

Appendix 1 Correspondence of the “System Management Standards – Supplementary Edition” to other standards

Figure 1-1 shows representative IT control frameworks.

Fig. 1-1 Representative IT control frameworks

Representative framework	Establisher	Scope of each framework
System Management Standards	Ministry of Economy, Trade and Industry	IT control in general
COBIT (4th edition)	IT Governance Institute	
IT control objectives for observance of the Sarbanes-Oxley Act (2nd edition)	IT Governance Institute	IT control over financial reporting
Report No. 3 released by the IT Committee	Japanese Institute of Certified Public Accountants	
Information Security Management Standard	Ministry of Economy, Trade and Industry	IT security control
JIS Q 27002	Japanese Industrial Standard	
ISO/IEC 20000:2005 Information technology - Service management	ISO/IEC	IT operation control
ITIL (Information Technology Infrastructure Library)	Office of Government Commerce	

Agreement is not necessarily reached as to whether all these frameworks can be used as “IT control standards generally acknowledged as fair and appropriate” to appraise and audit the status of internal control over financial reporting. For example, some frameworks contain items that this system does not require or are biased towards a certain area of activities. In addition, overseas frameworks are formulated based on the business practices of Western countries, and there are cases in which it is difficult to apply these frameworks to Japanese companies because the internal control systems of Japanese companies function based on not only common business operation concepts but also some non-Western concepts particular to Japan.

Figure 1-2 shows a comparison of three frameworks: (1) System Management Standards - Supplementary Edition (Guidance for IT controls over financial reporting) (hereafter called the “Supplementary Edition”); (2) IT control objectives for observance of the Sarbanes-Oxley Act 2nd edition, September 2006 (hereafter called “IT Control Objectives V2”); and (3) the 3rd report of the IT Committee (“Assessment of important misstatement risks in the information system using IT during the audit of financial statements, and the auditor procedure for dealing with the evaluated risks,” which was revised on March 17, 2006) (hereafter called the “3rd IT report”).

Fig. 1-2 Comparison between the Supplementary Edition and other standards

Standard name Components	3rd IT report	IT control objectives V2	Supplementary Edition (Guidance for IT controls over financial reporting)
Introduction	I. Purpose of this report	1. Executive summary	Introduction
Basics of control over financial reporting	III. Understanding a company with internal control in place and its business environment 1. Information reliability and IT 2. Relationships between executive assertions and IT control objectives 5. Understanding the control environment	2. Foundation for reliable financial reporting • Need for IT control guidance 3. Manage the human element of change • Committing to change • Assessing the current state	II. Overview of IT controls 1. Financial reporting and IT controls (1) Relations between internal control provided by the Financial Instruments and Exchange Law and IT (2) Relations between financial reporting and IT controls
Outline of IT control (classification of controls)	II. General understanding of IT III. Understanding a company with internal control in place and its business environment 3. Relationships among each operation process and IT 4. Understanding the relationships among account titles in financial statements, operation processes, and application systems 6. Understanding the information systems for which financial reports are prepared and the transmission of information 7. Understanding control	2. Foundation for reliable financial reporting • Where to find IT controls • Information technology controls - a unique challenge • PCAOB guidance for IT controls • Controls over IT systems 4. Setting the ground rules • COSO defined • Applying COSO to IT	II.2. Control items in IT controls (1) Company-level IT controls (2) IT general controls (3) IT application controls

	activities 8. Understanding monitoring activities		
Control frame and control objectives	Data from outside sources (report Nos. 29, 30, and 31 by the Watchdog Committee)	Appendix B: COSO and COBIT Appendix C: IT general controls • Activity-level IT controls Appendix D: Application controls • The importance of application controls • The business case for application controls • Defining application controls • Establishing the application benchmark • Examples of automated application controls	Appendix 2. Usage of control objectives for the System Management Standards
Control activities (control and assessment procedures)	IV. Assessment of important misstatement risks 1. Judgment of importance of risk assessment of information systems 2. Points to consider if a shortcoming is found with overall controls 3. Points to consider if a shortcoming is found with operation controls 4. Correction of risk assessments V. Communication between executives and auditors	5. IT compliance road map • Sarbanes-Oxley compliance	III. Assessment of IT controls by management 1. Roadmap for assessment of IT controls 2. Determination of the scope of assessment and identification of IT to be assessed 3. Assessment of company-level IT controls 4. Assessment of IT controls in business processes

	<p>VI. Performing the procedure for dealing with evaluated risks</p> <p>VIII. Using IT specialists</p> <p>IX. Defining the relative position of outsourcing</p>		<p>5. Determination of effectiveness of IT controls</p>
<p>Cases and others</p>	<p>VII. Examples of IT-related audit procedures</p> <ol style="list-style-type: none"> 1. Perusal of records and documents 2. Visiting and observing a site where a system is operated 3. Questions 4. Recalculation/CAAT 5. Reimplementation/CAAT 6. Analytical procedure <p>X. Issue and application</p>	<p>Appendix A: Sarbanes-Oxley primer</p> <p>Appendix E: Sample application and technology layer inventory</p> <p>Appendix G: Inherent risk assessment and control prioritization grid</p> <ul style="list-style-type: none"> • Risk assessment considerations • Information technology risk assessment • <p>Recommendations on where controls should be considered</p> <p>Appendix H: Sample control documentation and testing template</p> <p>Appendix I: Sample deficiency evaluation decision tree</p> <p>Appendix J: Sample approach for spreadsheets</p> <p>Appendix K: Lessons learned</p> <p>Appendix L: Issues in using SAS70 examination report</p> <ul style="list-style-type: none"> • Description of 	<p>IV. Guidance on Introduction of IT Controls (Illustration of IT Controls)</p> <ol style="list-style-type: none"> 1. Use of the guidance 2. Company-level IT controls 3. IT General Controls 4. IT Application controls 5. Monitoring <p>Appendix 1. Correspondence of the “System Management Standards – Supplementary Edition” with other standards</p> <p>Appendix 2. Usage of control objectives for the System Management Standards</p> <p>Appendix 3. Illustration of IT controls and specific information technologies (IT)</p> <p>Appendix 4. Recording and retention of assessment procedures</p> <p>Appendix 5. Sampling</p> <p>Appendix 6.</p>

		controls •Timing •Nature and extent of testing •Qualifications and exceptions •Service auditor Appendix M: Segregation of duties in significant accounting applications Appendix N: List of figures	Examples of the risk control matrix 6-1. Description of IT General Controls Assessment 6-2. Description of Company-level IT Controls Assessment 6.3 Description of IT Application Controls Assessment
--	--	---	--

The “3rd IT Report” is compiled with a focus on the concepts and procedures for the risk assessment of internal controls using IT to be reviewed during accounting audits conducted by auditors. It is suitable for use by internal auditors or accounting auditors as a handbook of audit activities.

The IT control objectives were established based on the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework, and disseminated mainly in the U.S.A. After two years of application, they were reviewed and established as the “IT Control Objectives V2.” This V2 edition is different from the first edition in that one whole chapter is used as an executive summary to provide executives with guidance and promote their understanding, and many assessment criteria and templates are provided as reference data to allow the materials to be used for a wide range of purposes. It is organized in a way that enables people concerned with internal controls to use it as a handbook for acquiring information on the specific tasks that they perform.

While the “Supplementary Edition” is compiled from the perspective of the IT side, the “IT Control Objectives V2” is based on the standpoint of controlling the status of IT controls. It is expected, therefore, that people concerned with IT controls will be able to gain a better understanding of IT controls by referring to both the “Supplementary Edition” and “IT Control Objectives V2” in a complementary manner. Additionally, if the viability of applying the performance standard of the Financial Services Agency to overseas operating bases of Japanese companies (particularly those in the U.S.A.) is uncertain, it could be useful to refer to the “IT Control Objectives V2.”

Appendix 2 How to use the control objectives of System Management Standards

1. Control objectives of System Management Standards

System Management Standards are designed to be used by an organization that wants to establish IT governance by dealing with the risks accompanying its information system, specifically by exercising control over its information system and making it function properly in a cycle comprising planning, development, operation, and maintenance. Although System Management Standards are designed to be used by information system operators, system auditors can also use them as criteria for judgment when conducting system audits.

⇒ (Preface, System Management Standards)

2. Organizing the control items of System Management Standards

To make it easier for a company to use System Management Standards when improving or evaluating IT controls concerning the reliability of financial reporting, all control items of System Management Standards have been organized and tabulated as shown in the pages that follow. The information given below corresponds to the information shown from left to right in the table.

- Control items are arranged in the order of chapter, section, and items that appear in System Management Standards.

- * Types of control of each control item (company-level IT control, IT general control, and IT application control) are classified into company, general, application or – (not applicable).

- Control objectives are shown for each control item.

- For each control item, “C” or “S” is shown. “C” means a control item that constitutes a greater risk to financial information, and “S” means a control item that constitutes a relatively small risk to financial information. For a control item that does not directly concern internal controls over financial reporting, the space is left blank and neither “C” nor “S” is entered.

- The purposes of each control item (abstracted from the purposes described in the handbook of System Management Standards) are shown.

3. Control objectives of System Management Standards (examples)

The control objectives (examples) of System Management Standards shall be used as follows:

- ① To understand the control items and purposes of each control item
- ② To understand the risks of control items shown in the guidance by clarifying corresponding control items (examples)
- ③ If you want to reduce a certain risk, the risk can be defined as a control item.
- ④ To enable a company to make up a list of control items (examples) and thereby recognize that the risks involved can be reduced (use of risk control matrix, etc.)

How the control objectives of System Management Standards are used varies greatly depending on the company and type of industry. Therefore, the control items (examples) of System Management Standards shall be applied by taking the actual situation of each company into consideration.

Appendix 2-1

Control items of System Management Standards, and corresponding control objectives (examples)

Item number	Control items of System Management Standards	Control type	Control objective (example)	Guidance item number	C or S	Purpose of the System Management Standards
I	Strategic IT Plan					
1	Overall optimization					
1.1	Policies on and goals of overall optimization	Company				
(1)	Define policies on IT governance.	Company	Formulating the IT governance policy (plan).	2-(1)-①	C	The policy for the establishment of IT governance must be clarified.
(2)	Define principles for use of IT and IT investment allocation.	Company	Establishing a computerization plan appropriate for management strategy.	2-(1)-①	C	The principles on which investments in computerization and computerization plans are to be determined must be established in order to formulate a coherent overall optimization plan.
(3)	The goals of the information system's overall optimization should be based on business strategies.	Company	Making the information system optimization plan consistent with management strategy.		S	To construct an information system that will enable business objectives to be accomplished, the objectives of the overall optimization plan must be established with consideration given to consistency with management strategy.
(4)	Define the model of the	Company	Formulating the overall	2-(1)-①	C	The overall optimization plan

	information system for the organization.		optimization plan.			must clearly present an ideal information system so that the information system for the whole organization functions to accomplish objectives efficiently and effectively in such a way that individual information systems interact with each other organically while consistency is mutually maintained.
(5)	Define policies on organizational structure and business process changes caused by introducing the new system.	Company	The overall optimization plan shows an organization to be systematized and changes in operations.	2-(3)-①	C	As the information system is constructed (rebuilt), new organizations and operations will be established, and existing organizations and operations will be altered or abolished. The overall optimization plan must clarify the policies for establishing new organizations and operations and for altering and abolishing existing organizations and operations.
(6)	Define primary policies on information security.	Company/ general	Making the overall optimization plan consistent with the basic information security policy.	2-(1)-⑤ 2-(3)-① 3-(3)-①-A	C	Prevention of fraud, security, protection of privacy, etc., is the basis on which sound business management activities can be promoted. Therefore, the policy for information security

						measures must be clearly presented in the overall optimization plan.
1.2	Approval of the overall optimization plan	Company				
(1)	Obtain approval on the organizational structure to develop the overall optimization plan from the management.	Company	The overall optimization plan must be approved by the top management.		S	Because the overall optimization plan must be formulated based on management strategies as medium- and long-term plans, a planning system must be established and the overall optimization plan created through this planning system must be approved by the top management of an organization.
(2)	Obtain approval on the overall optimization plan from the management.	Company	The overall optimization plan must be approved by the top management.		S	Computerization must be promoted based on management strategy by maintaining consistency throughout an organization. Therefore, the overall optimization plan must be approved by the top management of an organization.

(3)	Obtain agreement of related stakeholders on the overall optimization plan.	Company	Making the overall optimization plan well and widely known to the people concerned both in and outside an organization.		S	Agreement of the stakeholders must be obtained to allow the overall optimization plan to be implemented smoothly.
1.3	Development of the overall optimization plan	Company				
(1)	Create the overall optimization plan based on policies and goals of the plan.	Company	Formulating the overall optimization plan.	2-(1)-①	C	The overall optimization plan must be formulated based on policies and objectives so that computerization will be promoted throughout an organization in a consistent manner based on management strategy.
(2)	Consider compliance requirements in the development of the overall optimization plan.	Company	Making the overall optimization plan consistent with the compliance policy of a company.		S	To avoid violating related laws and regulations, voluntary standards of industry, etc., the overall optimization plan must be prepared with consideration given to compliance.
(3)	The entire optimization plan should define policies on IT investments and necessary resources.	Company	Acquiring the resources needed to implement the overall optimization plan.		S	To increase the cost effectiveness of investments in computerization, the policy for investments in computerization and the resources to be acquired must be clarified in the overall

						optimization plan.
(4)	Define how to measure the return and risks of IT investments in the overall optimization plan.	Company	Calculating the returns on investments made and the risks involved in the overall optimization plan.		S	To clarify the criteria for judging whether a plan should be adopted or modified, how to estimate returns on investments made and the risks involved must be presented in the overall optimization plan.
(5)	Define rules for standardization and quality management policies for system development and operations in the entire optimization plan.	Company	Including the standardization for system construction and the quality policies of a company in the overall optimization plan.		S	To maintain consistency between information systems in an organization and to construct and operate a system efficiently while maintaining high, homogeneous quality, the standardization and quality policies for system construction and management must be defined.
(6)	Define rules to specify the priority of each development plan in the overall optimization plan.	Company	Considering the importance and urgency of challenges in business management in the overall optimization plan.		S	To reflect the importance and urgency of challenges in business management and to use development resources effectively, the order of priority and the rules for prioritization must be defined in the overall optimization plan.
(7)	Consider the use of external resources in the entire optimization plan.	Company	Considering the utilization of resources in the overall		S	To remove resource-related restraints, the use of not only the resources inside an organization

			optimization plan.			but also external resources must be considered in the overall optimization plan.
1.4	Implementation of the overall optimization plan	Company				
(1)	Ensure that every stakeholder knows about the overall optimization plan.	Company	Making the overall optimization plan well and widely known and promoting a better understanding of it.	2-(1)-①	C	The overall optimization plan must be made fully understood by all stakeholders to allow it to be implemented efficiently and smoothly.
(2)	Review the overall optimization plan periodically and when changes occur in the business environment.	Company	Maintaining and controlling the overall optimization plan.		S	To prevent the overall optimization plan from losing flexibility or becoming outdated, it must be reviewed periodically to make it fit the changing business environment.
2	Organizational					
2.1	Computerization Committee	Company				
(1)	Clarify missions of the committee and allocate appropriate authorities and responsibilities to the committee based on the overall optimization plan.	Company	Organizing the computerization committee to realize overall optimization.	2-(1)-②	C	To optimize the whole of an information system based on management strategy, the top management (executive machine) must establish a computerization committee to implement information strategies, and define the tasks,

						authority, and responsibilities of this committee.
(2)	The committee should monitor all the activities concerning the information systems in the organization and implement necessary corrective measures.	Company	The computerization committee conducts appropriate supervising activities.	5-(2)-①	C	To plan, develop, operate, and maintain an information system based on the overall optimization plan, the computerization committee has the function and responsibility to supervise all information-related activities conducted in a company, and must take appropriate remedial actions if improper conditions are noted.
(3)	The committee should adopt the technology guidelines to stay current with trends in information technologies.	Company	Establishing a reasonable standard based on which an information technology infrastructure is to be introduced.		S	To cope with changing trends in information technology quickly and properly, a consistent information technology infrastructure functioning in a consistent, seamless manner throughout an organization must be established, thereby reducing the risks involved. The computerization committee must define the guideline for the introduction of technologies.
(4)	The committee should report its activities to the management.	Company	The computerization committee contributes to the decision-making of business management		S	To contribute to the decision-making of business management operations, the computerization committee must report the

			operations.			contents of its activities to the top management of an organization at the appropriate times.
(5)	The committee should provide to the management the information necessary for strategic decision support.	Company	The computerization committee reflects important matters related to the overall optimization plan and information system in the management policies of a company.		S	The computerization committee must provide the top management of an organization with information to support them in making decisions so that a change in the environment affecting the overall optimization plan, technical trends, and conditions of ongoing development, operation, and maintenance activities can be addressed properly and quickly in management policies.
2.2	Information System Department	Company				
(1)	Clarify the missions of the information system department and allocate appropriate authority and responsibilities to the department.	Company	Defining the roles and functions of the information system department, and assigning it appropriate authority and responsibility.	2-(1)-③	C	For information system functions to be performed at the appropriate times, the top management of an organization must define the roles and functions of the information system department, and assign it appropriate authority and

						responsibility.
(2)	The information system department should consider reforming the organizational structure with separation of duty, specialization, authorization and outsourcing, based on the size and characteristics of the organization.	Company	The information system department shall be so organized as to enable it to implement the overall optimization plan appropriately.	2-(1)-㉓	C	To implement the overall optimization plan effectively and efficiently, the information system department must use not only resources inside a company but also external resources in an appropriate manner, while considering an organization's need for computerization and the effect of investment.
2.3	Human Resource Management polices	Company				
(1)	Identify the current status of human resources for IT and clarify the necessary human resources.	Company	An organization shall acquire the human resources needed to achieve overall optimization.		S	To allow an organization to accomplish overall optimization objectives, it is necessary to grasp the present situation of human resources related to information technology inside an organization and to clarify the human resources and capabilities that are needed in an organization.
(2)	Clarify policies on sourcing and training of human resources.	Company	An organization shall acquire the human resources for overall optimization.		S	A future plan and the policies for the introduction and cultivation of human resources must be documented by taking note of the present situation of

						human resources needed to computerize an organization, and the documented policies must be fully understood throughout the company.
3	IT Investments					
(1)	Ensure that the IT investment plan is created in a manner consistent with corporate strategies.	–	Utilizing IT investments to meet challenges in business management.			To utilize IT investments to solve the problems of business management, a computerization investment plan consistent with management strategy must be formulated from the standpoint of benefits to be brought to business management, improvements to be made to operation procedures, and other factors related to overall optimization.
(2)	Compare multiple IT investment plan alternatives based on impact, effects, schedule and feasibility.	–	Determining an IT investment plan through the agreement of the stakeholders.			To determine an IT investment plan through the agreement of the (people) stakeholders, multiple choices must be presented and studied by considering effects, periods, feasibility, etc., and the most appropriate plan must be selected.
(3)	Execute IT investment	–	Implementing the IT			To implement an IT investment

	budgets properly.		investment plan.			plan properly, budgets must be executed in appropriate amounts through appropriate contracts at appropriate times.
(4)	Establish the standard methodology for estimating the return on IT investments.	–	Evaluating the effects of IT investments objectively, and reflecting the evaluation results in a future IT investment plan.			To evaluate the effects of IT investments objectively and to reflect the evaluation results in a future IT investment plan, it is necessary to define a method of calculating the return on investments.
(5)	Assess financial performance of the entire information system and individual projects, and take the necessary actions to solve any problems.	–	Detecting financial problems in the overall achievements of an information system and the achievements of individual projects as early as possible, and taking appropriate countermeasures.			To detect financial problems in the overall results of an information system and the results of individual projects as early as possible and take appropriate corrective measures, it is necessary to conduct monitoring activities from a financial standpoint. To deal with the types of financial problems that are expected to occur, procedures for dealing with them must be established beforehand.
(6)	Review whether IT investments have been properly executed or not.	–	Making IT investments as planned, and making adjustments if there is a divergence from the			IT investments must be made as planned, and appropriate adjustments must be made if there is a divergence from the IT

			plan.			investment plan. To achieve this, it is necessary to grasp all related data, including the amount invested, for what purposes investments are made, etc.
4	Policies on Information Asset Management	Company				
(1)	Define policies of information asset management and establish appropriate organizations.	Company	Managing information assets - one important business management asset - properly, and using them effectively.	2-(3)-②	C	To manage information assets properly, which are important assets for business management, and to use them effectively, an information assets management policy and information assets system must be established.
(2)	Assess risks for information assets, and take appropriate measures to reduce those risks.	Company	Maintaining the reliability and safety of information assets.	2-(2)-①	C	To maintain the reliability and safety of information assets, apparent and potential risks of information assets must be identified, the level of each risk must be determined, and measures to deal with each risk must be taken.
(3)	Consider efficient and effective use of information assets.	Company	Achieving the objectives specified in management and information strategies.		S	To achieve the objectives specified in management and information strategies, information assets must be used efficiently and effectively, based

						on the IT investment policy.
(4)	Consider productivity improvement through information asset sharing.	–	Achieving the objectives specified in management and information strategies.			To achieve the objectives specified in management and information strategies, productivity must be improved through sharing of information assets.
5	Business Continuity Plan					
(1)	Establish policies for ensuring the business continuity of the information system.	–	Securing the business continuity of an organization.			To secure the business continuity of an organization, a business continuity policy related to an information system must be established.
(2)	Establish the business continuity plan by all stakeholders, and obtain the approval of the head of the organization for the plan.	–	Establishing preparedness so that all people concerned can perform the given functions if an incident affecting the business continuity occurs.			A highly viable business continuity plan must be prepared in an organization, in which stakeholders are included, and the top management of an organization must approve the plan, so that all stakeholders are able to deal smoothly with an incident affecting business continuity.
(3)	Ensure that policies for the business continuity plan include employee training.	–	Performing procedures specified in the business continuity plan quickly and properly when a threat to business			The policy for personnel education and training must be presented in the business continuity plan to enable them to perform the procedures

			continuity occurs.			specified in the business continuity plan quickly and properly if a threat to the continuity of business occurs.
(4)	Ensure that all necessary personnel in the relevant departments are reformed of the business continuity plan.	–	Increasing the viability of the business continuity plan.			To increase the viability of the business continuity plan, the plan must be fully understood by the people concerned.
(5)	Review the business continuity plan as and when necessary.	–	Maintaining the effectiveness of the business continuity plan.			To maintain the effectiveness of the business continuity plan, the plan must be reviewed and updated as necessary.
6	Compliance					
(1)	Establish an organization for legal and regulatory compliance and appoint management for it.	–	Observing and managing laws and regulations properly.			To observe laws and regulations and manage their application, a department responsible for the management of laws and regulations must be established in an organization, and a laws and regulations management system must also be established.
(2)	Identify laws and regulations applicable to the organization, and inform and educate stakeholders.	–	Identifying and specifying the laws and regulations that must be observed in an organization.			To observe laws and regulations and manage their proper application, laws and regulations to be observed in an organization must be identified and specified. A training system

						must then be established to enable the people concerned to have a good understanding of the identified laws and regulations.
(3)	Define the information ethics, and inform and educate related persons.	–	Observing and managing laws and regulations properly as an organization.			To allow laws and regulations to be observed and managed properly in an organization, an ethical code for information security must be established as the rules to be observed in an organization, and the people concerned inside and outside an organization must be oriented and educated to allow them to have a good understanding of the ethical code.
(4)	Establish policies regarding processing of personal information, protection of intellectual property rights and for the provision of information disclosure.	–	Establishing policy that clearly shows the organizational philosophy.			For personnel to observe laws and regulations, an organization must establish its policies for the handling of personal information, protection of intellectual property rights, provision of data to the outside world, etc., from the standpoint of protection of various rights in and outside an organization.
(5)	Assess level of compliance with laws,	–	Checking and evaluating the status of			To observe and manage laws and regulations properly, the

	regulations, and the information ethics, and take necessary actions for improvement.		observance in an organization periodically, and improving the shortcomings that are pointed out.			status of observance of identified laws and regulations and that of observance of the ethical code for information security, which are established as internal rules, must be evaluated periodically, and measures necessary to improve the shortcomings found must be implemented.
II	Planning processes					
1	Development Plans	General				
(1)	Obtain approval for the development plan from the management.	General	Making a decision to put the development plan of an organization into practice.		S	To confirm that the development plan is based on the overall optimization plan and implement the development plan, it is necessary for the top management of an organization to approve the development plan.
(2)	Establish the development plan considering its consistency with the overall optimization plan.	General	The information system to be developed shall have the maximum possible beneficial effect on an organization.		S	The information system to be developed and other information systems must together perform the assigned functions through the division of roles to allow an organization to deliver its best performance. To achieve this,

						the development plan must be formulated with consideration given to consistency with the overall optimization plan.
(3)	Define the development plan to specify its objective, target process, cost, system development structure and cost efficiency for investment.	General	The people concerned shall share a common understanding of the purposes, functions, etc., of an information system, and confirm the returns on investments made in an information system.		S	To allow the people concerned to have a common understanding of the purposes, functions, etc., of an information system and to verify the returns on investments made in an information system, the development plan must describe purposes, operations to be performed, costs, schedule, development system, returns on investments, etc.
(4)	Define the development plan to include education and training programs for stakeholders.	General	Maintaining the quality of an information system, and achieving the goals of an information system as scheduled.		S	To maintain the quality of an information system specified in the development plan and construct this information system as scheduled, the people concerned with development must be guided to have a common understanding of the contents of the development plan, and an education and training plan must be established to improve technical

						competence.
(5)	Define the development plan to specify the roles of the user department and of the information system development department.	General	Performing development, operation, and maintenance tasks effectively.		S	To allow development, operation, and maintenance work to be performed effectively, the division of roles between the user department and the information system department must be clarified and mutually confirmed by both departments.
(6)	Define the development plan to indicate the cost calculation methodology for system development, operation and maintenance.	General	Calculating the costs of an information system during its life cycle reasonably.		S	To calculate the costs of an information system during its life cycle reasonably, the development plan must clarify the grounds for calculating development, operation, and maintenance costs.
(7)	Define the development plan to specify conditions for defining system life cycle.	General	Estimating the life of an information system reasonably.		S	To estimate the system life of an information system reasonably, the system life conditions must be clarified.
(8)	Ensure that the formulation and the system development methodology are defined based on a target scale and specific system requirements when designing the	General	Developing an information system with the highest efficiency while maintaining consistency with the overall optimization plan.		S	To develop an information system with the highest efficiency while maintaining consistency with the overall optimization plan, the development plan must be formulated by considering the system characteristics and the

	development plan.					scale of development and by selecting an appropriate information system configuration and development method.
(9)	Ensure that a feasibility study with alternatives is studied to achieve the objectives of the information system when designing the development plan.	General	Realizing the functions, capabilities, quality, etc., required of an information system with the highest efficiency.		S	To realize the functions, capabilities, quality, etc., required of an information system with the highest efficiency, multiple system implementation plans must be prepared, compared, and evaluated.
2	Analysis	General				
(1)	Obtain approval of responsible personnel from the user department, the system development department, the operation department and the application maintenance department for the defined requirements based on the development plan.	General	Having all departments (user, development, operation, and maintenance) share a common understanding.		S	To allow user, development, operation, and maintenance departments to share a common understanding of the contents of the requirement definitions, persons in charge at all these departments must approve the requirement definitions.
(2)	Define target, scope and methodology for user requirement survey.	General	Reflecting user needs accurately.		S	To address user needs appropriately, it is necessary to define targets to be surveyed,

						the scope of a survey, and a survey method prior to conducting a survey of user needs.
(3)	Analyze the present states of information systems with personnel who are familiar with the business process from the user department, the system development department, the operation department and the application maintenance department.	General	Understanding the flows, procedures, workloads, etc., of operations now being performed.		S	To analyze the operations now being performed correctly and efficiently and to grasp the flows, procedures, workloads, etc., of operations now being performed, persons in charge at user, development, operation, and maintenance departments who have a good knowledge of daily operations must analyze the present status of operations.
(4)	Ensure that user requirements are documented and confirmed by the user department.	General	Reflecting the results of surveys of user needs in the development plan and development work.		S	To reflect the results of surveys of user needs properly in the development plan, user needs must be documented, and a person in charge at the user department must confirm the contents of documented user needs.
(5)	Analyze potential risks in introducing the information system.	Company/ General	Analyzing the risks that will accompany the introduction of an information system to ensure the sound operation of an	2-2-②	C	To ensure the sound operation of an information system, the risks that may occur with the introduction of an information system must be analyzed.

			information system.			
(6)	Ensure that affected business processes, management structures and rules/procedures are reviewed and assessed regarding the introduction of the information system.	General	Having a correct understanding of the effects that the introduction of an information system will produce on operations, management systems, various rules, etc.		S	To have a correct understanding of the effects that the introduction of an information system will produce on operations, management systems, various rules, etc., and to operate an information system smoothly, it is necessary to establish new operations, modify or abolish existing operations, change management systems, and review various rules.
(7)	Assess the effectiveness from both qualitative and quantitative perspectives when introducing the information system.	General	Monitoring the development plan (evaluating the effects quantitatively and qualitatively).		–	To calculate the effects of introducing an information system reasonably based on the results of calculations made in the development plan, the effects of an information system must be evaluated quantitatively and qualitatively.
(8)	Ensure that suitability with user requirements is assessed before implementing software packages.	General	Monitoring to review the appropriateness of introducing a plan (evaluating package software).		–	To verify that an information system can perform the expected functions and produce the expected results, it is necessary to confirm the compatibility of user needs with package software with respect

						to functions and effects prior to introducing package software.
3	Acquisition	General				
(1)	Define acquisition requirements from the development plan and user requirements. Obtain approval of the responsible personnel from the user department, the system development department, the operation department and the application maintenance department for the defined requirement based on the development plan.	General	Listing the requirements for the functions, performance, quality, etc., of an information system to be constructed based on the development plan.	3-(1)-㉑-D	C	To realize the functions, quality, and other requirements for an information system to be constructed according to plan, requirements for the procurement of the various resources needed to construct an information system must be listed based on the development plan and user needs, and persons in charge at user, development, operation, and maintenance departments must approve the requirements.
(2)	Ensure that hardware, software and networking products are acquired based on the procurement requirements.	General	Realizing a system configuration that should allow the required functions, capabilities, etc., to be realized.		S	To realize a system configuration that allows the required functions, capabilities, etc., to be realized, it is necessary to select software, hardware, network, etc., based on the development plan and user needs.
(3)	Ensure that necessary staff members, budgets,	General	Developing an information system as		S	To develop an information system as scheduled, it is

	facilities and periods are prepared for completing system development.		scheduled.			necessary to acquire the required personnel, budget, equipment, period, etc.
(4)	Ensure that skills required for staff members are specified clearly.	General	Developing an information system as scheduled.		S	To realize the functions, performance, and quality specified in the development plan, it is necessary to clarify what skills are required of personnel inside and outside an organization.
(5)	Ensure that hardware, software and networking products are procured in accordance with procurement rules.	General	Developing an information system as scheduled.		S	To procure the resources needed for development at the appropriate times while ensuring compatibility with requirements, it is necessary to procure software, hardware, and a network based on the rules.
(6)	Ensure that acquired resources are managed in accordance with acquisition rules.	General	Developing an information system as scheduled.		S	To use resources effectively according to the development plan, procured resources must be controlled by the rules.
III	System Development					
1	System Development Methodology	General				

(1)	Obtain approval for system development methodology from the responsible personnel in the system development department.	General	Confirming that the system development methodology meets the requirements for the personnel, budget, period, etc., specified in the system analysis report and requirement definitions.	3-(1)-①-A	C	To confirm that the system development methodology meets the requirements for the personnel, budget, period, etc., specified in the system analysis report and requirement definitions, a person responsible for supervising development activities must approve the documented system development methodology.
(2)	Define development procedures based on the system development methodology.	General	Standardizing the development procedure throughout an organization.	3-(1)-①-A	C	To carry out development activities consistently and efficiently in an organization, the development procedure must be prepared based on the system development methodology that is standardized throughout an organization.
(3)	Determine system development procedures considering the size of system development and characteristics of the system.	General	Developing an information system efficiently, and achieving the required quality.		S	To develop an information system efficiently while maintaining the required quality, the development procedure must be determined with consideration given to the scale of an information system, development period, system characteristics, etc.
(4)	Assess potential risks of	Company/	Developing an	2-(2)-②	C	To develop an information

	system development, and take necessary actions.	General	information system of high quality efficiently according to a development schedule.			system of high quality efficiently according to the development plan, it is necessary to list all the risks involved in development processes and implement measures necessary to remove or reduce the risks.
2	System Design Phase	General				
(1)	Obtain approval for system design documentation from the user department, the system development department, the operation department and the application maintenance department.	General	Securing the quality specified in the system design documentation, ensuring consistency between the system design document and requirement definitions, and providing the system design document as a common property to be used by both development and operation personnel.	3-(1)-㉑-A	C	The quality of the system design documentation must be maintained, consistency between the system design document and requirement definitions must be ensured, and the system design document must be provided as a common property to be used by user, development, and operation departments. To achieve all this, persons in charge at user, development, operation, and maintenance departments must approve the system design documentation.
(2)	Define basic policies on operations and application maintenance	General	Carrying out operation and maintenance work smoothly and	3-(1)-㉒-A	C	To carry out operation and maintenance work smoothly and effectively, basic operation and

	before starting design procedures.		effectively.			maintenance policies must be established at the system design phase so that they can be reflected in the system design documentation.
(3)	Ensure that input-output screens and print-out formats are considered convenient by the users of the system.	General	Preventing data entry mistakes, improving work efficiency, and increasing the utilization efficiency of output information.		S	To prevent data entry mistakes, improve work efficiency, and increase the utilization efficiency of output information, it is necessary to design the input and output forms, input and output screens, and codes by ensuring that they are easy for users to use.
(4)	Ensure that the databases are designed based on the business processes and characteristics of the system.	General	Storing, searching, and updating a large volume and great diversity of data efficiently.	3-(1)-①-B	C	A large volume and great diversity of data must be stored efficiently, and the data must be able to be searched and updated with a level of performance that meets the requirement definitions. To achieve this, a database must be designed with consideration given to the contents of specific operations.
(5)	Ensure data integrity.	General	Guaranteeing the accuracy of data processing.	3-(1)-①-B 3-(1)-②-A	C	The accuracy of data processing must be guaranteed, and data must be free of mistakes, overlaps, omissions, or alterations. To achieve this, the

						integrity of data must be ensured.
(6)	Ensure that the network is designed based on business processes and the characteristics of the system.	General	Making the performance of a network meet the requirement definitions.	3-(1)-②-A	C	To transmit a large volume and great diversity of data with a level of performance that meets the requirement definitions, a network must be designed with consideration given to operation and system characteristics.
(7)	Ensure that the performance criteria of the information system meet the defined requirements.	General	Accomplishing the results that an information system is expected to produce.	3-(1)-②-A	C	To realize the results that an information system is expected to produce, the performance of an information system must meet the requirement definitions.
(8)	Ensure that operability and maintainability are considered in the information system design.	General	Ensuring the smooth operation of an information system, identifying the cause of problems quickly, taking effective corrective measures, and performing effective maintenance work to make improvements.		S	An information system should operate smoothly, the cause of problems should be identified quickly, and maintenance work should be performed effectively and efficiently to allow corrective measures to be implemented. To meet all these requirements, an information system must be designed with consideration given to performance and configuration management, and actions to take to deal with cases of failure, all

						of which are needed to accomplish operation and maintenance tasks.
(9)	Ensure that inter-operability with other information systems is considered for the information system design.	General	Making an information system compatible with the IT infrastructure and other information systems.	3-(1)-①-C	C	An information system must be designed with consideration given to not only matters related to the information system to be designed but also compatibility with the IT infrastructure and other information systems.
(10)	Ensure that potential incidents are considered in the information system design.	General	Preventing the occurrence of information system failure, keeping the effects of failure to a minimum, and allowing an information system to recover from failure quickly.		S	To prevent the failure of an information system, keep the effects of failure to a minimum, and recover an information system from failure quickly, it is necessary to design an information system with due consideration given to specific procedures and measures for recovering it from failure.
(11)	Ensure that error prevention, fraud prevention and information security are considered in the information system design.	General	Ensuring the safety and sound operation of an information system.	3-(1)-①-B	C	To ensure the safety and sound operation of an information system, an information system must be designed with consideration given to the functions for preventing mistakes, preventing misconduct, protecting security, and protecting privacy.

(12)	Ensure that the test plan has a clearly specified objective, scope, methodology and schedule.	General	Verifying correctly and efficiently that an information system has been developed according to the design specification.	3-(1)-①-E	C	To confirm correctly and efficiently that an information system has been developed according to the design specification, it is necessary to verify the purpose and scope of the test plan, test method, test schedule, etc.
(13)	Establish policies on user training, the course plan and the schedule for the information system.	General	Introducing an information system smoothly, and allowing it to produce the expected results.		S	To introduce an information system smoothly and allow it to produce the expected results, it is necessary to clarify the policy for user education regarding the use of an information system, education schedule, etc., at the design stage.
(14)	Ensure that monitoring functions are considered in the system design phase.	General	It should be verifiable that an information system is delivering the level of performance specified in the design specification.	5-(2)-②-A	C	To verify that after an information system starts operation, it is delivering the designed performance specified in the system development plan, it is necessary to incorporate a monitoring function into the information system, and to collect and analyze data.
(15)	Review documentation for the system design.	General	The system design documentation should properly reflect users' requests of an		S	Because the system design documentation must reflect users' requests of an information system properly, it must be

			information system.			reviewed and evaluated with all people concerned at user, development, operation, and maintenance departments in attendance at a review meeting.
3	Program Design Phase	General				
(1)	Obtain approval for program design documentation from the responsible personnel for system development (project manager).	General	Ensuring the quality of the program design documentation, maintaining compatibility with system design, and allowing efficient programming work to be performed.	3-(1)-㉑-A	C	To secure the quality of the program design documentation, ensure consistency between the program design documentation and system design, and allow efficient programming work to be performed, a person in charge of development must approve the program design documentation.
(2)	Design programs based on the system design documentation.	General	Reflecting the functions and system structure defined by system design in a program without any excess or shortage.		S	To reflect the functions and system structure defined by the system design accurately in a program without any excess or shortage, it is necessary to design a program based on the system design documentation.
(3)	Define and document the test requirements.	General	Verifying the appropriateness of the results of program design and programming.		S	To verify the appropriateness of the results of program design and programming, it is necessary to define and document test requirements.

(4)	Review program design documents and the test requirements.	General	Enhancing the quality of program design.		S	To enhance the quality of program design, it is necessary to review the program design documents and test requirements.
(5)	Return to the system design phase to resolve contradictions in the system design found during program design.	General	Ensuring consistency between system design and program design.		S	To ensure consistency between system design and program design, the inconsistencies in the system design noted during the program design must be resolved by making a review of the system design.
4	Programming Phase	General				
(1)	Perform programming based on the specifications of the program design documentations.	General	Reflecting the functions defined by the program design documentations accurately in a program without any excess or shortage.		S	To reflect the functions defined in the program design documentations accurately in a program without any excess or shortage, programming must be carried out based on the program design documentations.
(2)	Ensure that programming activity complies with the coding standards.	General	Securing the program quality by observing the coding standards.		S	To ensure the quality of a program, program codes must conform to the coding standards.
(3)	Ensure that the program codes and test results are assessed properly, recorded and stored.	General	Verifying that programmed functions work accurately as specified in the program		S	It must be confirmed that programmed functions work accurately as specified in the program design document

			design document without any excess or shortage, and confirming the appropriateness of the program test.			without any excess or shortage, and the appropriateness of a program test must be verified. To achieve this, program codes must be evaluated, and the results of a program test must be recorded and kept.
(4)	Ensure that important programs are tested by someone other than the software developer.	General	Preventing mistakes and misconduct associated with programming.	3-(1)-①-E	C	To prevent mistakes and misconduct associated with programming, important programs must be tested by a person other than the person who wrote them.
5	System Tests and User-acceptance Tests Phase	General				
(1)	Obtain approval for the system test plan from the responsible personnel for the software development project and the test leader.	General	Ensuring the appropriateness of a system test plan.	3-(1)-①-E 3-(1)-④-B	C	To verify the appropriateness of a system test plan, a system plan must be approved by persons in charge of development and testing.
(2)	Obtain approval for the user-acceptance test plan from the responsible personnel in the user department and the system development department.	General	Ensuring the appropriateness of a user-acceptance test plan.	3-(1)-①-E	C	To verify the appropriateness of a user acceptance test plan, a user-acceptance test plan must be approved by persons in charge of user services and development.
(3)	Prepare potential test	General	Verifying that system	3-(1)-①-E	C	To verify that system

	cases covering all the system requirements for system tests.		requirements are met.			requirements are met, a test case must be set up by listing all system requirements and a system test must be conducted.
(4)	Prepare test data and perform system tests in accordance with the test plan.	General	Accomplishing the purposes of a system test accurately and efficiently.	3-(1)-①-E	C	To accomplish the purposes of a system test accurately and efficiently, test data must be prepared and a system test must be conducted based on a test plan.
(5)	Ensure that system tests are performed in an environment separated from the production environment.	General	Conducting a system test in a way that does not affect the production environment.	3-(1)-①-E 3-(1)-④-C	C	Because conducting a system test may adversely affect the production environment, a system test must be conducted in an environment separated from the production environment.
(6)	Ensure that system tests are performed by personnel who are not members of the software development team.	General	Verifying equitably and objectively that the development information system as a whole functions properly.	3-(1)-①-E	C	To verify equitably and objectively that a developed information system as a whole is functioning properly, personnel other than those involved in the development work must attend a system test.
(7)	Ensure that appropriate testing methodologies and standards for system tests are used.	General	Conducting a system test efficiently and effectively.	3-(1)-①-E	C	To conduct a system test efficiently and effectively, appropriate test methods and standards must be adopted and used.

(8)	Ensure that the user-acceptance test is performed in an environment similar to the production environment.	General	Verifying the appropriateness of user requirements.	3-(1)-①-E 3-(1)-④-D	C	To verify the appropriateness of user requirements, the user acceptance test must be conducted in much the same environment as the production environment.
(9)	Prepare test cases based on user manuals and simulate the live processes in the user-acceptance tests.	General	The user conducts the user-acceptance test from the user's standpoint by assuming operations in the production environment.	3-(1)-①-E 3-(1)-④-E	C	The user conducts the user-acceptance test from the user's standpoint by assuming operations in the production environment. The test is conducted to obtain final confirmation. It must be conducted in accordance with the requirement definitions and user manual by establishing a test case in which operations in the production environment are assumed.
(10)	Ensure that personnel from the user department and the operation department are involved in the user-acceptance tests, and that they review the user-acceptance test results.	General	Conducting the user-acceptance test by assuming operations in the production environment.	3-(1)-①-E 3-(1)-④-F	C	The user-acceptance test is conducted to obtain final confirmation by assuming operations in the production environment. To minimize the problems that may occur after the start of production, the user acceptance test must be attended by persons in charge in the user and operation departments.

(11)	Obtain approval for the results of system tests and user-acceptance tests from responsible personnel in the user departments, the system development department, the system operations and application maintenance departments.	General	Unifying the understanding of the results of the system test and user-acceptance test.	3-(1)-㉑-E	C	To unify the understanding of the results of the system test and user-acceptance test, the test results must be approved by persons in charge in the user, development, operation, and maintenance departments.
(12)	Ensure that the progress and results of the system tests and the user-acceptance tests are documented, recorded and stored.	General	Using the records of the progress and results of the system test and user acceptance test as basic data for identifying the cause of problems occurring during operations.	3-(1)-㉑-E 3-(1)-㉒-G	C	The results of the system test and user acceptance test must be recorded, and the recorded data must be retained as basic data to be used to identify the cause of problems occurring during operations and to perform maintenance work.
(13)	Ensure that the software package developer has tested the quality of the software before implementing the package.	General	Confirming that the package software developer has conducted quality tests.	3-(1)-㉑-E	C	If an information system is constructed by introducing packaged software, the quality of the information system is affected by the quality of the packaged software. Therefore, it must be confirmed that the packaged software developer has conducted tests to verify the packaged software quality.

6	Promotion to Production	General				
(1)	Establish the promotion plan, and obtain approval from the responsible personnel in the user departments, the system development department, the system operations department and the application maintenance department.	General	Smoothly and efficiently moving from the system development and testing stages to the operation stage.		C	The development department carries out the promotion process to turn over the information system to the user, operation, and maintenance departments. A promotion plan must be prepared to move smoothly and efficiently from the system development and testing stages to the operational stage, and it must be approved by persons in charge in each department.
(2)	Document the promotion processes, and obtain approval from the system operation department.	General	Ensuring smooth operations in the operation stage.		S	To ensure smooth operations in the operation stage, the results of promotion work performed to move the results of development work into the production environment must be recorded and documented, and a person in charge must approve the contents of this documented data.
(3)	Define the criteria for the completion of promotion to production in the promotion plan.	General	Confirming that an information system is ready to be operated in the production environment.		S	To confirm that an information system is ready to operate in the production environment, how the completion of promotion can be verified must be

						described in the promotion plan.
(4)	Ensure that the necessary staff, budgets and equipment are secured based on the promotion plan.	General	Performing operations as scheduled in the promotion plan.		S	To perform promotion work as scheduled and specified in the promotion plan, it is necessary to prepare the personnel, budget, equipment, etc., needed to carry out the promotion process.
(5)	Prepare procedure manuals for promotion and follow them.	General	Preventing omissions, overlaps, insufficient evaluations or confirmations, etc., when carrying out promotion.		S	To perform promotion work as specified in the promotion plan and to prevent omissions, overlaps, insufficient evaluations or confirmations, etc., a promotion procedure must be prepared to train personnel for promotion and to make prior confirmations.
(6)	Consider contingency plans for the potential risks.	General	Identifying the harmful events that may occur during promotion.		S	To clarify the effects of harmful events occurring during promotion and to minimize their effects, it is necessary to identify the risks involved in the promotion process and prepare measures for dealing with the risks.
(7)	Hand over all necessary development documents and tools from the development team to the	General	Making sure that the system operations can be performed and maintenance work can		S	Personnel at the operation and maintenance departments of the system should be able to start specific operations smoothly

	system operations department and the application maintenance department.		be performed smoothly			upon completion of promotion before the start of production. To achieve this, design documents, test results, promotion results, various tools, operation manuals, etc., must be turned over from a person in charge of development to persons in charge in the operation and maintenance departments.
(8)	Ensure that the stakeholders are informed of the completion of the promotion.	General	Preventing promotion from hampering the operations of other systems related to this system.		S	To prevent promotion from hampering the operations of this system and other related internal and external systems, it is necessary to make the outline of promotion fully understood by the people concerned.
IV	Operation Processes					
1	Operation Management Rules	General			C	
(1)	Obtain the approval of the responsible personnel from the operation department for the operation management rules and procedures.	General	Establishing and approving the operation management rules and procedures.	3-(2)-①-A	C	Operations management rules and operation procedures are needed to perform operations smoothly and efficiently. A person in charge of supervising operations must confirm the contents and approve them.

(2)	Define operation management rules based on the operation management design.	General	Managing operations based on the basic principles of operation management design.	3-(2)-①-A	C	Basic principles of the operations management rules are specified in the application operation management design and infrastructure operation design. Therefore, they must be established based on these operation designs. If an operations management method is determined based on the general optimization plan for a large-scale system or if an operations management method is based on the use of services, operations management rules must be established based on such basic operation management methods.
(3)	Define operation procedures based on the operation management design and rules considering the target scale, periods and specific system requirements.	General	Performing operations efficiently.		S	To perform operations efficiently, it is necessary to determine operation procedures based on the operation design and operations management rules, with consideration given to scale, period, system characteristics, etc.
(4)	Ensure that responsible personnel are selected based on the operational	General	Designating a person in charge of supervising operations.		S	To perform operations smoothly, persons in charge of operating specific operations must be

	management design and rules.					designated. This is particularly important in a situation where a decision must be made quickly, for example, when handling exceptions, faults, etc. Specifically, persons in charge should be designated for each set of system functions.
2	Operation Management	General				
(1)	Define the annual operation plan and obtain approval from the responsible personnel for the annual system operation plan.	Company	Formulating an annual system operation plan.	3-(2)-①-B	C	An information system must be operated smoothly, and the events of each information system must be processed and completed as scheduled. To achieve this, the system operation plan must be formulated every year, a person in charge must obtain the agreement of the people concerned and approve the plan, and the system operation plan approved must be made fully understood by the people concerned.
(2)	Ensure that monthly and daily system operation plans are created from the annual operation plan.	Company	Operating an information system smoothly and efficiently.	3-(2)-①-B	C	To operate an information system smoothly and efficiently, it is necessary to prepare a monthly operation plan, a daily

						operation plan, etc., based on the annual operation plan.
(3)	Ensure that the operation activities comply with the operation management rules.	General	Preventing mistakes and misconduct related to an information system.	3-(2)-①-B	C	Operations must be standardized, and mistakes and misconduct related to an information system must be prevented. To achieve this, operations must be managed based on the management system, procedures, and rules.
(4)	Ensure that job schedules are organized according to the priorities of the business processes.	General	Using operation resources effectively.	3-(2)-①-D	S	To use resources effectively and perform operations in a way that meets user needs, a job schedule must be established with consideration given to the priority of operations.
(5)	Ensure that the system operation complies with the job schedules and operational instructions.	General	Preventing operation mistakes and misconduct.	3-(2)-①-D	C	To use resources effectively and prevent operation mistakes and misconduct, operations must be performed based on the job schedule and instruction sheets.
(6)	Ensure that exceptional operation of the system is handled based on the operation management rules.	General	Preventing operation mistakes and misconduct.	3-(2)-①-C	C	To prevent operation mistakes and misconduct and to perform operation smoothly, exception handling must be carried out properly based on the operations management rules.
(7)	Ensure that shift handovers are carried out	General	Performing operations smoothly and accurately		S	To carry out operations smoothly and accurately,

	in accordance with the operation management rules.					operators must be rotated based on the operations management rules.
(8)	Ensure that job schedules are recorded with operation logs and the differentials from the original ones are analyzed.	General	Preventing operation mistakes and misconduct.	3-(2)-①-D	C	Operation mistakes and misconduct must be prevented, and operations must be performed smoothly. To achieve this, any differences between the job schedule and operation records must be analyzed.
(9)	Ensure that operational records are retained for a certain period in accordance with operation management rules.	General	Investigating the causes of operation mistakes, misconduct, incidents, and failures.	3-(2)-①-E	C	To investigate the causes of operation mistakes, operation misconduct, incidents, or failures, the operation records must be retained for a specified period of time based on the operation management rules.
(10)	Define a reporting system and procedures in proportion to the levels of impact of incidents or failures.	General	Dealing with an incidents or failure by considering the scale and the degree of effect.		C	Because the effect of incidents or failure varies greatly depending on its scale and where it occurs, an escalation flow for coping with a situation flexibly according to the scale and the degree of effect must be established so that the most appropriate action can be taken quickly to keep the effect of an accident or failure to a minimum.

(11)	Ensure that all records of incidents or failures are retained and reported to the responsible personnel for operation (management).	General	Recovering an information system from incidents or failures quickly, and preventing it from occurring again.	3-(2)-①-F	C	To recover an information system from incidents or failures quickly and to prevent them from occurring again, the contents of incidents or failures must be recorded, and reported to a person in charge of supervising operations.
(12)	Ensure that root causes of incidents or failures are investigated, and take proper actions to prevent reoccurrences.	General	Achieving fast recovery from an accident or failure, and preventing it from occurring again.	3-(2)-①-F	C	To prevent an accident or failure from occurring, its cause must be identified when it occurs, and measures must be taken to prevent it from occurring again.
(13)	Establish a support environment to help and assist users of the information system.	General	Contributing to EUC operations, and performing EUC tasks smoothly.	3-(2)-①-G	C	The opportunity for users to perform information-processing tasks by using computers is expanding quickly; a typical example is EUC (End-user Computing). To contribute to increasing the efficiency of information-processing operations, the information system department must play the leading role in establishing a user support system.
(14)	Provide users with information security education and training.	General	Enhancing users' awareness of information security.	3-(2)-①-G	C	To enhance users' awareness of information security, education and training must be provided.
(15)	Establish a monitoring	General	Confirming and	5-(2)-②-B	C	To confirm and control the

	framework for system operations.		managing the reliability, safety, efficiency, effectiveness, resources, etc., of an information system.			reliability, safety, efficiency, effectiveness, resources, etc., of an information system, it is necessary to establish a monitoring system regarding the operations of an information system.
(16)	Ensure that operational efficiency is attained for the information system to improve performance and the utilization of resources.	General	Increasing the cost effectiveness of an information system.		S	To increase the cost effectiveness of an information system, operation records must be analyzed based on the results of monitoring information system operations, and the results of analyses must be used to control the status of performance and to use resources effectively through discussion with the people concerned.
3	Manage Input	Operation				
(1)	Define and comply with input control rules.	Operation	Documenting procedures, verification methods, and authorization methods regarding a series of operations performed to input data into an information system.	4-(1)-①	C	A series of operations performed to input data into an information system, including preparation of data to be inputted, giving and receiving of data, verification of data, data input, checking of data after it is inputted, storage of data, etc.,

						shall be documented as a data input procedure. A data verification method and data approval method must also be established as data input management rules. This procedure and these rules must be observed.
(2)	Ensure that input data is accurate and without omissions or duplications, and comply with input control rules.	Application	Preventing errors in data input, such as data omissions, double inputs, etc.	4-(1)-②	C	When inputting data into an information system, a procedure described in the input management rules must be performed, and data must be input carefully by taking care to prevent errors in data input, such as data omissions, double inputs, etc.
(3)	Ensure that error prevention, fraud prevention and confidentiality protection measures are included in creation procedures and operational procedures for input data.	Application	Preventing the misconduct that may occur when preparing data to be input, handling data, etc.		S	To prepare and handle data to be inputted properly and prevent misconduct in data input, it is necessary to implement measures for preventing mistakes and misconduct and protecting confidentiality during data preparation, data handling, and data input.
(4)	Ensure that error prevention, fraud prevention and	Application	Inputting data correctly.	4-(1)-③	S	Measures taken to input data correctly, specifically measures taken to prevent mistakes and

	confidentiality protection for input data are put in place effectively.					misconduct and to protect confidential and personal information must work effectively.
(5)	Define procedures for input data storage or disposal and ensure they comply with input data control rules.	Application	Preventing the loss, theft, leakage, etc., of data.	4-(1)-④	S	To prevent the loss, theft, leakage, etc., of inputted data, data must be retained or discarded based on the input management rules.
4	Manage Data	Application				
(1)	Define and ensure they comply with data control rules.	General / Application	Preventing data-processing mistakes and protecting confidential and personal information.	3-(2)-③-A 4-(2)-①	C	To prevent data-processing mistakes and to protect confidential and personal information, it is necessary to document the rules for handling and managing data at each development, operation, and maintenance department, and to observe them.
(2)	Ensure that access control and monitoring data (creation, changes, and deletion) are put in place effectively.	General / Application	Preventing unauthorized access to data and unauthorized use of data, and protecting confidential and personal information.	3-(3)-②-A 4-(2)-②	C	To prevent unauthorized data access and abuse of data and to protect confidential and personal information, it is necessary to verify that the access control and monitoring functions are working effectively.

(3)	Ensure that data integrity is assured.	General / Application	Making data accurate and complete.	3-(2)-③-C 4-(2)-③	C	To ensure that data is accurate and complete or that data integrity is maintained, data must be updated correctly.
(4)	Ensure that data usage is recorded and analyzed periodically.	Application	Preventing unauthorized use of data.		S	To prevent the abuse of data, the situation with regard to the use of data must be monitored and recorded, and data collected this way must be analyzed periodically.
(5)	Define the scope, method and timing of data backup according to business requirements, the data processing structure and data restoration.	Application	Minimizing the effects of failed data-recording media, operation mistakes, computer viruses, etc.	3-(2)-③-D	C	The effects of failed data-recording media, operation mistakes, computer viruses, etc., must be minimized by creating a backup of data. In creating a backup, the types of data for which the backup is to be created and the timing to create the backup must be determined with consideration given to the contents of operations, data-processing methods, and data recovery methods.
(6)	Ensure that data delivery complies with data control rules.	General/ Application	Preventing the use of wrong data, unauthorized use of data, falsification of data, etc.	3-(2)-③-A 3-(2)-③-B 4-(2)-④	C	To prevent the use of wrong data, abuse of data, falsification of data, etc., data must be given and received in accordance with the data management rules.
(7)	Ensure that fraud	General/	Preventing the use of	3-(2)-③-B	C	To prevent the misconduct and

	prevention and confidentiality protection measures are used whenever data is exchanged.	Applicati on	wrong data, abuse of data, falsification of data, etc. Preventing the abuse of data and leakage of confidential information, and protecting personal information.	4-(2)-㉔		leakage of confidential information associated with an exchange of data, necessary measures must be taken to prevent misconduct and to protect confidential and personal information.
(8)	Ensure that procedures for data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection.	Applicati on	Preventing the abuse of data, leakage of data, abuse of personal information, etc.	4-(2)-㉕	C	To prevent data including personal information from being abused or leaked, it is necessary to establish measures for preventing such mistakes or misconduct from occurring whenever data is stored, copied, or discarded.
(9)	Ensure that data is protected from computer viruses.	Applicati on	Protecting data from computer viruses.		S	To protect data from computer viruses, measures must be taken to eliminate computer viruses.
(10)	Ensure that the intellectual property rights of data are managed properly.	–	Protecting the intellectual property rights of constructed data, and preventing intellectual property rights of data introduced from outside sources from being infringed.			To protect the intellectual property rights of data and to prevent the infringement of intellectual property rights introduced from outside sources, the management of intellectual property rights must be carried out properly.

5	Manage Output	Applicati on				
(1)	Define and comply with output control rules.	Applicati on	Preventing output mistakes, and abuse and leakage of output data, and protecting confidential and personal information.	4-(3)-①	C	Mistakes in the output method and the abuse or leakage of output data must be prevented, and confidential and personal information must be protected. To achieve this, it is necessary to establish and observe a data output procedure, data approval procedure, related rules, etc.
(2)	Ensure output data is accurate and free from omissions or duplications.	Applicati on	Preventing errors, omissions, double outputs, etc., in output data.	4-(3)-②	C	To ensure that data output from an information system does not contain errors, omissions, double outputs, etc., a procedure described in the output management rules must be performed in a careful, strict manner.
(3)	Ensure that output data control and operational procedures are taken for error prevention, fraud prevention and confidentiality protection.	Applicati on	Preventing the falsification, theft, leakage, etc., of data	4-(3)-③	C	Data to be outputted must be prepared and handled carefully by taking care to prevent the falsification, theft, leakage, etc., of data. Specific measures must be taken to prevent mistakes, misconduct, or the leakage of confidential information during the preparation and handling of data.

(4)	Ensure that output data is delivered based on output data control rules.	Application	Preventing output data from being delivered to a wrong party, lost, stolen, etc.	4-(3)-④	C	To prevent output data from being delivered to a wrong party, lost, stolen, etc., it is necessary to establish a data delivery procedure and related rules, and to observe them.
(5)	Ensure that output data retention or destruction is based on output data control rules.	Application	Preventing output data from being lost, stolen, leaked, etc.	4-(3)-⑤	C	To prevent the loss, theft, leakage, etc., of output data, it is necessary to store or discard data in accordance with the output management rules.
(6)	Ensure that errors occurring in the output process are recorded and reviewed periodically.	Application	Maintaining the accuracy of output data.		S	To maintain the accuracy of output data, the status of errors must be recorded, and analyzed periodically.
(7)	Ensure that usages of output data are recorded and reviewed periodically.	Application	Utilizing output data.		S	To use output data effectively, the situation with regard to the use of output data must be recorded, and analyzed periodically.
6	Software Management	General				
(1)	Define and comply with software control rules.		Using software equitably and preventing misconduct.	3-(2)-②-A	C	To ensure that software is used properly and to prevent software from being abused, rules for handling and management of software must be established and observed at each development, operation, and

						maintenance department.
(2)	Ensure that access control and monitoring functions for software are put in place effectively.	General	Preventing the abuse of software.	3-(2)-②-B 3-(3)-②-A	C	To prevent the abuse of software, it must be verified that the access control and monitoring functions are working effectively.
(3)	Ensure that software usage information is stored and reviewed periodically.	General	Preventing the abuse of software.		S	To increase the operating efficiency of software and prevent the abuse of software, the situation with regard to the use of software must be recorded, and analyzed periodically.
(4)	Define the scope, method and timing of software backups according to business requirements and the data processing structure.	General	Minimizing the risks associated with the failure of recording media of software, operation mistakes, computer viruses, etc.		S	To minimize the effects of failed recording media of software, operation mistakes, computer viruses, etc., it is necessary to determine for which software a backup is to be created and the backup method with consideration given to the contents of operations and data-processing methods.
(5)	Ensure that software delivery is complies with software control rules.	General	Preventing software from being used in a wrong way, abused, falsified, etc.		S	To prevent software from being used in a wrong way, abused, falsified, etc., software must handled based on software management rules that specify a giving and receiving procedure,

						a delivery method, etc.
(6)	Ensure that procedures for software data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection.	General	Preventing software from being used in a wrong way, abused, falsified, etc.		S	Measures must be taken to prevent software and related data from being abused, leaked, etc., when data is stored, copied, or discarded.
(7)	Ensure that software is protected from computer viruses.	General	Protecting software from computer viruses.		S	To protect software from computer viruses, measures must be taken to eliminate computer viruses.
(8)	Ensure that the intellectual property rights of software are managed properly.	–	Protecting the intellectual property rights of developed software, and preventing the intellectual property rights of software that has been introduced from being infringed.			The intellectual property rights of developed software must be protected, and the intellectual property rights of introduced software must be prevented from being infringed. To achieve this, the management of intellectual property rights must be carried out properly.
(9)	Define policies for the utilization of free software (open source).	General	Minimizing the risks associated with the use of free software.		S	Although free software offers a great advantage in terms of cost, there are the risks involved in using free software: no guarantee of processed results, the possibility of computer viruses lurking within them, possible infringement of

						intellectual property rights, etc. To use free software, an organization must establish a policy for its use.
7	Manage Hardware	General				
(1)	Define and comply with hardware management rules.	General	Promoting the proper use of hardware, preventing failure from occurring, protecting hardware from natural hazards and misconduct, etc.	3-(2)-②-A	C	To promote the proper use of hardware, prevent hardware failure, and to protect hardware from natural hazards and misconduct, etc., it is necessary to establish hardware management rules and observe them.
(2)	Ensure that hardware is installed in an environment resilient to potential risks.	General	Minimizing the effects of failure, natural hazards, misconduct, etc., on an information system.	3-(2)-②-G 3-(3)-②-A	C	To minimize the effects of failure, natural hazards, misconduct, etc., on an information system, hardware must be installed in an environment that allows an organization to deal with assumed risks properly.
(3)	Ensure that periodical maintenance is provided for hardware.	General	Preventing hardware failure from stopping the operation and/or deteriorating the functions of an information system.		S	To prevent hardware failure from stopping the operation or deteriorating the functions of an information system, maintenance must be conducted periodically.
(4)	Ensure that proper	General	Preventing the	3-(2)-②-E	C	To prevent the suspension of the

	measures are taken for hardware failures.		suspension of the operation and/or deterioration of the functions of an information system.			operation or deterioration of the functions of an information system and to achieve fast recovery in the event of hardware failure, it is necessary to establish measures for handling cases of hardware failure.
(5)	Ensure that hardware usage is recorded and reviewed periodically.	General	Using hardware effectively, and preventing the abuse of hardware.		S	To allow hardware to be used effectively and prevent the abuse of hardware, the situation with regard to the use of hardware must be recorded, and recorded data must be analyzed periodically.
(6)	Ensure that procedures for hardware retention, relocation and disposal are taken for error prevention, fraud prevention and confidentiality protection.	General	Preventing the leakage of confidential information that may occur if hardware is stolen, lost, disposed of, etc.		S	Cases in which a piece of hardware is stolen or lost and it is used by a person other than the one entitled to ownership must be avoided, and data and other information assets must be protected. Therefore, measures must be taken to prevent the misconduct and leakage of confidential information that may occur when hardware is stored, relocated, or disposed of.
8	Manage Network	General				

(1)	Define and comply with network management rules.	General	Operating the network normally and efficiently.		S	To operate the network normally and efficiently, network management rules must be established and observed.
(2)	Ensure that access control and the monitoring functions for the network are put in place effectively.	General	Preventing hacking or abuse of the network.		S	To prevent hacking or abuse of the network and to detect cases of hacking or abuse as quickly as possible, it must be ensured that the control of network access and monitoring is functioning effectively.
(3)	Ensure that the network is periodically reviewed for monitoring logs.	General	Preventing hacking or abuse of the network.		S	To detect cases of network hacking or abuse and take necessary action, it is necessary to analyze network monitor logs periodically.
(4)	Ensure that proper measures are taken against failures in the network.	General	Ensuring the availability of an information system, electronic mail, Web, and other various services.	3-(2)-②-E	C	To ensure the availability of an information system, electronic mail, Web, and other various services, measures must be established to cope with a possible failure of the network.
(5)	Ensure that the network usage is periodically analyzed from stored records.	General	Operating the network stably and efficiently.		S	To operate the network stably and efficiently, the situation with regard to the use of the network must be recorded, and the recorded data must be analyzed periodically.
(6)	Define organization	General	Allowing an		S	An organization's policy for

	policies for services provided by network operators.		organization to use the network efficiently.			information-providing services using the network must be clarified to use the services efficiently.
9	Manage Configuration	General				
(1)	Ensure that the scope of software management, hardware management and network management is clearly defined. Ensure that a proper management level is provided.	General	Managing software, hardware, and networks properly.		S	Persons in charge of user and network management must coordinate properly with vendors by clarifying the division of responsibilities for specific pieces of software and hardware and networks in order to avoid a situation where a piece of software or hardware or a certain network is doubly overseen by both persons of the organization and the vendor or not overseen at all by either.
(2)	Ensure that system configuration, vendors and support conditions for software, hardware and networks are clearly specified.	General	Maintaining the functions of an information system, and achieving fast recovery in the event of failure.	3-(2)-②-D	C	To maintain the functions of an information system and achieve fast recovery in the event of failure, it is necessary to clarify software, hardware, and network configurations, procurement sources, support conditions, etc.
(3)	Ensure that the introduction and	General	Preventing the suspension of the	3-(2)-②-G	C	To ensure the stable operation of an information system by

	replacement of software, hardware and networks is decided before an assessment of its impact.		operation of an information system and the deterioration of its functions to ensure the stable operation of the information system.			preventing the suspension of its operation and the deterioration of its functions, software, hardware, or the network shall be introduced, and the existing software, hardware or network must be replaced with new ones after carefully considering the extent of the impact.
(4)	Ensure that the introduction and replacement of software, hardware and networks is planned systematically.	General	Minimizing the effects on an information system.		S	To minimize the effects on an information system, it is necessary to introduce software, hardware, or a network or to replace the existing software, hardware, or network according to the plan.
10	Manage Facilities and Equipment	General				
(1)	Ensure that facilities are located in an environment resilient to potential risks.	General	Designing buildings and facilities so that they function to minimize the effects (damage) of the suspension of the operation of an information system, the breakdown of an information system, etc.			To minimize the effects (damage) of the suspension of the operation or the breakdown of an information system, buildings and related facilities must be established in an environment that allows an organization to avoid assumed risks properly.
(2)	Ensure that accesses to	General	Separating an			To protect an information

	facilities and machine rooms are controlled for fraud prevention and protection of confidentiality.		information system to protect it from misconduct.			system from misconduct, measures for preventing misconduct and protecting confidentiality must be included as part of the control of entry and exit into/from buildings and rooms.
(3)	Ensure that facilities are properly operated.	General	Allowing an information system to operate in the same stable environment.			Related facilities must be operated continuously and stably by establishing and observing rules for managing and operating them.
(4)	Ensure that maintenance of facilities is provided periodically.	General	Preventing the failure of related facilities from suspending the operation or deteriorating the functions of the information system, etc.			Periodic maintenance must be conducted on related facilities to prevent their failure from causing the suspension of the operation of the information system, the deterioration of its functions, etc.
(5)	Ensure that proper measures against failures are taken.	General	Preventing the failure of related facilities, and recovering them from failure quickly.			To prevent the failure of related facilities and achieve fast recovery in the event of failure, measures for dealing with cases of failure must be established.
(6)	Ensure that the access logs to the facilities and machine rooms are recorded and reviewed periodically.	General	Identifying the persons who enter a building or room so that a follow-up can be conducted at a later date (to prevent			The control of entry and exit into/from buildings and rooms requires that persons who enter a building or room when an accident occurs be identified so

			misconduct or crime).			that a follow-up investigation can be conducted. Therefore, entry into buildings and rooms must be recorded, and the recorded data must be analyzed periodically by a person in charge of entry and exit control.
V	Maintenance					
1	Maintenance Procedures	General				
(1)	Obtain approval for maintenance rules and procedures from the person responsible for maintenance.	General	Conducting maintenance smoothly.		C	To standardize maintenance operations and perform maintenance operations smoothly while ensuring reliability, maintenance rules and a maintenance procedure must be established and a person responsible for supervising maintenance operations must approve them.
(2)	Define maintenance procedures according to the scale and necessary period of maintenance and specific system requirements.	General	Conducting maintenance efficiently.		S	To conduct maintenance efficiently, a maintenance procedure must be determined based on the maintenance rules, the scale of maintenance, period, system characteristics, etc.
(3)	Assess potential risks	General	Preventing system		S	To prevent maintenance work

	inherent in the maintenance, and develop necessary preventive measures.		failure or other types of problems from occurring.			from causing system problems or other types of problems, it is necessary to identify all assumed risks and to take necessary measures after evaluating each risk.
2	Maintenance Plan	General				
(1)	Obtain approval for the maintenance plan from the personnel responsible for maintenance.	General	Clarifying the scope of maintenance and the contents of maintenance work.		S	To clarify the scope of maintenance and the contents of maintenance work, a maintenance plan must be formulated based on the results of surveys and analyses, and persons in charge in the service and maintenance departments must approve it.
(2)	Examine and analyze the contents and influence of maintenance against change requests.	General	Performing maintenance work smoothly.		S	To have a correct understanding of the contents of a request to change a maintenance plan and conduct maintenance smoothly, it is necessary to survey and analyze the contents of maintenance work and the extent of the impact.
(3)	Define the objective, scope, methodologies, and schedule for the maintenance test plan.	General	Conducting maintenance smoothly.		S	To allow a maintenance test to be conducted smoothly, a test plan describing the purpose, scope method, schedule, etc.,

						must be prepared.
3	Maintenance Implementation	General				
(1)	Ensure that any modifications of the system design documents and the program design documents are implemented according to the maintenance plan. Prior to the modification, obtain approval for any changes of documents from the personnel responsible for maintenance, together with the appropriate stakeholders.	General	Preventing or reducing maintenance-related mistakes, misconduct, failure of performance, etc.	3-(1)-③-F	C	To prevent or reduce mistakes, misconduct, performance failure, etc., a system design document, program design document, etc., must be changed, and persons in charge in the user and maintenance departments must approve the changed documents.
(2)	Ensure that all program modifications are implemented according to the authorized maintenance procedures. Prior to modifications, changes must be approved by the personnel responsible for maintenance.	General	Preventing the mistakes and misconduct that may occur when a program is changed.	3-(1)-③-G	C	To prevent the mistakes and misconduct that may occur when a program is changed, a person in charge of maintenance must approve the contents of the program change.

(3)	Verify that programming is written according to the modified program design documents.	General	Preventing the mistakes that may occur during programming.	3-(1)-㉓-H	C	To prevent mistakes during programming, it must be verified that programming is carried out based on a changed program design document.
4	Maintenance Verification	General				
(1)	Ensure that tests of modified programs are performed in accordance with the maintenance test plan.	General	Conducting a program test smoothly.	3-(1)-㉓-I	C	To test a changed program properly and smoothly, a test must be conducted based on a maintenance test plan.
(2)	Ensure that any tests of modified programs are performed taking into account of the range of impact of the tests.	General	Preventing a changed program from affecting the functions and performance of an information system.		S	To prevent the deterioration of functions and performance of an information system, a test must be conducted on a changed program with consideration given to the extent of the impact.
(3)	Ensure that the user department of the system is involved in the tests for the modified program, and that the tests are performed in accordance with the user manuals.	General	Confirming that an information system meets requirements, including those specified in a change request.	3-(1)-㉓-J	C	To verify that an information system meets the requirements for a change request, etc., the user must attend a program test, and the test must be conducted based on a user manual.
(4)	Obtain approval of the results of the tests of the modified programs from	General	Checking the functions and performance of an information system.	3-(1)-㉓-K	C	To verify the appropriateness of a test and the functions and performance of an information

	the appropriate stakeholder and personnel responsible for operations and maintenance.					system, test results must be approved by persons in charge at user, operation, and maintenance departments.
(5)	Ensure that the results of the tests of the modified programs are properly recorded and stored.	General	Confirming the appropriateness of the conducted test.	3-(1)-㉓-L	C	To verify the appropriateness of a test and to use test results as basic data for investigating the cause of failure and other types of problems, test data and test results must be recorded and retained.
5	Promotion to Production	General				
(1)	Define promotion procedures taking into account of the promotion conditions.	General	Performing the promotion process accurately and smoothly.		S	To perform the promotion process correctly and smoothly, it is necessary to clarify the period, method, system, and other promotion conditions and to prepare a promotion procedure.
(2)	Ensure that backups of the pre-modified program and data are created.	General	Providing for possible promotion-related problems.		S	To provide for the possible problems that may occur during promotion, backups of a program and data to which a change is not yet made must be created.
(3)	Ensure that the personnel responsible for operations and the maintenance	General	Preventing promotion from causing the deterioration of the		S	To prevent the deterioration of functions and performance of other information systems,

	department ensure that the modified system does not affect other information systems.		functions and performance of other information systems.			persons in charge in the operation and maintenance departments must verify the effects of information system promotion.
6	Disposal of Old Information Systems	General				
(1)	Define the disposal plan of old information systems accounting for any risks that may be incurred. Obtain approval for the plan by the appropriate stakeholders and the responsible personnel in the operations and maintenance departments.	General	Minimizing the risks associated with the abolishment of an information system.		S	To abolish an old information system smoothly and completely, an abolishment plan must be prepared with consideration given to risks, and an old information system must be abolished with the approval of persons in charge at user, operation, and maintenance departments.
(2)	Decide the disposal measure and timing of disposal of old information systems, taking measures to prevent fraud and protect confidentiality.	General	Preventing the misconduct, leakage of confidential information, or breach of privacy that may occur when an information system is abolished.		S	To prevent misconduct and protect confidentiality and privacy, the method of abolishing an old information system and the time to abolish it must be determined with consideration given to measures for preventing misconduct and protecting confidentiality.

VI	Common Processes					
1	Document Management					
1.1	Document Creation	Company				
(1)	Obtain approval for created documents from the appropriate stakeholders and responsible personnel in the information system department.	Company	Ensuring the quality of documents and making documents the common property of an organization.		S	To verify the quality of documents and to make documents the common property of an organization, documents must be approved by persons in charge at user and information system departments.
(2)	Define and comply with documentation rules.	Company	Making documents consistent in appearance and quality throughout an organization.		S	To make documents consistent in appearance and quality throughout an organization, it is necessary to define how a document should be organized, its description format, descriptive content, etc., as the rules to be observed.
(3)	Define the documentation plan.	Company	Preparing required documents efficiently.		S	To prepare required documents efficiently, a document preparation plan must be formulated.
(4)	Define the type, the objective and the method of creation of documentation.	Company	Preparing documents efficiently in a way that suits the intended use.		S	Required types of documents should be specified without excess or shortage, and documents should be prepared efficiently in a way that suits the

						intended use. To achieve this, types and purposes of documents, document preparation methods, etc., must be clarified in a document preparation plan.
(5)	Ensure that all documents are created in accordance with the documentation plan.	Company	Preparing documents by including all required information, and getting them ready for use by the time they are needed.		S	To prepare documents by including all necessary information and get them ready for use by the time they are needed, documents must be prepared based on a document preparation plan.
1.2	Documentation Control	Company				
(1)	Obtain approval for the contents of any modifications to documents from the appropriate stakeholders and the responsible personnel in the information department.	Company	Ensuring the quality of updated documents.		S	To check the quality of updated documents and make them the common property of an organization, persons in charge in the user and information system departments must approve the documents.
(2)	Define and comply with documentation control rules.	Company	Maintaining the documents congruous with the contents of an information system, and making them easy to use.		S	To maintain the of compatibility documents with the contents of an information system and to make them easy to use, rules for managing original and distributed documents must be

						established and observed.
(3)	Update descriptions in documents and record the update history following any modification to the information system.	Company	Maintaining the compatibility of documents with the contents of an information system, and showing the latest status of each document.		S	To maintain the compatibility of documents with the contents of an information system and to show the latest status of each document, the contents of related documents must be updated when a change is made to an information system, and updates must be recorded in the update record.
(4)	Ensure that document storage, duplication and destruction measures are taken in accordance with fraud prevention and confidentiality protection.	Company	Preventing documents from being abused, leaked, etc.		S	To prevent documents from being abused, leaked, etc., measures must be taken to prevent the misconduct or leakage of confidential information that may occur when documents are stored, copied, or discarded.
2	Perform Project Management					
2.1	Implementation	General				
(1)	Define a project management approach and structure based on the project plan, and obtain approval from the	General	Performing planning, development, operation and, maintenance operations as planned.		S	To perform planning, development, operation, and maintenance operations as planned, each planning, development, operation, and

	appropriate stakeholders and the personnel responsible for planning, development, operations development and maintenance development.					maintenance department must clarify an appropriate progress management method and progress management system, and a person in charge in each department must approve them.
(2)	Ensure that stakeholders and the personnel responsible in the planning department, the development, the operations department and the maintenance department are monitoring the progress of the project.	General	Detecting problems as early as possible.		S	To detect problems as early as possible, persons in charge at user, planning, development, operation, and maintenance departments must have a correct understanding of the progress of operations.
(3)	Ensure that the appropriate measures are taken against delays.	General	Performing planning, development, operation, and maintenance operations as planned.		S	To perform planning, development, operation, and maintenance operations as planned, measures must be taken to keep delays to a minimum.
2.2	Assess Project Management	General				
(1)	Analyze and assess project performance against the project plan at	General	Reviewing a plan for the next operation process, improving the		S	To review a plan for the next operation process, improve the progress management method,

	the end of each phase of the project, and obtain approval for the assessment result from the project manager.		progress management method, and providing feedback information to the plan for an operation process performed simultaneously or an operation process of the same type that will be performed in the future.			and provide feedback information to a plan for an operation process performed simultaneously or a plan for an operation process of the same type to be performed in the future, it is necessary to analyze and evaluate the results of performance by checking them against a plan upon completion of a planning process, development process, operation process, or maintenance process.
(2)	Ensure that the assessment results are properly reflected in the plan for the next subsequent phase of the project.	General	Increasing the feasibility of a plan for the next process.		S	To increase the feasibility of a plan for the next process, the results of evaluation must be reflected in a plan for the next operation process.
(3)	Ensure that the assessment results are properly reflected in improvements to the approach and the structure of project management.	General	Performing the progress management task efficiently and effectively.		S	To perform the progress management operations efficiently and effectively, the results of evaluation must be used to improve the progress management method, progress management system, etc.
3	Quality Assurance					

3.1	Quality Management Plan					
(1)	Develop a quality management plan according to quality criteria, and obtain approval of the plan from the appropriate stakeholders and the responsible personnel in the planning department, the development department, the operations department and the maintenance department.	General	Maintaining a level of quality worthy of the effort made to achieve organizational objectives.		S	A quality management plan is required to maintain a level of quality worthy of the effort made to achieve organizational objectives in all life cycles of an information system and to perform quality management operations smoothly and effectively. Persons in charge in the user, planning, development, operation, and maintenance departments must approve the quality management plan.
(2)	Define the quality management plan methodology, systems and so on.	General	Operating the quality management system of an organization smoothly.		S	To operate the quality management system of an organization smoothly, it is necessary to clarify how the quality management plan should be implemented, the quality management plan implementation system, the time to implement it, etc. The quality management plan must present the quality management policy specified in the general optimization plan in a concrete

						form.
3.2	Perform Quality Management	General				
(1)	Analyze and assess quality performance against the quality management plan at the completion of each phase of the project, and obtain approval of the result from the project manager.	General	Evaluating the quality management objectives for each operation.		S	To verify that operations have been performed as planned and quality management objectives have been achieved, the results of performance must be analyzed and evaluated based on the quality management rules by checking them against a plan. The results of analysis and evaluation must be approved by a person in charge.
(2)	Ensure that the assessment results are properly reflected in improvements on quality management standards, approaches, and systems.	General	Achieving the quality management objectives of an organization.		S	The results of quality management evaluation must be reflected in the quality management standard, quality management method, quality management system, etc., to improve the activities conducted to achieve the quality management objectives of an organization.
4	Human Resource Management					
4.1	Roles and	Company				

	Responsibilities					
(1)	Define roles and responsibilities for each member of personnel in accordance with the characteristics and requirements assigned to the personnel.	Company	Preventing mistakes and misconduct and protecting confidential information.	2-(1)-③	C	Planning, development, operation, and maintenance operations must be performed efficiently, mistakes and misconduct must be prevented, and confidential information must be protected. To achieve all this, the responsibility and authority of personnel must be clearly defined.
(2)	Verify roles and responsibilities of each member of personnel in accordance with changes in the business and the IT environment.	Company	Coping with changes in the operation environment and information environment.	2-(1)-③	C	To cope with changes in the operation environment and information environment, the responsibility and authority of personnel must be reviewed periodically or with appropriate timing.
(3)	Provide each member of personnel is provided with appropriate orientation and chances to communicate so as to maintain their awareness of their roles and responsibilities.	Company	Performing operations efficiently and effectively, and ensuring good coordination between personnel.	2-(1)-③	C	To perform planning, development, operation, and maintenance operations efficiently and effectively and to ensure good coordination between personnel, assigned responsibility and authority must be made fully understood by all personnel.
4.2	Job Performance	General				

(1)	Ensure that each member of personnel complies with his/her assigned roles and responsibilities.	Company/ General	Preventing mistakes and misconduct.	2-(1)-③	C	To prevent mistakes and misconduct and to perform planning, development, operation, and maintenance operations efficiently and effectively, personnel must obey the assigned authority.
(2)	Verify that assigned tasks and work volume is appropriate for each member of personnel on the basis of their knowledge, skills and so on.	General	Ensuring the quality of a target product.		S	To perform planning, development, operation, and maintenance operations according to plan and to ensure the quality of target products, the division of duties and workload must be determined based on the knowledge, ability, etc., of personnel.
(3)	Ensure that shifts are handed over carried out with error and, fraud prevention and confidentiality protection.	General	Preventing the mistakes and misconduct associated with personnel rotation.		S	Personnel rotation must be practiced with consideration given to preventing mistakes during takeover, preventing the misconduct of personnel who have been taken over and are off duty, and protecting confidential information.
(4)	Ensure that a reserve staffing plan is prepared for contingencies.	General	Maintaining the continuity of operations.		S	To maintain the continuity of planning, development, operation, and maintenance operations, substitute personnel must be arranged for to prepare

						for unforeseen occurrences.
4.3	Education and Training	Company				
(1)	Develop and update the educational training plans and curriculums in accordance with the human resource management policies.	Company	Providing education and training based on a consistent policy of an organization.	2-(1)-④	C	To provide education and training based on a consistent policy of an organization, a curriculum must be prepared based on the policy for human resource management, and it must be reviewed to cope with advances in information technology.
(2)	Ensure that the educational training plans and curriculums are prepared on the basis of the improvement of technological skills, the acquisition of business knowledge, the assurance of information security of the information system, and so on.	Company	Improving the quality of personnel.	2-(1)-④	C	The educational training curriculums must be prepared for the purpose of improving the quality of personnel, specifically increasing their technical competence, and allowing them to learn the knowledge of each operation, as well as ensuring the security of an information system.
(3)	Provide educational training chances to each member of personnel periodically and effectively, based on the educational training plans	Company	Allowing personnel to learn the knowledge, acquire the skills, etc., needed to perform operations.	2-(1)-④	C	To allow personnel to acquire the knowledge, ability, etc., needed to perform planning, development, operation, and maintenance operations efficiently, education and

	and curriculums.					training must be provided periodically and effectively based on the education and training curriculum.
(4)	Develop a career path program for each member of personnel, and review it in accordance with changes in the business and IT environment.	Company	Allowing personnel to learn the knowledge, acquire the skills, etc., needed to perform operations.		S	To allow personnel to acquire the knowledge, ability, etc., needed to perform planning, development, operation, and maintenance operations efficiently, a career path must be established, and it must be reviewed as required to cope with changes in the operation environment and information environment.
4.4	Healthcare					
(1)	Ensure that the work environment is properly managed in accordance with healthcare considerations.	–	Personnel remain physically and mentally fit so that they perform given tasks efficiently.			Personnel remain physically and mentally fit so that they are able to perform planning, development, operation, and maintenance operations efficiently. To achieve this, the working environment must be improved with healthcare considerations.
(2)	Carry out regular medical examinations and prepare mental healthcare	–	Taking care of the physical and mental aspects of personnel.			To maintain the health of personnel, health checkups and counseling about their physical

	programs.					and mental health must be conducted.
5	Consignment / Entrustment					
5.1	Consignment or Entrustment Business Plans	General				
(1)	Develop consignment or entrustment business plans in accordance with the overall optimization plan, and obtain approval to those plans from the management.	General	Preparing consignment or entrustment business plan in concrete form.	3-(4)-①-A	C	The policies for fulfilling a consignment or entrustment are described in the use of “External Resources” in the overall optimization plan (I Strategic IT Plan, 1. Overall optimization, 1.3 Development of the overall optimization plan (7)). To prepare consignment or entrustment business plan in concrete form, the consignment or entrustment business plan must be prepared, and approved by persons in charge.
(2)	Define the objectives, scopes, budget, and structure of the consignment or entrustment business.	General	Clarifying the contents of the actual consignment or entrustment business to allow related operations to be performed smoothly.	3-(4)-①-B	C	The contents of the actual consignment or entrustment business must be clarified to allow related operations to be performed smoothly. Specifically, the purposes, scope, system, budget, etc., of

						these projects must be clarified.
(3)	Assess concrete effects and potential problems of the consignment or entrustment business make decisions based on the results of the assessments.	General	Performing the tasks associated with contractor and consignee operations efficiently.		S	Expected results, problems, risks, etc., must be carefully considered before concluding the consignment or entrustment. This step is necessary to accomplish the purposes of the consignment or entrustment operations project completely.
5.2	Selection of the Service Provider of Consignment Business	General				
(1)	Define selection criteria of service providers.	General	Selecting a consignee based on the plan for operations as a contractor.	3-(4)-①-C	C	To select a consignee based on the plan for operations as a contractor, the criteria for selecting a consignee must be clarified.
(2)	Present requirement specifications to candidate service providers.	General	Clarifying the conditions for working as a consignee when preparing a proposal.		S	Required specifications must be presented to a candidate contractor to clarify the conditions for working as a consignee when preparing a proposal.
(3)	Assess proposals submitted by candidate service providers.	General	Selecting the most appropriate consignee in a fair manner.		S	To select the most appropriate consignee in a fair manner, proposals presented by candidate consignees must be compared and evaluated based

						on the criteria for selection.
5.3	Contracts	General				
(1)	Conclude contracts in compliance with the consignment contract rules and/or the entrustment contract rules.	General	Concluding a contract with a selected consignee.	3-(4)-①-E	C	A contract to be concluded with a consignee must be in accordance with the rules for concluding a contract as a contractor or the rules for concluding a contract as a consignee.
(2)	Define provisions concerning compliance.	General	Preventing the abuse or leakage of information and breach of privacy.	3-(4)-①-E	C	To prevent the abuse or leakage of information and breach of privacy, measures for preventing misconduct and protecting confidential information shall be clarified when concluding a contract.
(3)	Define whether to allow re-commission.	General	Preventing problems related to the reselection of consignees.		S	To prevent problems related to the reselection of consignees, whether the reselection of consignees is allowed must be clarified when concluding a contract.
(4)	Define the holders of the intellectual property rights.	General	Preventing problems related to intellectual property rights.		S	To prevent problems related to intellectual property rights, the ownership of intellectual property rights must be clarified when concluding a contract.
(5)	Define the special	General	Assuming the		S	To deal with problems that are

	agreement and disclaimer clauses.		occurrence of problems.			expected to occur, special agreement clauses and waiver clauses must be included in a contract.
(6)	Define details of services and the sharing of responsibilities.	General	Supporting a consignee in performing subcontracted operations smoothly.	3-(4)-①-F	C	The contents of subcontracted operations and the division of duties must be clarified in a contract and specifications so that a consignee can perform subcontracted operations smoothly.
(7)	Reexamine contents of the contract in case of additions to or changes in the contract.	General	Clarifying the contents of subcontracted operations and supporting a consignee in performing operations smoothly.		S	If there is a change in or addition to the contents of subcontracted operations after a contract is concluded, the contents of a contract must be reexamined to check the contents of subcontracted operations at a consignee and help the consignee perform operations smoothly.
(8)	Define policies for system audit.	General	Ensuring the reliability, safety, and efficiency of operations being performed by a consignee.		S	To ensure the reliability, safety, and efficiency of operations being performed at a consignee, the policy for system auditing must be included in a subcontracting contract.
5.4	Consignment	General				

(1)	Assess consistencies between the actual consigned business and the contracted business.	General	Having the actual consigned business without excess or shortage.	3-(4)-①-G	C	To allow a consignee to perform subcontracted operations without excess or shortage, the contents of subcontracted operations performed by a consignee must be in agreement with the contents described in a subcontracting contract.
(2)	Provide necessary specifications, data and other materials according to the contract.	General	Having a consignee perform subcontracted operations according to a plan for operations as a contractor.		S	To allow a consignee to perform subcontracted operations according to a plan for operations as a contractor, it is necessary to provide a consignee with the required specifications, data, materials, etc., based on a subcontracting contract.
(3)	Monitor progress of the consigned business, and take necessary measures against delay of the project.	General	Performing the consigned business according to a plan for operations as a consignee.	3-(4)-①-G	C	To allow a consignee to perform subcontracted operations as specified in a plan for operations as a contractor, the progress of subcontracted operations must be monitored, and measures must be implemented to avoid or deal with the risks properly.
(4)	Monitor the status of error prevention, fraud prevention and	General	Preventing mistakes, misconduct, leakage of confidential	3-(4)-①-E	C	To prevent mistakes, misconduct, leakage of information, breach of privacy,

	confidentiality protection at the consigned partners, and take measures as and when necessary.		information, breach of privacy, etc., as specified in a subcontracting contract.			etc., as specified in a subcontracting contract, the status of measures implemented to prevent mistakes and misconduct and to protect confidentiality must be monitored, and appropriate action must be taken as required.
(5)	Ensure that the acceptance of deliverables is carried out based on the consignment contract.	General	Confirming that the purposes of subcontracting have been accomplished.	3-(4)-①-H	C	Products must be subjected to a receiving inspection based on a subcontracting contract to see if the purposes of subcontracting are accomplished.
(6)	Ensure that the restitution and/or disposal of data and materials that are provided for the consignment are properly executed after completion of the consigned services.	General	Preventing unfair competition and protecting security after subcontracted operations are completed.		S	After subcontracted operations are completed, it must be confirmed that data, materials, etc., provided to a consignee to prevent unfair competition and protect confidentiality have been withdrawn or disposed of.
(7)	Assess and analyze results of the consigned services.	General	Reflecting the results of analysis and evaluation in the next plan for operations as a contractor and in selecting consignees.		S	To reflect the results of analysis and evaluation in future plans for operations as a contractor and in selecting consignees, it is necessary to analyze and evaluate the results of subcontracted operations performed.

5.5	Entrustment	Company				
(1)	Ensure that the actual entrusted business is consistent with the contracted provisions.	Company	Having the actual entrusted business without excess or shortage.		S	To act entrusted business without excess or shortage, the contents of entrusted business must be in agreement with the contents described in a contract.
(2)	Monitor progress of the entrusted business, and take measures against potential risks.	Company	The entrusted business according to a plan for operations as a consignee.		S	To act entrusted business according to a plan for entrusted business, the progress of entrusted business must be monitored, and measures must be implemented to avoid or reduce the risks.
(3)	Implement a quality management process for deliverables.	Company	Managing the quality of products based on a contract as a consignee.		S	Quality management must be carried out by a consignee so that the quality of a product reaches the product acceptance standard specified in a contract as a consignee.
(4)	Ensure that restitution and/or disposal of data, materials and other resources supplied from the contracted party are properly executed in accordance with the contract, after the completion of the	Company	Preventing unfair competition and protecting confidentiality after operations are completed.		S	After operations are completed, it must be verified that data, materials, etc., provided by a contractor to prevent misconduct and protect confidentiality have been withdrawn or disposed of.

	contracted business.					
6	Change Management					
6.1	Change Management	General				
(1)	Define change management rules, and obtain approval of the rules from the appropriate stakeholders and the responsible personnel in the development department and the maintenance departments.	General	Making changes smoothly and effectively.	3-(1)-㉓-A	C	Change management rules and a change procedure are required to make changes smoothly and effectively, and must be approved by persons in charge at user, development, and maintenance departments. Large changes must be controlled by a development department on the system management standard.
(2)	Ensure that the decisions made for change management issues appropriately take into account impacts on other systems, in case of modifications to specifications, problems, unresolved issues and so on.	General	Not disturbing the smooth operation of an information system in operation.		S	How changes in case of modifications to specifications, problems, unresolved issues, and so on., should be handled through change management issues must be determined with consideration given to the effects on other systems by taking care not to hamper the smooth operation of the information system.
(3)	Track change management issues from the proposal to its completion, and	General	Making the changes necessary for organizational operations at the	3-(1)-㉓-E	C	The progress of matters being processed through change management issues must be monitored from when proposals

	periodically analyze uncompleted issues.		appropriate times.			are made to when the matters are resolved to ensure that the changes necessary for organizational operations are being made at the appropriate times. Matters that remain unresolved must be analyzed periodically.
6.2	Implement Change Management	General				
(1)	Implement change management issues in compliance with change management rules.	General	Carrying out change management smoothly and safely.		S	Change management issues must be carried out in accordance with the change management rules so that changes can be made smoothly and safely.
(2)	Ensure that the environment of other related systems is changed simultaneously when implementing change management issues.	General	Avoiding system problems caused by a change, and making changes efficiently.	3-(1)-③-B	C	If a change has been made to a matter to be handled by change management issues, a change must also be made to the environment of a related information system to prevent the change from causing problems to the information system and to make the change efficiently.
(3)	Obtain approval of the results of change	General	Confirming that a change has been made	3-(1)-③-D	C	It must be verified that a change has been made as specified by a

	management issues from the appropriate stakeholders and the responsible personnel in the development department, the operation department and the maintenance department.		as specified by a change request.			change request, and the change must be approved by persons in charge at user, development, and maintenance departments.
7	Disaster Recovery					
7.1	Risk analysis					
(1)	Assess potential risks such as earthquakes and the range of impacts on the information system.	–	Presenting the countermeasures for protecting an information system from a disaster or an act of terrorism.			To illustrate what actions are taken to protect information systems from a disaster or an act of terrorism, it is necessary to clarify the types of risks, including earthquake, flood, terrorism, etc., and the extent of the impact on information systems.
(2)	Analyze potential damage to the organization suffered from a shutdown of the information system and so on.	–	Clarifying the importance and urgency of recovering operations relative to the magnitude of a disaster.			To clarify the importance and urgency of recovering operations relative to the magnitude of a disaster, the extent of loss caused to an organization due to the breakdown of an information system must be analyzed.
(3)	Assess the acceptable	–	Minimizing the			The allowable operation

	recovery time for each business processes and prioritize them.		suspension of operations caused by a disaster and the resultant effects, and recovering information systems efficiently			recovery time and the order of priority of recovery must be determined to minimize the suspension of operations caused by a disaster and the resultant effects and to achieve efficient recovery.
7.2	Contingency Plan	General				
(1)	Develop contingency plans based on risk analysis and ensure that the plan is consistent with the business continuity plan.	General	Implementing appropriate countermeasures quickly and efficiently and minimizing confusion if a disaster occurs.			A disaster contingency plan must be formulated by ensuring consistency with the business continuity plan so that appropriate actions can be taken quickly with the least confusion if a disaster occurs.
(2)	Obtain approval for the contingency plan from the top management of the organization.	General	Taking appropriate actions quickly with the least confusion if a disaster occurs.			The top management of an organization must approve the contingency plan to make it fully understood by the people concerned so that appropriate measures can be implemented quickly with the minimum possible confusion if a disaster occurs.
(3)	Assess the feasibility of the contingency plan.	General	Ensuring the continuity of operations in a way commensurate with the degree of damage, and			To ensure the continuity of operations in a way commensurate with the degree of damage and to achieve

			achieving recovery in a reliable manner.			recovery in a reliable manner, it is necessary to confirm the feasibility of the contingency plan.
(4)	Define educational training policies for employees in the contingency plan.	General	Having a good understanding of the countermeasures specified in the contingency plan, and implementing them in a reliable, efficient manner.			To have a good understanding of the countermeasures specified in the contingency plan and to implement them in a reliable manner, the policy for employee education and training must be clarified, and education and training must be provided periodically based on the contingency plan.
(5)	Communicate and inform related departments of the contingency plan.	General	Having a good understanding of the countermeasures specified in the contingency plan, and implementing them in a reliable, efficient manner.			To have a good understanding of the countermeasures specified in the contingency plan and to implement them in a reliable manner, education and training must be provided based on the contingency plan, and the contents of the countermeasures must be made fully understood by all departments concerned.
(6)	Update the contingency plan regularly and ensure that the plan is kept up to date.	General	Maintaining the feasibility of the contingency plan by modifying its contents to cope with changes in			As the business and operation environments change, the contingency plan must be reviewed at the appropriate times to maintain feasibility.

			the business and operation environments.			
7.3	Backups	General				
(1)	Define methods and procedures for backing up the system, data and forget necessary resources to meet the recovery objectives of the businesses.	General	Recovering an information system in a reliable manner with consideration given to recovery work efficiency and the cost efficiency of recovery work.	3-(2)-③-D	C	To recover an information system from failure in a reliable manner with consideration given to recovery work efficiency and the cost efficiency of recovery work, it is necessary to establish backup methods and procedures with consideration given to operation recovery goals.
(2)	Assess and confirm the backup methods and procedures by the responsible personnel in the operations department.		Recovering an information system in a reliable manner.	3-(2)-③-D	C	To verify the feasibility of backup methods and procedures established, a person responsible for the operation of an information system must verify the appropriateness of the backup methods and procedures.
7.4	Alternative Operations and Recovery	General				
(1)	Define and assess alternative processing procedures and structures until resumption. This	General	Continuing operations by using alternative methods until an information system is			Alternative processing procedures and structures must be established to continue operations until an information

	task should be conducted by the appropriate stakeholders and the responsible personnel in the operations department.		recovered from failure.			system is recovered from failure. Persons in charge at user and operation departments must verify the feasibility of the alternative processing procedures and structures.
(2)	Define and assess recovery procedures and structures. This task should be done by the appropriate stakeholders and the responsible personnel in the operations department.	General	Recovering an information system from failure in a smooth, reliable manner.	3-(2)-③-E	C	Recovery procedures and structures must be established to recover a failed information system in a smooth, reliable manner. Persons in charge at user and operation departments shall verify the feasibility of the recovery procedures and structures.

Appendix 3 Examples of IT controls and IT

1. Prevention and indication of input errors

(1) Input screen functions for preventing input errors

Typical functions are as follows:

- ① Showing a pull-down menu so that the operator who inputs data makes a choice instead of inputting a code on the keyboard
- ② Showing a pull-down menu of part numbers related to specific customers or suppliers to narrow the scope of selection in inputting data
- ③ Showing the items most recently inputted by a specific operator or the items that he or she inputs with a high degree of frequency
- ④ Limiting the range of codes that can be inputted according to the scope of responsibilities assigned to each operator
- ⑤ Showing a warning if a specific operator inputs a code or abnormal value that he or she has never inputted before

(2) Program functions for preventing input errors

A program validates data when data is input on the input screen or when it performs an input data acceptance process (data received from outside suppliers is included in the data processed by this acceptance process). The main functions of this program are shown in Table 3-1 below.

Table 3-1 Program's functions for preventing and indicating input errors

Function	Description
Checking the completeness of data processing	<p>Data that is lost or data that is mistakenly left unprocessed are detected based on the number of data processed, control totals, hash totals, results of sequential number checks, etc.</p> <p>Notes:</p> <ol style="list-style-type: none">1. Control totaling is checking for omissions or overlaps in a particular processing step by comparing the total amount of money calculated before and after this processing step, as well as hash total, the number of records, etc.2. Hash totaling is checking data for completeness by totaling the numerical values, totaling of which is usually meaningless. For example, the total quantity of a certain part number (if the part number is expressed as a number) shown on original input forms is calculated manually, and this total quantity calculated is compared with the total quantity of the same part number shown on the screen during data input.
Performing	Incorrect data is prevented from be mixed in by performing

arithmetic calculation checks	<p>limit value checking, crossfooting, balance checking, etc.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Limit value checking is checking to see if input data deviates from the predetermined range of values. 2. Crossfooting is checking data for the consistency between a total in the vertical direction and that in the horizontal direction. In payroll calculations, for example, a gross pay, total deduction and take-home pay are calculated, and the total take-home pay is validated as against the total take-home pay calculated by subtracting total deduction from gross pay. Crossfooting is similar to this payroll calculation. 3. Balance checking is checking to see if a total debit is equal to a total credit in journalizing in an accounting procedure.
Using check digits	<p>Numerical values (check digits) are embedded into codes to allow a program to detect mistakenly inputted codes or prevent incorrect codes from being inputted.</p> <p>Note: Check digits are used to prevent incorrect codes from being inputted. Specifically, the value of a sequence of five digits, from the first to the fifth digits, of a six-digit code is calculated, and a value calculated from this five-digit value is put into the sixth digit of this six-digit code to verify the validity of the input code.</p>
Checking the data format	<p>A blank test, a test to discern a numerical value or a character, a sign test, etc., are conducted to detect the data containing errors or to prevent different types of data from mixing.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. A blank test is for checking to see if data is mistakenly inputted into a space that should always be a blank space. 2. A sign test is for checking to see if positive numerical data designated as always being positive is input as negative numerical data or vice versa.
Checking the logical reasonableness	<p>The relationships between pieces of inputted data are checked, and only the data that is logically reasonable is accepted.</p>
Checking input data against predefined control values	<p>Input data is checked against registered credit limits, payment limits, quantity limits, unit price limits, etc., so that data larger or smaller than a specified limit is not accepted.</p>
Checking input data against related files	<p>Purchase data is collated with data in ordering files, data on shipping orders are collated with data in files of accepted orders, etc., to verify the consistency between mutually related data.</p>

2. Preventing or indicating errors in the data processing process

A large volume of data is processed and totaled in the data processing process, and there are cases in which errors contained in the results of data processing remain unnoticed for a long time.

Functions for preventing or indicating errors in data must be provided to maintain the accuracy, completeness and file continuity of information processing operations. Table 3-2 shows these functions.

Table 3-2 Functions for preventing or indicating errors in the data processing process

Function	Description
Indicating errors when data is updated, and conducting a follow-up	An error message is shown during an update of files of transaction data or other data if data cannot be updated with the conditions specified by the system design or if inconsistencies in data are detected. This is a basic function to be implemented by program design. Based on information given by an error message, the contents of data and those of related programs must be investigated to identify the cause of the error.
Automatically checking the consistency of the results of updating	The total number of data, total quantity, total amount, etc. of multiple files shown below are automatically collated to check the consistency of data between files so that the presence or absence of errors can be detected and thereby the accuracy and completeness of the results of updating can be ensured. ① Detail file containing the original data to be used for updating ② Contents of an update to be made to the file that is to be updated by the original data ③ Summary file containing the original data to be used for updating
Unifying information sources by integrating databases	Basic transaction data and aggregate data databases (itemized account, account balance, production results, stock, records of goods put into and taken out of storage, etc.) are unified, and various types of output information are output from a unified database so that the errors caused by the inconsistencies between files can be prevented.
Checking for the sameness between the totals and balance totals of output forms and those of summary files	Errors during the preparation of output forms are prevented by collating total values, total balances, etc., output to output forms with data in summary files.
Review of output	Output forms are reviewed by management personnel at a

forms conducted by managing personnel at a user department	user department or persons in charge of operation management who are familiar with the contents of data so that errors or inconsistencies in data can be detected.
--	--

3. Function for ensuring the relevance between application data and system data

This function is for ensuring the relevance (possibility of mutual tracing) between data related to financial reporting and data related to financial information. The relevance between data must be ensured to enable an automatic transfer (automatic journalizing, automatic coordination, etc.) of data between applications and systems. Table 3-3 shows examples of how data is cross-referenced.

Table 3-3 Function for ensuring the relevance between application data and system data

Function	Description
Individual reference method	The individual reference method is used to allow applications and systems to recognize their individual reference counterparts. In this case, serial numbers, form numbers (same numbers or same numbers with sub-numbers), etc., are recorded on both application and system data to ensure the relevance between data.
Total reference method	If the result of totaling in a certain application or system must be transferred to another application or system, the total reference method is used to allow the application or system to recognize its reference counterpart by recording its own information (application or system, the range of totaling, etc.) in that counterpart. In the case of this method, the relevance is maintained by recording the items to be totaled (account titles, departments, etc.), the period during which totals are calculated, etc., in transferred data of an application or system as abstracts in textual form or by recording the ID of an application or system from which data is to be transferred, automatic journalizing patterns, etc.

Appendix 4 Recording the assessment procedure, etc.

1. Records of IT controls

Items shown below shall be recorded to demonstrate that appropriate IT controls are placed in operation and operated properly and that the status of IT controls in operation has been assessed in an appropriate manner. Although only IT controls are described in this appendix, not only IT controls but also overall internal controls must be described in management's assessments.

- ① Policies and procedures for the introduction and operation of IT controls over financial reporting
- ② Status of the introduction and operation of each assessment item to be adopted by management when the company-level IT controls are assessed
- ③ Outline of operation processes related to important account titles and items to be disclosed (including the system flows of each operation process, outline of IT application controls, listing of systems used, etc.)
- ④ Risks of important deceptive indications occurring in each operation process, and the contents of IT controls carried out to reduce involved risks
- ⑤ Status of the introduction and operation of IT controls concerning (4) above
- ⑥ Procedure for making an assessment of the effectiveness of IT controls over financial reporting, assessment results, identified shortcomings, and measures taken to correct the shortcomings
- ⑦ Records of assessment plans
- ⑧ Records of a decision made concerning the range of assessment (including a method for determining the range of assessment, and the grounds for adopting the method)
- ⑨ Procedure for making an assessment of implemented IT controls, and records of assessment results, corrective measures, etc.

(⇒ II 3 ⑦, Practice Standards)

2. Keeping records

The range of internal control records related to financial reporting to be kept, a method for records keeping, a period during which records are kept shall be determined through a proper judgment of each company with consideration given to the relationships with vouchers. It is recommended that these records be kept for a period identical to the inspection period (5 years, etc.) of annual security reports and attached documents, based on an appropriate range of records by using an appropriate method of records keeping (magnetic media, paper, film, etc.).

(⇒ II 3 (7) ②, Practice Standards)

If electronic media are used, there is the possibility that records may be overwritten or deleted after assessment due to errors in the system setting. Additionally, records shall be kept properly and safely with consideration of intentional falsification. Assessment results, related documentary evidence, etc., shall also be kept properly and safely. For example, related documentary evidence can be printed on sheets of

paper or stored on the type of media that cannot be overwritten. To prevent the falsification of records, it will be possible to introduce electronic signatures.

The results of management' assessment shall be recorded so that auditors can review them at a later date.

Prior discussions with auditors shall be held to determine how assessment results should be retained, to what extent the documentary evidence used for assessment should be retained, how the documentary evidence should be stored (for example, printing on paper or such electronic media as CD-ROMs, etc., whether measures should be taken to prevent falsification, and so forth.)

Appendix 5 Sampling

1. Points to notice when conducting sampling

The following two points shall be considered when determining a method for making an assessment of the status of internal controls in operation processes (the number of sampled cases, the period during which sampling is conducted, etc.).

- ① Forms and features of internal controls, etc.
- ② Account settlement and financial reporting processes

Concerning the forms and features of internal controls, the following shall be considered when determining a method for making an assessment of the status of internal controls:

- a. Importance of internal controls
- b. Complexity of internal controls
- c. Nature of judgment made by persons in charge
- d. Ability of persons who carry out internal controls

Because IT controls are carried out by performing a set of operations repeatedly in a consistent manner, the amount of assessment work can usually be decreased if IT controls are considered to be operating effectively, on the condition that IT general controls are also working effectively; specifically, the number of cases to be sampled can be decreased (the number of operations performed by personnel should remain the same), the period during which cases are sampled can be shortened, etc.

(⇒ III 4 (2) ② C, Practice Standards)

2. Types of sampling

Types of sampling are generally classified into two as shown below, depending on what sample extraction method and estimation method are used.

- ① Statistical sampling
- ② Nonstatistical sampling (sampling based on the experience of persons who make assessments, etc.)

When estimating the conditions of the whole of a population, assessments are usually made by using a statistical sampling approach. Therefore, it is thought that statistical sampling will be used more frequently when making an assessment of the status of IT controls in operation. However, because a population is small during quarterly processing, monthly processing, weekly processing, etc., the amount of available data may not be sufficient and, therefore, means other than statistical sampling can be used.

3. Number of cases to be sampled

(1) If assessments are made manually

Although it is inappropriate to mention a proper number of cases to be sampled in a generalizing manner, the conditions of internal controls in operation processes may be assessed by referring to a table like Table 5-1, which shows the number of cases to be sampled and the allowable number of deviations. The frequency of sampling applies to the number of cases used to make an assessment of the conditions of internal operations; for example, the number of transactions.

Table 5-1 Example of the quantity of samples

Frequency of sampling	Number of cases to be sampled	Allowable number of deviations
Many samples in one day	25	0
Daily	25	0
Weekly	5	0
Monthly	2	0
Quarterly	2	0
Yearly	1	0

Table 5-1 shows that when making an assessment of the effectiveness of a population in which many internal controls are carried out daily, 25 cases should be sampled in a random manner, and internal controls should be considered to be working effectively if there is no one deviation in these 25 cases sampled. The number of cases to be sampled and the allowable number of deviations shown to the right of “Many samples in one day” and “Daily” were calculated by using a statistical method. If 25 cases are sampled from an infinitely large population and if no one deviation is found in these 25 cases, the number of deviations accounts for 9% or less of the total number of samples collected can be expressed as 90% confidence level. (⇒ III 4 (2) ① B a, Practice Standards) In Table 5-1, the number of cases to be sampled and the allowable number of deviations shown to the right of “Weekly,” “Monthly,” “Quarterly,” and “Yearly” are calculated using a means other than a statistical method.

Although IT general controls do not have a direct effect on misstatements concerning financial reporting, they guarantee that the IT application controls are working effectively and, therefore, the amount of work expended to validate application systems based on each IT application control will be able to be lessened. In this case, the number of cases to be sampled can be determined by using information in Table 5-1 as reference information.

(2) If internal controls are automated

Once internal controls are placed in operation, IT controls continue functioning in a consistent manner until the time when a change or error occurs. Therefore, operation tests can be conducted based on the policies shown in Table 5-2. (⇒ II 3 (3) ⑤ D c, Practice Standards)

Table 5-2 Operation tests for automated internal controls

Condition	Operation test
<ul style="list-style-type: none"> • It is considered from the results of assessments made on the status of introduction and operation of related general controls that general controls are working effectively. 	<p>One application is validated with respect to one IT-related application control.</p>
<p>In addition to the above condition, the following three conditions are applicable:</p> <ul style="list-style-type: none"> • Shortcomings in internal controls were not found in the previous year. • A change is not made to internal controls after they are assessed the last time. • Failure, errors and other problems have not occurred. 	<p>The fact that internal controls conform to all four conditions is recorded, and the results of internal controls assessments made in the previous year are used as is.</p>

Appendix 6 Example of the risk control matrix

This appendix describes the risk control matrix concerning company-level IT controls, IT general controls and IT application controls.

1. Items of the risk control matrix

To support a company in using the risk control matrix, a table is provided so that a company can make an assessment of each control item of IT application controls, company-level IT controls and IT general controls. This table exemplifies risks, control objectives, actual control conditions, whether controls are newly introduced or are already in place and operating, prevention or detection through controls, automated or manual controls, assertion, control frequency, control assessment procedure, items to be assessed and detected, related audit working paper, assessment results, etc. All this information is provided as examples. Based on these examples, a company should customize the table in a way that suits its needs and conditions.

- **Risks:** Risks of misstatement being made in financial reporting are described. Types of risk that should be of interest for companies are listed.
- **Control objectives:** Control objectives for each types of risk (system management standard) are described.
- **Situation of controls (control activities):** The situation of applicable controls at companies are outlined.
- **Placed in operation or now in operation:** Whether controls are newly introduced or now in operation is indicated.
- **Frequency:** The frequency with which controls are carried out (quarterly, yearly, monthly, weekly, daily, etc.) is shown.
- **Automated or manual:** Whether control objectives are achieved through an automated IT system or a combination of IT and manual work is shown.
- **Items to be assessed:** IT application controls to be assessed are shown; specifically, completeness, existence, period allocation, attribution of rights and duties, valuation, and presentation (indication).
- **Control assessment procedure:** What kind of control assessments is made is shown as a procedure.
- **Assessments and items to be detected:** The results of assessment are entered. If a problem is noted, the contents of the problem are entered.
- **Document number:** Documents and forms (including electronic media) used to record the results of control assessments are shown.
- **Assessment results:** Whether the target risks have been reduced or not is entered. If the risks are considered high, a review of control items must be made.

2. How to use the risk control matrix

The risk control matrix should be used as follows:

- ① Enter the name of a specific risk.

- ② Enter the controls being carried out (or to be constructed), and enter information on related items in the risk control matrix.
- ③ Understand the situation of controls, and make an overview of what assessment items should be addressed. To assess the status of controls, enter information in the control assessment procedure, and carry out an assessment of controls.
- ④ To assess the status of controls, whether the assumed risks about selected control items have been reduced or not is examined.
- ⑤ To construct controls, make a list of candidate control items, and select the most appropriate control items that will enable the reduction of risks.
- ⑥ Enter the results of assessment in the assessment space and the space for matters detected, and enter reduced risks in the assessment result space on the extreme right.

Appendix 6-1

Company-level IT control assessment

Company name		Originator and data created							
Settlement term		Official position and name of a person who answered questions							
Basic element	Risk	Control objectives	No.	Situation of controls	Placed in operation or now in operation	Control assessment procedure (to be assessed from the aspects of documentation, education, level of understanding on the part of personnel, system, implementation, monitoring, and improvement).	Assessment and items detected (If there are detected items, what effects they will produce must be clarified)	Document number	Assessment result
Control environment	Because an approach to the introduction of IT is not organizational or systematic, the reliability of financial reporting is impaired.	The management shall establish the strategies and plans for dealing with IT concerning financial reporting and financial information.		IT-related policies concerning financial reporting are described in an annual business management plan, and are approved by the management council and the board of directors.	Placed in operation, now in operation	It must be confirmed that the management's policy for IT is described in an annual business management plan, and is approved by the management council and the board of directors.		Omitted	Low
	IT concerning financial reporting is not addressed properly due to organizational weaknesses in handling IT-related matters.	A companywide organization is established to establish IT-related policies and plans, and it is being operated effectively.		A computerization committee is established to determine specific IT-related policies and implement them.	Placed in operation	The "computerization committee rules" and the "list of committee members" were reviewed. Based on the results of this review, the standing and functions of the committee were identified, and it was confirmed that the committee is organized by the members capable of company-wide coordination and adjustment.		Omitted	Low
				A computerization committee is managed effectively.	Now in operation	By reviewing the meeting minutes of the computerization committee, it must be verified that specific IT-related policies are discussed and necessary actions are taken based on the results of discussions.		Omitted	Low
	The rest is omitted.								
Assessment and handling of risks									
Control activities									
Information and communication									
Monitoring									

Appendix 6-2

IT general control assessment

Risk	Control objective	No.	Situation of controls	Placed in operation or now in operation	Prevention or detection	Manual or automated	Placed in operation			Frequency	Control assessment procedure	Assessed and detected items (if there are detected items, what effects they will produce must be clarified)	Document number	Assessment result	
							Document	Process	System implementation						
	Point to notice														
Because a system affecting the reliability of financial information is not developed and procured properly, confidence cannot be put in the financial information generated by the system.	Development		Check that malicious programs are not embedded into a system during system development or that there are no mistakes in the results of processing operations performed by the system	Standardized policies and procedures for system development are in place. Based on the policies and procedures, IT is developed and updated.	Placed in operation	Prevention	Manual work	<input type="radio"/>	<input type="radio"/>	NA	Quarterly	It was verified that the system to be assessed is developed in accordance with standardized procedures and documents.	None	Omitted	Low
			Check that no intentional misconduct is committed and all processing tasks are programmed into a system with no mistakes.	In the system development process, a system is so constructed as to enable it to achieve the reliability of financial information, specifically financial information's validity, integrity and accuracy.	Now in operation	Prevention	Manual work	<input type="radio"/>	<input type="radio"/>	NA	Quarterly	It was verified based on the results of reviews of development specifications, basic design documents (conceptual design documents), etc., that control functions are integrated into the system to ensure the reliability of financial information.	None	Omitted	Low
			The rest is omitted.												
If maintenance is not conducted properly, the reliability of application controls is lost.	Maintenance		Check that a program is not altered or changed without authorization.	System change management and system maintenance management are carried out in accordance with the change management procedure (standardized, recorded, approved, and documented).	Placed in operation or now in operation	Detected	Manual work	<input type="radio"/>	<input type="radio"/>	NA	Monthly Weekly	It was confirmed that the change management rules are in place. It was also confirmed that changes are managed according to the change management rules by conducting tests on 25 cases.	Although the absence of evidence of approval was noted with one out of 25 cases, it was explained that a person in charge mistakenly left the space for affixing a seal blank and, therefore, approval is actually given. As a result of conducting another test on additional 25 cases, there was no case of the space for affixing a seal being left blank. It was judged, therefore, that the absence of evidence of approval found is due to a simple mistake of not affixing a seal caused by a lack of care.	Omitted	Low
			The rest is omitted.												

Appendix 6-3

IT application control assessment

Company name	XX Company, Ltd.
Settlement term	Year and date
Location	Order receiving center
Transaction cycle	Sales cycle
Function	Order receiving
Related account titles	Amount of sales, account receivable

Completeness	Existence or occurrence	Allocation	Rights and obligations	Valuation	Presentation and disclosure
--------------	-------------------------	------------	------------------------	-----------	-----------------------------

Originator and date created	◇◇◇◇2006/12/23
Person who checked the contents, and date checked	□□□□2007/1/24

Risk	Control objective	No.	Main control activities	Automated Manual	Frequency	Requirement						Placed in operation Now in operation	Control assessment procedure	Assessed and detected items (If there are detected items, what effects they will produce must be clarified)	Document number	Assessment result

Omissions or overlaps occur in financial information	Completeness	Are all orders received recorded without omissions or overlaps?	No.	Main control activities	Automated Manual	Frequency	Completeness	Existence or occurrence	Allocation	Rights and obligations	Valuation	Presentation and disclosure	Placed in operation Now in operation	Control assessment procedure	Assessed and detected items (If there are detected items, what effects they will produce must be clarified)	Document number	Assessment result
						1	The order receiving operations using EDI are controlled by performing the JCA procedure. If illicit data transmission is attempted, mail is sent to a person responsible for the system operations.	Automated	Quarterly	○	NA	○	NA	NA	NA	Placed in operation Now in operation	Select a particular month, and check that the system operation report is reviewed, abnormal termination is reported to a person in charge according to the JCA procedure, and a follow-up is conducted.
			2	A facsimile transmission is received at the call center. After it is received, one person enters a serial number, and then outputs a proof list. Another person checks the contents of the proof list against the received facsimile transmission.	Automated Manual	day	○	NA	NA	NA	NA	NA	Now in operation	Select 25 cases in a particular month, and check that the collation with the proof list is carried out.	None	Omitted	Low
			3	Only the orders to which goods in stock are allocated can be registered in a delivery order file. Persons at a sales department shown in a back order file conduct a follow-up of each back order to which goods in stock are not allocated until each ordered quantity is delivered in full to customers.	Automated Manual	day	○	○	NA	NA	×	NA	Placed in operation Now in operation	Check that persons in charge at a sales department conduct a follow-up of each back order in the back order file until each ordered quantity is delivered in full to customers.	None	Omitted	Low
Financial information cannot be recorded correctly	Accuracy	Are there any mistakes in the status of registration of orders received?	4	Orders received by EDI are checked for existence by referring to the customer master and merchandise master. If errors are found, an error file is created, the data with which an error was found is sent to a customer, and the customer is requested to resend the order. The error file is retained until the customer sends corrected data.	Automated	day	NA	○	NA	○	○	NA	Placed in operation Now in operation	Select 25 cases in a particular month, and check the situation of error file processing.	None	Omitted	Low
			5	A facsimile transmission is received at the call center. After it is received, one person enters a serial number, and then outputs a proof list. Another person checks the contents of the proof list against the received facsimile transmission. (Same as in 2 above)	Automated Manual	day	NA	○	NA	○	○	NA	Placed in operation Now in operation	Select 25 cases in a particular month, and check that the collation with the proof list is carried out. (Same as in 2 above)	None	Omitted	Low
			6	The date when an order is received is generated by the system, and registered.	Automated	day	NA	○	○	NA	NA	NA	Placed in operation Now in operation	Check the date-of-sale setting, and confirm that the date in the data on sales is generated by the system.	None	Omitted	Low
			7	If a customer code is input, the name of a customer is loaded from the customer master.	Automated	day	NA	○	○	NA	○	○	NA	Placed in operation Now in operation	Check that a customer name can be registered by inputting a customer code on the screen.	None	Omitted

False financial information is recorded	Validity	Aren't invalid orders registered?	8	Unit prices registered for each customer in the customer master are automatically loaded. These unit prices cannot be changed on order receiving terminals.	Auto mated	day	NA	○	NA	NA	○	NA	Placed in operation Now in operation	Check that a unit price is automatically registered and cannot be changed by inputting data on the keyboard.	None	Omitt ed	Low
			9	Customers other than those registered in the customer master cannot be registered.	Auto mated	day	NA	○	NA	○	NA	NA	Placed in operation Now in operation	Check that only the customers registered in the customer master can be registered (check the setting in the master registration).	None	Omitt ed	Low
			10	Unit prices registered for each customer in the customer master are automatically loaded.	Auto mated	day	x	○	NA	○	○	NA	Placed in operation Now in operation	Check that registered unit prices are automatically input and they cannot be input on the keyboard (check registered unit prices in the master registration).	None	Omitt ed	Low
			11	The input of orders received is controlled by the ID and password assigned to each person in charge.	Automated	day	NA	○	NA	NA	NA	NA	Placed in operation Now in operation	Check that the screen for order receiving can be opened only if the ID and password of a person in charge are input. Note: In the case of single sign-on, the password setting must be checked by using general controls. However, to verify that the authority to access the sales system can be established in the same way as the operation-related authority, application controls must be used.	None	Omitted	Low
			12	If the amount of an order received exceeds the credit limit of a customer, such an order cannot be input.	Auto mated	Quart erly	NA	○	NA	NA	NA	NA	Placed in operation Now in operation	Check that an order cannot be input if its amount exceeds the specified credit limit.	None	Omitt ed	Low
			13	Omitted										Omitted			
Financial information is not kept up to date, and cannot be used in a continuous manner.	Continuity	Isn't data in a file of received orders changed with malicious intent?	14	A change in data in a file of received orders is controlled by the ID and password assigned to each person in charge.	Automat ed	Quarterly	○	○	○	○	○	NA	Placed in operation Now in operation	Check that only persons in charge can access a file of received orders. (If databases are integrated, there are cases in which the authority to access to a file of received orders is checked by using general controls.)	None	Omitted	Low
			15	Logs of access to a file of received orders are monitored.	Automated Manual	Quarterly	NA	○	NA	NA	NA	NA	Placed in operation Now in operation	Check that the logs of access to master data are monitored according to specified conditions. (Although there are cases in which access logs are monitored through general controls, it should be noted that the range of monitoring can be narrowed by monitoring them through application controls.)	None	Omitted	Low
			16	The inventory master is collated with the master at the distribution center by batch processing every night to prevent a mismatch between data of these two masters.	Auto mated	Quart erly	○	○	NA	NA	NA	NA	Placed in operation Now in operation	Check that the inventory master is replaced. (There are cases in which the normal completion of batch processing can be checked by using general controls.)	None	Omitt ed	Low