>(1) System monitoring and operation Perform monitoring of the service performance status, system operational status, and faults in order to keep track of system operational status as well as service performance status, and to promptly address troubles:</p>	<p>The following regarding operations:</p> <ul style="list-style-type: none"> System monitoring and operation Operations support tools (monitoring tools, diagnostic tools) 	<ul style="list-style-type: none"> Monitoring and managing system operational status Using operations support tools Creating system operation procedures
		<p>(2) Operational status management Record and report operational status in conjunction with system operational status monitoring.</p>	<ul style="list-style-type: none"> Recording and reporting operational status 	<ul style="list-style-type: none"> Recording and reporting system operational status Collecting, analyzing, and reporting system monitoring data
		<p>(3) Job scheduling Create schedules for scheduled processes, create procedures for handling and processing exceptions and unplanned processes, and record, report and manage job processing results so that output can be obtained in a timely manner in accordance with a data processing cycle.</p>	<ul style="list-style-type: none"> Job scheduling Schedule design 	<ul style="list-style-type: none"> Creating and maintaining job schedules Managing job schedules Designing job schedules and jobnet
		<p>(4) Output management Manage output services such as printing.</p>	<ul style="list-style-type: none"> Form delivery and media management Handling secret forms and bulk forms Storing and discarding media 	<ul style="list-style-type: none"> Implementing and managing form delivery services Managing media

Major category	Minor category	Outline	Required knowledge	Required skills
		(5) Backup Create procedures and methods for backup and recovery, implement and use backup management tools, and perform data backup.	<ul style="list-style-type: none"> Backup types Rollback/rollforward 	<ul style="list-style-type: none"> Designing how to back up data and systems, and maintaining and managing the backups Installing and utilizing backup management tools
		(6) Personnel management Put in place a working system for operations personnel, or perform activity management concerning commission if personnel are supplied by an external party.	<ul style="list-style-type: none"> Personnel management Related laws such as the Labor Standards Act 	<ul style="list-style-type: none"> Establishing an appropriate work system Developing staff on the basis of the work system, or the content of outsourcing and operations management
	4-3 Service desk	A service desk is the support group who acts as the direct contact for customers and takes charge of a large portion of the total support work. It serves as a daily liaison with users and handles incidents and service requests.	<p>The following regarding service desk:</p> <ul style="list-style-type: none"> Service desk Level 1 support Level 2 and 3 support Organizational structure for service desk (local service desk, virtual service desk, central service desk, follow-the-sun service desk) Call center SPOC FAQ CTI Knowledge base Staffing (maintaining staff skills, managing working schedules, and deciding the necessary number of staff members) Management indicators (average response time, call abandon rates, talk time, availability, resolution rates, customer satisfaction) 	<ul style="list-style-type: none"> Supporting customers (interpersonal and communication skills) Managing and operating the support infrastructure of a service desk Setting, monitoring, and evaluating management indicators or indexes (monitoring the progress of incidents and service requests, analyzing calls, and understanding and explaining problems and points for improvement) Performing incident and service request management processes (initial supports) Using support tools such as knowledge bases and diagnostic scripts
5 Facility management	5-1 Basic technology of hardware	For the purpose of stable operation of hardware (e.g., computer, related devices) installed or to be installed, perform activities such as installation, set up, normal functional maintenance, enhancement, fixing of failures, and instruction of operation.	<p>Hardware:</p> <ul style="list-style-type: none"> IT architecture (hardware) Basic technology of hardware Installation and maintenance of hardware products International hardware standards and related specifications Techniques for repairing hardware products 	<ul style="list-style-type: none"> Having expertise in hardware, and providing team members with technical guidance on the installation and maintenance of systems
	5-2 Basic technology of software	For the purpose of stable operation of software (e.g., computer programs, software products) installed or to be installed, perform activities such as installation, set up, normal functional maintenance, enhancement, fixing of failures, and instruction of operation.	<p>Software:</p> <ul style="list-style-type: none"> IT architecture (software) Installation and maintenance of software products System software products and their operational environments International software standards and related specifications 	<ul style="list-style-type: none"> Having expertise in software, and providing team members with technical guidance on the installation and maintenance of systems

Major category	Minor category	Outline	Required knowledge	Required skills
			<ul style="list-style-type: none"> • Understanding and utilizing network technologies 	
	5-3 Management of system maintenance	<p>With expertise in hardware, software, and facilities, maintain and repair hardware and software in accordance with service requirements.</p> <ul style="list-style-type: none"> • Develop a plan for system maintenance. • Install and maintain hardware and software. • Develop and implement a plan for preventive maintenance. 	<p>Management of system maintenance:</p> <ul style="list-style-type: none"> • Installing and maintaining hardware products and software products • Designing and implementing structures for mutual backup with remote centers 	<ul style="list-style-type: none"> • Maintaining hardware products according to their maintenance manuals • Utilizing instruments and test tools necessary to maintain hardware • Understanding the specifications and manuals of software products, and installing the products • Understanding the support manuals of software products, and supporting their users

Major category	Minor category	Outline	Required knowledge	Required skills
	5-4 Facility management	<ul style="list-style-type: none"> • Design, construct, manage, maintain, and operate IT-related facilities that meet the usability and maintainability of a data center. • Design, lay out, maintain, and operate a physical network (communications network). • Install, transfer, update, and migrate computer systems. • Identify the causes of impacts on the environment, and investigating the necessary measures. 	Facility management: <ul style="list-style-type: none"> • Managing facilities • Trends in the latest technology of facilities and network products • Reliability, availability, and maintainability of facilities • Basics of the laws, regulations, and standards of facility management • Environmental aspects • Green IT • DPPE (Datacenter performance per energy) (GEC, PUE, ITEE, ITEU, etc.) 	<ul style="list-style-type: none"> • Designing, constructing, managing, and maintaining facilities with expertise in technology • Resolving technical problems related to facility management
	5-5 Equipment management	<ul style="list-style-type: none"> • Design, construct, maintain, and operate the facilities (or equipment) of the data center. Take measures against faults for related equipment. • Take measures for safety management in constructing the facilities (or equipment) of the data center. • Design, construct, maintain, and operate equipment for security and disaster prevention. 	<ul style="list-style-type: none"> • Equipment management • Building management (surge protection devices such as quake-absorbing unit, lightning arrester, accident/crime prevention facility, and safety management-related knowledge, etc.) • Electric facilities (UPS, private power generator, etc.) • Air-conditioning facilities (air-conditioning equipment, hot aisle, cold aisle, etc.) • Communication facilities (MDF, IDF, etc.) • Standards for Information System Safety Measures • Basics of the laws and regulations related to safety and health 	<ul style="list-style-type: none"> • Designing, constructing, maintaining, and operating data center facilities (or equipment), and other facilities (or equipment) such as offices and factories where IT devices are installed

**■ Information Technology Service Manager Examination (Level4)
Syllabus (Version 4.1)**

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/>

September 2016