■ Information Technology Engineers Examination

Systems Auditor Examination

(Level 4)

Syllabus

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

Version 3.1

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 Planning of System Audits	1-1 Preparation of documented medium- and long-term plan	Document a medium- and long-term plan for system audits that address medium to long term management plans, information strategies, and information system plans in order to inspect and evaluate IT governance improvements and compliance in an effective and efficient manner, with the aim of achieving business objectives. In the documented medium- and long-term plan, include medium- and long-term audit policy, high priority audit targets, a personnel and skill development plan for system audit engineers, budget plan, change management process regarding how to align the system audit plan with changes in the business strategy and top management policy, and so on. This plan is approved by the top management after appropriate review.	• Roles and procedures of a system audit • Determination of audit purpose • IT governance • Business management in general • Medium- and long-term business strategies • Medium- and long-term information strategies • Trends in information technology • Education and training for system audit engineers • Planning, development, operations, and maintenance of information systems • Embedded systems • Risk analysis and risk-based approach • Information security • IT control and internal control • Linkage and alignment with other audits (such as accounting audit and business operations audit) • Engagement of external experts	• Understanding the business strategy, management organization, and business management • Understanding the risks related to IT governance to successfully make an audit plan • Understanding information strategy • Understanding the overall picture of information systems • Understanding information system plans • Deploying system audit procedures • Determining the audit policy, audit purpose, and high priority audit theme • Understanding embedded systems • Understanding risks and related controls • Collecting the information required for developing the medium- and long-term plan from corporate managers, information system departments, and user departments • Investigating the necessity of engaging external experts • Creating a medium- and long-term audit plan based on risk-based approach
	1-2 Preparation of documented annual plan	Based on the documented medium- and long-term plan, document an annual plan on an annual basis. In documenting the annual plan, explicitly describe the annual goals of the system audit department in line with the business plan and information system plan for the year. In the documented annual plan, include the audit purpose, audit targets, high priority audit theme, implementation framework, implementation schedule, employment and training plan for system audit engineers, expense budget, revised internal audit standards and revision of such standards.	• Roles and procedures of a system audit • IT governance • Business management in general • Annual business plan • Annual information system plan • Trends in information technology • Planning, development, operations, and maintenance of information systems • Embedded systems • Roles of basic plan, audit purpose, high priority audit theme, and audit target and scope • Management of system audit tasks • Education and training for system audit engineers • Risk analysis and risk-based approach • Information security	• Determining the annual audit purpose (high priority audit theme) in accordance with the business strategy, information strategy, and the documented medium- and long-term plan • Understanding risks related to IT governance to successfully make an audit plan • Selecting the information systems and embedded systems as an audit target to achieve the audit purpose • Analyzing the business operations of the user department • Clarifying the audit schedule for each system and embedded system to be audited, and performing the audit activities according to the schedule

Major category	Minor category	Outline	Required knowledge	Required skills
			• Linkage and alignment with other audits (such as accounting audit and business operations audit) • Engagement of external experts	• Ensuring the linkage and alignment of the audit purpose and schedule with other audits • Engaging external experts • Providing education and training for system audit engineers • Documenting an annual plan based on risk-based approach • Calculating the necessary cost for system audits
	1-3 Preparation of individual documented plans	Based on the documented annual plan, document an individual plan for each system audit which addresses all processes including goal setting (with detailed audit purpose), auditing, audit report, and follow-up. In the individual documented plan, explicitly describe the schedule of each system audit assigned to each of the system audit engineers. In the individual documented plan, include the audit purpose, audit target, audit scope, audit goals, audit procedure, audit term and schedule, the lead auditor and work assignment, the supervisor and staff of the target department, linkage and alignment with other audits, schedule of audit report, audit costs, and so on. In creating the individual documented plan, ensure the effectiveness of the system audit itself, and consider the feasibility and efficiency of the auditing.	• System audit procedure • Formulation of audit purposes and goals • Selection of audit target and scope • Information systems, embedded systems, and communication network (general business management, information strategy, information systems (application system, software package, cloud computing, mobile computing, SNS, IoT, big data, AI, etc.), embedded systems (electrical products, machine and equipment, transportation equipment, etc.), communication network, file system and database, software life cycle model, project management (WBS, EVM, etc.), IT service management (SLA/SLM, intelligent management, etc.), risk management, quality management, information security management and information security related technologies (information security policy, authentication, vulnerability tests, measures against unauthorized access, measures against malware, measures against cyber-attacks, measures against cybercrimes, electronic watermarks, etc.), information security policy, and BCM (Business Continuity Management), BCP (Business Continuity Plan), etc.) • IT governance • IT control • Audit of planning, development, operations,	• Setting the audit goals according to the business strategy, information strategy, and documented annual plan • Selecting audit targets, scope, and procedure required to achieve the audit goals • Understanding the general outline of business operations of the user department • Estimating resources such as staff and costs required for auditing • Engaging external experts • Appropriately distributing tasks among auditors for effective and efficient auditing • Coordinating the audit schedule and procedure with the target department

Major category	Minor category	Outline	Required knowledge	Required skills
			and maintenance activities, audit of business continuity management, audit of system development projects, information security audit, and personal information protection audit (including Social Security and Tax Number) • Laws and regulations on system-related audits (laws and regulations on information security (Criminal Law, Act on the Prohibition of Unauthorized Computer Access, Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers, etc.); laws and regulations on personal information protection; Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures, laws and regulations on intellectual property rights; laws and regulations on labor; laws and regulations on statutory audit (Companies Act, Financial Instruments and Exchange Law, etc.); standards, guidelines, and measures regarding system audits and information security audits; standards, guidelines, and measures of internal audit and internal control; etc.) • Estimation of resources for auditing • Linkage and alignment with other audits (such as accounting audit and business operations audit) • Engagement of external experts	
2 System Auditing	2-1 Preparation for auditing	Perform system audits in the following sequence: preliminary audit, main audit, evaluation, and conclusion. Prior to the preliminary audit, the system auditors review the individual documented plan. They also notify the target department of the individual documented plan and solicit the cooperation of the department.	• Individual documented plan • Procedures for preliminary audit • Engagement of external experts • IT governance • Communication with the target department • Internal organization • Information-communication technologies (information systems (application systems, software packages, cloud computing, mobile computing, SNS, IoT, big data, AI, etc.), embedded systems (electrical products,	• In light of the roles of the target department and the line of command in the organization, appropriately notifying the relevant departments that an audit is to be conducted. • Explaining the background, objectives, scope, evaluation perspectives, and procedure regarding the individual documented plan, to the target department • Conducting an audit without prior notice

Major category	Minor category		Outline	Required knowledge	Required skills
				machines and equipment, transportation equipment, etc.), information equipment (Internet, wired/wireless LAN, servers, tablet terminals, etc.), planning, development, operations, and maintenance of information systems and embedded systems, development methods (agile, etc.), project management (WBS, EVM, etc.), IT service management (SLA/SLM, intelligent management, etc.), IT risk management, system quality management, information security management and information security related technologies (information security policy, authentication, vulnerability tests, measures against unauthorized access, measures against malware, measures against cyber-attacks, measures against cybercrimes, electronic watermarks, etc.), BCM (Business Continuity Management), etc.) • Implementation of concrete audits (audits of planning, development, operations, and maintenance of information systems and embedded systems, audits of system development projects, audits of outsourcing (including BPO), audits of software packages, audits of mobile computing, audits of cloud computing, audits of IoT, audits of big data and AI, audits of smartphones, audits of information security, audits of personal information protection, audits of business continuity plan and management, illegal investigations, CSA (Control Self-Assessments), etc.)	• Understanding risks due to implementation of information-communication technologies and controls required for making a proposal for each risk, and implementing audits • Acquiring knowledge required for specific audits, and implementing audits according to a specific situation
	2-2 Preliminary audit	(1) Collection of relevant material and information (e.g., interview)	Perform the preliminary audit, which is an activity to identify the business operations to be audited, for a smooth and efficient main audit. In the preliminary audit, collect information required to understand the outline of the system and business operations to be audited, the status of controls, and so on. Such information	• Materials related to system development • Materials related to system operations • Materials related to system maintenance • Materials related to IT control and internal control • Materials related to the audited business operations • Business processes	• Collecting information required to understand the outline of the systems, business operations, and controls to be audited • Appropriately requesting and collecting the reference materials from the relevant departments • Interviewing related parties to collect

Major category	Minor category		Outline	Required knowledge	Required skills
			includes related documents and material, data collected through interviews with related parties and field investigations. Also, send and retrieve a questionnaire to an audited department to collect necessary information.	• Application systems • Risk analysis and risk-based approach • Information security • Information collection techniques	necessary information • Collecting information required for risk analysis and control assessment on the information system • Collecting information required for audits by utilizing IT • Utilizing the reference materials regarding IT control and internal control for system audits
		(2) Baseline assessment	Identify the current status of the target system, business operations, and control based on the collected materials, the information collected through interviews with related parties and field investigations, and analysis of the answers to the questionnaire. Next, identify the gap between the current status and the ideal status. The first step to identify the current status is to clarify the target level to be achieved by the organization, for the audit purpose described in the individual audit plan. Also, deal with problems that could not be anticipated when the individual documented plan was created.	• Risk analysis and control assessment based on the reference materials • Statistics • Utilization of information security-related standards and guidelines • Risk analysis and Information security • Control of information systems • Evaluation of information systems (reliability, security, efficiency, effectiveness, confidentiality, integrity, profitability and compliance) • Cyber-attacks, cyber-crimes, illegal behavior, and illegal programs • Digital forensics	• Analyzing the current status and problems based on the collected information • Performing risk analysis on the information system based on the collected information • Identifying the control of the information system based on the collected information • Evaluating the information system based on the collected information • Identifying risks associated with computer crimes and fraudulent conducts based on the collected information • Identifying the current status by applying digital forensic techniques
	2-3 Preparation of statement on auditing procedure		Based on the identified current status, examine specific auditing procedures for the main audit, and prepare the statement on auditing procedure. In the statement on auditing procedure, describe the audit goal, audit technique, time frame, target, scope, auditors, projected working hours, and so on. Also, create it in a format so that the date, signature of auditors, actual working time, reference number of audit working papers can be recorded (this clarifies the processes in the auditing procedure). Moreover, prepare the statement on auditing procedure so that it clarifies the actions of system audit engineers during the system audit (verification process) and may	• General outline of the statement on auditing procedure • Format of the statement on auditing procedure • Selection of audit procedures • System audit techniques • Computer-aided audit techniques (CAAT: data analysis tool, electronic record system, etc.) • Audit evidence • Control of information systems • Risk analysis and risk-based audit approach • Information security • Statistics and sampling • IT control	• Clarifying the audit goals in accordance with the individual documented plan • Selecting a specific audit procedure in accordance with the audit goals • Selecting appropriate audit techniques • Applying computer-aided audit techniques (CAAT: data analysis tool, electronic record system, etc.) to the audit procedure • Applying digital forensic techniques to the audit procedure • Selecting audit techniques required to collect reasonable audit evidence in an efficient manner • Analyzing risks in the information system • Preparing the statement on auditing

Major category	Minor category		Outline	Required knowledge	Required skills
			be available as a reference for future auditing.		procedure based on risk-based approach • Appropriately evaluating the control of information systems • Preparing the statement on auditing procedure using sampling technique • Preparing the statement on auditing procedure by utilizing the materials related to IT control
	2-4 Main audit	(1) Field investigation	Conduct a main audit (auditing procedure) after the statement on auditing procedure is created. A system audit engineer conducts the field investigation by visiting the site to perform on-site examination and evaluation. Although the field investigation is performed in accordance with the statement on auditing procedure, the procedure may be modified according to the actual circumstances in cases where they are different from the assumptions in such statement. In the field investigation, obtain audit evidence which supports the audit opinion.	• Procedures for main audit • Statement on auditing procedure • Audit on installation environment • Control of information systems • System audit techniques (field investigation) • Formulation of audit judgment • Audit evidence	• Obtaining reasonable audit evidence in an efficient manner • Changing the auditing procedure depending on the situation, and selecting a more effective audit technique • Determining the admissibility of audit evidence • Formulating the correct audit judgment based on the audit evidence
		(2) Interview	In accordance with the statement on auditing procedure, perform an interview with the related parties, starting with the target department. Interviewees should include those who need to be questioned for the purpose of the audit. Also, coordinate in advance with the target department regarding the interviewees, time, date, and method so that the auditing does not affect the daily business operations of the department. Moreover, adequately review and arrange the questions in advance to ensure an effective and efficient interview.	• General outline of the main audit • Statement on auditing procedure • Division of job responsibilities • System audit techniques (interview) • Audit evidence • Communication with the target department	• Conducting an interview • Conducting an interview from a fair, unbiased, and objective perspective • Collecting audit evidence through interviews • Understanding the actual business operations performed by the target department • Reconsidering the interviewees and questions based on the actual situation of the target department
		(3) Document review	In accordance with the statement on auditing procedure, obtain and review the documents. In the document review, investigate the approval procedure, how the risk and control are examined, maintained, and implemented, etc. The target of the	• General outline of the main audit • Statement on auditing procedure • Division of job responsibilities • System audit techniques (document review) • Audit evidence • Statistics and sampling	• Understanding the roles and meanings of the documents created during the system planning, development, operations and maintenance • Reviewing the documents from an objective perspective

Major category	Minor category		Outline	Required knowledge	Required skills
			document review (including matching, reconciliation, etc.) should include not only paper-based documents and materials but also electronic data.	• IT control	• Evaluating the importance of the document content in light of the audit goals • Understanding the current status of the business operations and control of the target department through the document review • Reconsider the target documents and review process depending on the situation of the target department • Applying sampling techniques to the document review process • Using the materials regarding IT control in the document review process
		(4) Other system audit techniques	In accordance with the statement on auditing procedure, perform the audit by applying other system audit techniques. More specifically, apply methods such as audit tools and utility software, checklist, or the like. Apply appropriate system audit techniques suitable for particular audit goals and system environment because each system audit technique has its own advantages and disadvantages.	• General outline of the main audit • Statement on auditing procedure • System audit techniques • Engagement of external experts • Audit evidence • Trends in information technology • Statistics and sampling • CAATs (Computer-Aided Audit Techniques) • Digital forensics	• Selecting an appropriate system audit technique suitable for achieving audit goals • Selecting an appropriate system audit technique suitable for the current situation within the target department • Performing the main audit using the computer aided audit techniques (CAAT: data analysis tool, electronic record system, etc.) • Developing and applying effective audit techniques in response to changes in information technology • Applying digital forensic techniques to the main audit • Performing the main audit using statistics and sampling techniques
	2-5 Record of audit results (preparation of audit working papers)		Record the audit results in audit working papers as they are obtained, and confirm the details with the target department as required because the main audit procedure leads to acquisition of audit evidence (formulation of audit judgment). The audit working papers collectively refer to the documents prepared or collected by system audit engineers in the course of the entire	• Individual documented plan and statement on auditing procedure • Audit working papers • Audit evidence	• Describing the findings in the audit working papers from an objective perspective • Preparing audit working papers in light of the process of audit judgment formulation • Preparing audit working papers, which meet the necessary requirements, through the entire audit process • Preparing audit working papers in an

Major category	Minor category	Outline	Required knowledge	Required skills
		system audit processes, classified into documents obtained from the target department and those prepared by system audit engineers. The preparation of the audit working papers are one of the important duties of system audit engineers because it is required to support their audit opinions. In audit working papers, also describe the judgment of the auditors.		efficient manner
	2-6 Clear statement of audit opinion (formulation of audit judgment)	Prepare a draft of the overall evaluation, findings, and recommended improvements based on the audit working papers. Prepare the overall evaluation in line with the audit purpose. Compile the findings in such a way that the recommended improvements are understood correctly. In particular, ensure the appropriateness of the findings by confirming that supporting evidence has been collected and there are no factual errors. Prepare the recommended improvements so that they contribute to the improvement of IT governance, which is the ultimate aim of system audits. Therefore, the recommended improvements must be provided appropriately in line with the audit purpose and from the perspective of IT governance improvement. Also, prepare the draft by reflecting the opinions of the department that implements these improvements regarding the feasibility of the recommendations.	• Individual documented plan and statement on auditing procedure • Audit working papers • Professional ethics of system audit engineers • Formulation of audit judgment • Presentation of audit opinion (assurance opinion and advisory opinion) • Audit report • Evaluation of information systems (including the evaluation of cost-benefit performance) • Risk analysis and risk-based approach • Information security • Related laws and regulations, and guidelines • Communication with the audited departments • Validation of information systems, embedded systems, and communication network	• Presenting audit opinions in an intelligible and concise manner • Performing problem analysis and evaluation based on audit purpose and findings • Grasping and analyzing the current issues and making a recommendation for improving business operations • Communicating with the target departments in an appropriate manner • Investigating feasibility of recommended improvements • Judging appropriateness of the auditing procedure (and judging whether additional audit procedure is necessary or not) in presenting the audit opinion • Validating information systems, embedded systems, and communication network
	2-7 Review of overall evaluation and results	The lead auditor conducts a meeting with system audit engineers to review the evaluation and conclusions from a company-wide viewpoint. In particular, discuss matters, such as findings for which feedback will only be provided on-site and is excluded from the audit report, opinions that differ between the target department and the system auditors, and consistency among system auditors until the system	• IT governance • Business management in general • Information strategy in general • Audit working papers • Audit evidence • Evaluation of information systems • Audit report • Formulation of audit judgment • Presentation of audit opinion (assurance opinion and advisory opinion)	• Reviewing audit findings from a company-wide viewpoint • Evaluating the findings from an objective perspective, and judging the level of importance and urgency from the perspective of top management

Major category	Minor category	Outline	Required knowledge	Required skills
		audit department arrives at a consensus.	• Communication with the target departments • Related laws and regulations, and guidelines	
	2-8 Preparation of a draft audit report	Summarize the audit results in a predetermined format and specify that it is a draft version. Submit the report to the audited department to have them confirm that there are no factual errors.	• Significance of audit report • Format and contents of audit report	• Writing an audit report to present the overall audit results in an intelligible manner • Preparing a concise summary of significant issues for top management • Distinguishing between the findings and opinions
3 System Audit Reporting	3-1 Description of findings	Compile the system audit results into an audit report and submit it to top management. In the report, describe the findings that indicate the problems revealed as a result of the system audit. The description should include explanation of issues (phenomenon), rationale for identifying them as a problem, cause and impact of the problem, and relationship with other findings. When there is more than one finding, describe them in order of priority, which should be judged from the perspectives of management issues, alignment with audit purpose, urgency of the improvement, risk of potential problems, etc.	• IT governance • Business management in general • Information strategy in general • General outline of findings • Items to be included as findings • Audit report • Audit evidence • Audit working papers • Related laws and regulations, and guidelines	• Judging the significance of the audit findings from a management perspective • Judging the significance of the findings in an objective and rational manner • Presenting the findings in a plain, concise, and clear manner • Distinguishing between the findings and opinions • Identifying problems in light of related laws and regulations, and guidelines
	3-2 Description of recommended improvements	Include recommended improvements in the audit report. Describe the necessary actions to improve the findings. Based on significance and urgency, divide the recommended improvements into two sections – urgent improvement actions and general improvement actions. The urgent improvement actions include a problem causing a severe system defect that cannot be ignored. The general improvement actions include problems which do not cause a severe system defect but resolution of which may contribute to system enhancement. In the recommended improvements, also include implementation plans, the department that implements the	• IT governance • Business management in general • Information strategy in general • General outline of recommended improvements • Items to be included as recommended improvements • Business processes • Application systems • Trends in information technology • Risk analysis and control evaluation • IT control • Information security • Audit report • Presentation of audit opinion (assurance opinion and advisory opinion)	• Prioritizing recommended improvements from the perspective of business risk • Evaluating risk and control, prioritizing between urgent and general improvements, and identifying their urgency • Examining feasibility of the recommended improvements in economic and technical terms • Comparing multiple recommended improvements • Proposing recommended improvements using techniques such as benchmarking • Providing more specific and detailed recommendations in light of business processes

Major category	Minor category	Outline	Required knowledge	Required skills
		actions, and consistency with other recommended improvements. The recommended improvements are described in the audit report. When there is more than one recommendation per finding, sort them in order of priority of the corresponding management issues. Describe the recommendations as specifically and in as much detail as possible. Moreover, exchange opinions with the department that implements the improvement actions to examine the feasibility of those recommendations. Develop the recommended improvements from the perspectives not only of technologies but also of business management, IT governance, and business processes.		• Proposing effective and efficient recommendations from a comprehensive viewpoint including other recommended improvements
	3-3 Description of supplementary note	Include any supplementary notes regarding the system audit results in the audit report. For example, include items that do not fall into any of the overall evaluation, findings, and recommended improvements, supplementary materials required for top management to fully understand the audit results, information required to determine the current status or to improve the system, and so on.	• Overall evaluation • Findings • Recommended improvements • Communication with top management • Communication with the target departments • Presentation of audit opinion (assurance opinion and advisory opinion)	• Preparing materials required for the related parties to understand the overall evaluation, findings, and recommended improvements
	3-4 Submission of audit report	Prepare the audit report as soon as the system audit is completed, and submit it to top management. The audit report is a report created in accordance with the individual documented plan. A copy of the audit report should also be distributed to related parties (the department audited and the department that implements the improvements). Submit the audit report by the deadline specified in the individual documented plan. However, in urgent cases, report it in an oral presentation, and submit the report at a later date.	• IT governance • Business management in general • Destinations and submission schedule of audit report • The relationship between submission/distribution of the system audit report and implementation of the improvements	• Understanding the submission schedule and destinations of the system audit report from the perspective of business management • Submitting the audit report to top management and related parties in an appropriate manner
	3-5 Post-audit meeting	Hold a post-audit meeting with all related	• IT governance	• Identifying the appropriate departments

Major category	Minor category	Outline	Required knowledge	Required skills
		parties including top management, the departments audited, and the departments that implement the improvements so that they can recognize the significance and urgency of the recommended improvements and understand them correctly. In the meeting, negotiate the schedule for improvement actions, and decide on who are to be the persons in charge, in order to reach agreement among all parties.	• Business management in general • Information strategy in general • Organization structure of information systems • Overall evaluation, findings, and recommended improvements • Significance of system audit report • Format and description of a system audit report • Laws and regulations, and guidelines on system audits	involved in the post-audit meeting • Negotiating improvement plans with related departments • Appropriately explaining the overall evaluation, findings, and recommended improvements • Explaining the audit report in light of the laws and regulations, and guidelines on system audits
	3-6 Follow-up activities	Perform follow-up activities after the audit is completed in order to make the audit contribute to maintaining and enhancing reliability, security, efficiency, and usability of information systems through improvement of the problems found in the audit (implementation of the recommended improvements). More particularly, support the management of the company and department in charge of the implementation so that they can carry out the improvement activities smoothly. Also, follow up the audited department with regard to planning and implementation of the recommendation. When multiple departments are involved in the implementation, follow up to ensure the uniformity and consistency of the improvement activities, examine the validity of improvement results, and so on. Follow-up methods include post-audit meetings, documents, such as implementation plans and improvement reports that describe the implementation status, and reviews in the next scheduled system audit.	• IT governance • Business management in general • Information strategy in general • Overall evaluation, findings, and recommended improvements • General outline of follow-up activities • Follow-up methods	• Identifying the appropriate departments involved in improvement activities • Identifying the progress of improvement activities • Evaluating improvement results from a business management perspective • Providing follow-up on inappropriate improvement activities as required • Developing an individual documented plan for the next scheduled audit based on the current audit results
	3-7 Preparation of annual audit report	Prepare an annual audit report showing the results of audits performed during the year in accordance with the documented annual plan. The annual audit report describes activities of the system audit department	• IT governance • Business management in general • Information strategy in general • Documented annual plan • General outline of annual audit report	• Preparing a report in light of the documented annual plan so that top management can easily understand the activities of the system audit department • Identifying the status of the information

Major category	Minor category	Outline	Required knowledge	Required skills
		during the year and is provided to top management. In the annual audit report, describe the results of the activities planed in the documented annual plan, including the progress of system audit tasks, special notes regarding important findings and their improvement status, change in number of system audit engineers, education and training for system audit engineers, and issues to be addressed in the next year's documented annual plan.	• Format of annual audit report • Trends in information technology • Organization structure of information systems • Evaluation of information systems • Risk analysis and risk-based approach • Information security • Education and training for system audit engineers • Management of system audit tasks • Quality management of system audit • Improvement of system audit tasks	system from perspectives of planning, development, operations, and maintenance of such systems • Reflecting the audit results of the current year in the following year's documented annual plan and documented medium- and long-term plan • Prioritizing the audit results during the year from the perspective of business issues and audit purposes • Managing the system audit department or the system audit team • Identifying the issues to be followed up in the following year's audit, and reflecting such issues in the documented basic plan of the following year
4 Management of System Audit Tasks	4-1 Progress management	Manage the progress of the audit process so that the activities described in the documented annual plan, individual documented plan, and statement on auditing procedure can be performed smoothly and steadily. In the progress management, review the progress of the audit schedule, expected completion time, audit team organization (auditors and their duties), and so on.	• Documented annual plan • Individual documented plan • Statement on auditing procedure • Management of system audit project • Analysis of system audit work • System audit procedure	• Understanding the documented annual plan, and performing the audit tasks according to the plan • Understanding the individual documented plan, and performing the audit tasks according to the plan • Understanding the statement on auditing procedure, and performing the audit process according to the procedure • Determining the importance and urgency of significant findings from the perspective of top management • Reviewing and revising the individual documented plan and the statement on auditing procedure • Providing education and training for system audit engineers
	4-2 Quality management	Review the statement on individual documented plan, auditing procedure, audit working papers, and audit reports to improve the quality of system audit. For the statement on auditing procedure, review whether it complies with the individual documented plan, whether it employs an	• Evaluation points for system audit tasks • Quality management techniques • Quality evaluation of audit process (internal evaluation and external evaluation) • Auditing procedure • Risk-based audit approach • Risk analysis and control evaluation	• Evaluating appropriateness of the auditing procedure • Evaluating efficiency of the audit tasks • Reviewing the audit tasks to check if they are performed in accordance with the individual documented plan and the statement on auditing procedure

Major category	Minor category	Outline	Required knowledge	Required skills
		effective and efficient audit procedure for achieving the audit purpose, etc. For audit working papers, review them from the perspectives of their compliance with the individual documented plan and statement on auditing procedure, accuracy required for audit working papers, appropriateness of the opinion writing process, necessity and sufficiency of the audit evidence, consistency between the opinions of auditors, relevance of the overall evaluation to the audit purpose, accuracy of findings, validity of recommended improvements, and so on.	• Individual documented plan • Statement on auditing procedure • Record of audit results (preparation of audit working papers) • Formulation of audit judgment • Presentation of audit opinion (assurance opinion and advisory opinion) • Application of system audit techniques • Overall review • Findings • Recommended improvements • Follow-up actions • IT control • Computer-aided audit techniques (CAAT: data analysis tool, electronic record system, etc.)	• Reviewing the audit working papers to check if it is created in an appropriate manner • Reviewing the audit evidence to check if it is collected in an appropriate manner • Evaluating the admissibility of audit evidence • Reviewing the validity and effectiveness of the overall evaluation, findings, and recommended improvements from a top management perspective • Reviewing the feasibility of recommended improvements • Organizing, storing, and utilizing the documented audit plan, audit report, and audit working paper in an efficient manner • Understanding and implementing the issues to be addressed in the next scheduled system audit
	4-3 Improvement of audit tasks	Aggregate the actual performance data obtained through the system audit tasks to compare it with the planned data, and analyze the cause of any discrepancies. Also, identify the aspects to be refined in the individual documented plan and the statement on auditing procedure, and evaluate the effectiveness and efficiency of the system audit techniques. Based on these results, enhance the system audit tasks.	• Analysis of system audit tasks (including audit procedures) • Trends of system audits • Information collection techniques • Trends in information technology • System audit techniques • Computer-aided audit techniques (CAAT: data analysis tool, electronic record system, etc.) • Business processes (improve the business process for higher efficiency) • Application systems (improve the audit tasks using application system functions)	• Analyzing the system audit tasks • Accurately identifying the trends of information technology • Accurately identifying the trends of system audits • Adopting and utilizing computer-aided audit techniques (CAAT: data analysis tool, electronic record system, etc.) • Adopting and utilizing appropriate audit techniques • Improving the audit tasks from the perspective of the business process • Improving the audit tasks using IT • Improving the efficiency of the audit tasks
	4-4 Enhancement of audit framework	In order to achieve successful system audit outcomes, improvements in skills, knowledge, and experience of system audit engineers are essential. The manager of the system audit department should provide medium- and long-term plans for the	• Corporate governance • IT governance • IT control and internal control • Plans and methods of education and training for system audit engineers • Quality control of system audit operations	• Preparing the audit framework in light of corporate governance, IT governance, internal control, and IT control • Making top management and related parties understand corporate governance, IT governance, internal control, and IT

Major category	Minor category	Outline	Required knowledge	Required skills
		education and training of system audit engineers. He also needs to arrange such education and training based on engineers' job assignment.	• Job rotation • OJT (On-the-Job Training) • Engagement of external experts	control • Developing plans of education and training for system audit engineers in response to their educational needs

■ Systems Auditor Examination (Level 4)
Syllabus (Version 3.1)

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/

2016-09