p. 1

System Management Standards

Proposed on October 8, 2004

Preface

Today, the information system of an organization works as an important infrastructure of the organization to implement its management strategies. In addition, networks of individual information systems compose an essential social system. Meanwhile, information systems are increasingly becoming more diversified and complex, and consequently, various risks are becoming higher than ever. Stakeholders of information systems have become not only limited to the organization, but have expanded to include the general public. Therefore, it has become a crucial managerial challenge for organizations to properly control risks concerning their information systems. Under these circumstances, system auditing is an effective means to ensure appropriate control over such risks. System auditing also contributes to the realization of better IT governance and better accountability to stakeholders.

An organization properly establishes and operates its control over risks regarding the information system to fulfill the following objectives:

- To enable the information system to contribute to the organization in implementing its management policies and achieving strategic goals

- To enable the information system to achieve its objectives in a safe, effective and efficient manner

- To enable the information system to work to maintain the reliability of both disclosed and internal information

- To make the information system compliant with relevant laws and regulations, contracts and internal rules

The System Management Standards provide practical guidance for organizations to establish strategic IT plans based on management strategies, to design and implement appropriate control to improve the effectiveness of IT investment, and to reduce the risks based on the IT strategic plan over the system life cycle from planning to development, operation and maintenance.

The System Management Standards provide criteria on which the auditor should in principle base his/her audit judgments, when he/she performs system audits based on the System Audit

Standards, the companion volume of these Management Standards. It is also recommended for each authority to select the necessary standards or define unique standards that are in line with the philosophy and structure of this standard, based on the characteristics of the industry and individual business. Furthermore, such authorities are also advised to stipulate more detailed sub-control requirements, considering and reflecting current trends in related technologies, applicable laws and regulations, and social rules.

When performing an audit to ensure system security, the auditor is required to perform an information security audit based on the Information Security Audit System. Meanwhile, although the System Management Standards contain items to ensure information security, it is desirable to perform audits based on the Information Security Management Standards.

p. 2

System Management Guidelines (287 items)

I. Strategic IT Plan (47)

1. Overall optimization (18)

1.1 Policies on and goals of overall optimization (6)

(1) Define policies on IT governance.

(2) Define principles for use of IT and IT investment allocation.

(3) The goals of the information systems overall optimization should be based on business strategies.

(4) Define the model of the information system for the organization.

(5) Define policies on organizational structure and business process changes caused by introducing the new system.

(6) Define primary policies on information security.

1.2 Approval of the overall optimization plan (3)

(1) Obtain approval on the organizational structure to develop the overall optimization plan from the management.

(2) Obtain approval on the overall optimization plan from the management.

(3) Obtain agreement of related stakeholders on the overall optimization plan.

1.3 Development of the overall optimization plan (7)

(1) Create the overall optimization plan based on policies on and goals of the plan.

(2) Consider compliance requirements in the development of the overall optimization plan.

(3) The entire optimization plan should define policies on IT investments and necessary resources.

(4) Define how to measure the return and risks of IT investments in the overall optimization plan.

(5) Define rules for standardization and quality management policies for system development and operations in the entire optimization plan.

(6) Define rules to specify the priority of each development plan in the overall optimization plan.

(7) Consider the use of external resources in the entire optimization plan

1.4 Implementation of the overall optimization plan (2)

(1) Ensure that every stakeholder knows about the overall optimization plan.

(2) Review the overall optimization plan periodically and when changes occur in the business environment.

2. Organizational (9)

2.1 Computerization Committee (5)

(1) Clarify missions of the committee and allocate appropriate authorities and responsibilities to the committee based on the overall optimization plan.

(2) The committee should monitor all the activities concerning the information systems in the organization and implement necessary corrective measures.

(3) The committee should adopt the technology guidelines to stay current with trends in information technologies.

(4) The committee should report its activities to the management.

(5) The committee should provide to the management the information necessary for strategic decision support.

2.2 Information System Department (2)

(1) Clarify the missions of the information system department and allocate appropriate authority and responsibilities to the department.

p. 3

(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.

2.3 Human Resource Management polices (2)

(1) Identify the current status of human resources for IT and clarify necessary human resources.

(2) Clarify policies on sourcing and training of human resources.

3. IT Investments (6)

(1) Ensure that the IT investment plan is created in a manner consistent with corporate strategies.

(2) Compare multiple IT investment plan alternatives based on impact, effects, schedule and feasibility.

(3) Execute IT investment budgets properly.

(4) Establish the standard methodology for estimating the return on IT investments.

(5) Assess financial performance of the entire information system and individual projects, and take necessary actions to solve any problems.

(6) Review whether IT investments have been properly executed or not.

4. Policies on Information Asset Management (4)

(1) Define policies of information asset management and establish appropriate organizations.

(2) Assess risks for information assets, and take appropriate measures to reduce those risks.

(3) Consider efficient and effective use of information assets.

(4) Consider productivity improvement through information asset sharing.

5. Business Continuity Plan (5)

(1) Establish policies for ensuring business continuity of the information system.

(2) Establish the business continuity plan by all stakeholders, and obtain approval of the head of the organization for the plan.

(3) Ensure that policies for business continuity plan include employee training.

(4) Ensure that all necessary personnel in the relevant departments are reformed of the business continuity plan.

(5) Review the business continuity plan as and when necessary.

6. Compliance (5)

(1) Establish an organization for legal and regulatory compliance and appoint management for it.

(2) Identify applicable laws and regulations to the organization, and inform and educate stakeholders.

(3) Define the information ethics, and inform and educate related persons.

(4) Establish policies regarding processing of personal information, protection of intellectual property rights and for the provision of information disclosure..

(5) Assess level of compliance with laws, regulations, and the information ethics, and take necessary actions for improvement.

II. Planning processes (23)

1. Development Plans (9)

(1) Obtain approval for the development plan from the management.

(2) Establish the development plan considering its consistency with the overall optimization plan.

p. 4

(3) Define the development plan to specify its objective, target process, cost, system development structure and cost efficiency for investment.

(4) Define the development plan to include education and training programs for stakeholders.

(5) Define the development plan to specify the roles of the user department and of the information system development department.

(6) Define the development plan to indicate the cost calculation methodology for system development, operation and maintenance.

(7) Define the development plan to specify conditions for defining system life cycle.

(8) Ensure that the formulation and the system development methodology are defined based on a target scale and specific system requirements when designing the development plan.

(9) Ensure that a feasibility study with alternatives are studied to achieve the objectives of the information system when designing the development plan.

2. Analysis (8)

(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.

(2) Define target, scope and methodology for user requirement survey.

(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.

(4) Ensure that user requirements are documented and confirmed by the user department.

(5) Analyze potential risks in introducing the information system.

(6) Ensure that affected business processes, management structures and rules/procedures are reviewed and assessed regarding the introduction of the information system.

(7) Assess the effectiveness from both qualitative and quantitative perspectives when introducing the information system

(8) Ensure that suitability with user requirements is assessed before implementing software packages.

3. Acquisition (6)

(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.

(2) Ensure that hardware, software and networking products are acquired based on the procurement requirements.

(3) Ensure that necessary staff members, budgets, facilities and periods are prepared for completing system development.

(4) Ensure that skills required for staff members are specified clearly.

(5) Ensure that hardware, software and networking products are procured in accordance with procurement rules.

(6) Ensure that acquired resources are managed in accordance with acquisition rules.

III. System Development (49)

1. System Development Methodology (4)

(1) Obtain approval for System Development Methodology from the responsible personnel in the system development department.

(2) Define development procedures based on the system development methodology.

(3) Determine system development procedures considering the size of system development and characteristics of the system.

(4) Assess potential risks of system development, and take necessary actions.

2. System Design Phase (15)

(1) Obtain approval for system design documentation from the user department, the system development department, the operation department and the application maintenance department.

(2) Define basic policies on operations and application maintenance before starting design procedures.

(3) Ensure that input-output screens and print out formats should be considered convenient for the users of the system.

p. 5

(4) Ensure that the databases are designed based on the business processes and characteristics of the system.

(5) Ensure data integrity.

(6) Ensure that the network is designed based on business processes and the characteristics of the system.

(7) Ensure that the performance criteria of the information system meets the defined requirements.

(8) Ensure that operability and maintainability are considered in the information system design.

(9) Ensure that inter-operability with other information systems is considered for the information system design.

(10) Ensure that potential incidents are considered in the information system design.

(11) Ensure that error prevention, fraud prevention and information security are considered in the information system design.

(12) Ensure that the test plan has a clearly specified objective, scope, methodology and schedule.

(13) Establish policies on user training, the course plan and the schedule for the information system.

(14) Ensure that monitoring functions are considered in the system design phase.

(15) Review documentation for the system design.

3. Program Design Phase (5)

(1) Obtain approval for program design documentation from the responsible personnel for system development (project manager).

(2) Design programs based on the system design documentation.

(3) Define and document the test requirements.

(4) Review program design documents and the test requirements.

(5) Return to the system design phase to resolve contradictions in the system design found during program design.

4. Programming Phase (4)

(1) Perform programming based on the specifications of the program design documentations.

(2) Ensure that programming activity complies with the coding standards.

(3) Ensure that the program codes and test results are assessed properly, recorded and stored.

(4) Ensure that important programs are tested by someone other than the software develope.

5. System Tests and User-acceptance Tests Phase (13)

(1) Obtain approval for the system test plan from the responsible personnel for the software development project and the test leader.

(2) Obtain approval for the user-acceptance test plan from the responsible personnel in the user department and the system development department.

(3) Prepare potential test cases covering all the system requirements for system tests.

(4) Prepare test data and perform system tests in accordance with the test plan.

(5) Ensure that system tests are performed 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.

(7) Ensure that appropriate testing methodologies and standards for system tests are used.

(8) Ensure that the user acceptance test is performed in an environment similar to the production environment.

(9) Prepare test cases based on user manuals and simulate the live processes in the user-acceptance tests.

(10) Ensure that personnel from the user department and the operation department are involved in user-acceptance tests, and that they review the user-acceptance test results.

(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.

(12) Ensure that the progress and results of the system tests and the user-acceptance tests are documented, recorded and stored.

p. 6

(13) Ensure that the software package developer has tested the quality of the software before implementing the package.

6. Promotion to Production (8)

(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.

(2) Document the promotion processes, and obtain approval from the system operation department.

(3) Define the criteria for the completion of promotion to production in the promotion plan.

(4) Ensure that the necessary staff, budgets and equipment are secured based on the promotion plan.

(5) Prepare procedure manuals for promotion and follow them

(6) Consider contingency plans for the potential risks.

(7) Hand over all necessary development documents and tools from the development team to the system operations department and the application maintenance department.

(8) Ensure that the stakeholders are informed of the completion of the promotion.

IV. Operation Processes (73)

1. Operation Management Rules (4)

(1) Obtain the approval of the responsible personnel from the operation department for the operation management rules and procedures.

(2) Define operation management rules based on the operation management design.

(3) Define operation procedures based on the operation management design and rules considering the target scale, periods and specific system requirements.

(4) Ensure that responsible personnel are selected based on the operation management design and rules.

2. Operation Management (16)

(1) Define the annual operation plan and obtain approval from the responsible personnel for the annual system operation plan.

(2) Ensure that monthly and daily system operation plans are created from the annual operation plan.

(3) Ensure that the operation activities comply with the operation management rules.

(4) Ensure that job schedules are organized according to the priorities of the business processes.

(5) Ensure that the system operation complies with the job schedules and operational instructions.

(6) Ensure that exceptional operation of the system is handled based on the operation management rules.

(7) Ensure that shift handovers are carried out in accordance with the operation management rules.

(8) Ensure that job schedules are recorded with operation logs and the differentials from the original ones are analyzed.

(9) Ensure that operational records are retained for a certain period in accordance with operation management rules.

(10) Define a reporting system and procedures in proportion to the levels of impact of incidents or failures.

(11) Ensure that all records of incidents or failures are retained and reported to the responsible personnel for operation (management).

(12) Ensure that root causes of incidents or failures are investigated, and take proper actions to prevent reoccurrences.

(13) Establish a support environment to help and assist users of the information system.

(14) Provide users with information security education and training.

(15) Establish a monitoring framework for system operations.

(16) Ensure that operational efficiency is attained for the information system to improve performance and the utilization of resources.

3. Manage Input (5)

(1) Define and comply with input control rules.

p. 7

(2) Ensure that input data is accurate and without omissions or duplications,and comply with input control rules.

(3) Ensure that error prevention, fraud prevention and confidentiality protection measures are included in creation procedures and operational procedures for input data.

(4) Ensure that error prevention, fraud prevention and confidentiality protection for input data are put in place effectively.

(5) Define procedures for input data storage or disposal and ensure they comply with input data control rules.

4. Manage Data (10)

(1) Define and ensure they comply with data control rules.

(2) Ensure that access control and monitoring data (creation, changes, and deletion) are put in place effectively.

(3) Ensure that data integrity is assured.

(4) Ensure that data usage is recorded and analyzed periodically.

(5) Define the scope, method and timing of data backup according to business requirements, the data processing structure and data restoration.

(6) Ensure that data delivery complies with data control rules.

(7) Ensure that fraud prevention and confidentiality protection measures are used whenever data is exchanged.

(8) Ensure that procedures for data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection.

(9) Ensure that data is protected from computer viruses.

(10) Ensure that the intellectual property rights of data is managed properly.

5. Manage Output (7)

(1) Define and comply with output control rules.

(2) Ensure output data is accurate and free from omissions or duplications.

(3) Ensure that output data control and operational procedures are taken for error prevention, fraud prevention and confidentiality protection.

(4) Ensure that output data is delivered based on output data control rules.

(5) Ensure that output data retention or destruction is based on output data control rules.

(6) Ensure that errors occurring in the output process are recorded and reviewed periodically.

(7) Ensure that usages of output data are recorded and reviewed periodically.

6. Software Management (9)

(1) Define and comply with software control rules.

(2) Ensure that access control and monitoring functions for software are put in place effectively.

(3) Ensure that software usage information is stored and reviewed periodically.

(4) Define the scope, method and timing of software backups according to business requirements and the data processing structure.

(5) Ensure that software delivery is complies with software control rules.

(6) Ensure that procedures for software data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection.

(7) Ensure that software is protected from computer viruses.

(8) Ensure that the intellectual property rights of software is managed properly.

(9) Define policies for the utilization of free software (open source).

7. Manage Hardware (6)

(1) Define and comply with hardware management rules.

(2) Ensure that hardware is installed in an environment resilient to potential risks.

p. 8

(3) Ensure that periodical maintenance is provided for hardware.

(4) Ensure that proper measures are taken for hardware failures.

(5) Ensure that hardware usage is recorded and reviewed periodically.

(6) Ensure that procedures for hardware retention, relocation and disposal are taken for error prevention, fraud prevention and confidentiality protection.

8. Manage Network (6)

(1) Define and comply with network management rules.

(2) Ensure that access control and the monitoring functions for the network are put in place effectively.

(3) Ensure that the network is periodically reviewed for monitoring logs.

(4) Ensure that proper measures are taken against failures in the network.

(5) Ensure that the network usage is periodically analyzed from stored records.

(6) Define organization policies for services provided by network operators.

9. Manage Configuration (4)

(1) Ensure that the scope of software management, hardware management and network management is clearly defined. Ensure that a proper management level is provided.

(2) Ensure that system configuration, venders and support conditions for software, hardware and networks are clearly specified.

(3) Ensure that the introduction and replacement of software, hardware and networks is decided before an assessment of its impact.

(4) Ensure that the introduction and replacement of software, hardware and networks is planned systematically.

10. Manage Facilities and Equipment (6)

(1) Ensure that facilities are located in an environment resilient to potential risks.

(2) Ensure that accesses to facilities and machine rooms are controlled for fraud prevention and protection of confidentiality.

(3) Ensure that facilities are properly operated.

(4) Ensure that maintenance of facilities is provided periodically.

(5) Ensure that proper measures against failures are taken.

(6) Ensure that the access logs to the facilities and machine rooms are recorded and reviewed periodically.

V. Maintenance (19)

1. Maintenance Procedures (3)

(1) Obtain approval for maintenance rules and procedures from the person responsible for maintenance.

(2) Define maintenance procedures according to the scale and necessary period of maintenance and specific system requirements.

(3) Assess potential risks inherent in the maintenance, and develop necessary preventive measures.

2. Maintenance Plan (3)

(1) Obtain approval for maintenance plan from the personnel responsible for maintenance.

(2) Examine and analyze the contents and influence of maintenance against change requests.

(3) Define the objective, scope, methodologies, and schedule for the maintenance test plan.

3. Maintenance Implementation (3)

(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.

p. 9

(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.

(3) Verify that programming is written according to the modified program design documents.

4. Maintenance Verification (5)

(1) Ensure that tests of modified programs are performed in accordance with the maintenance test plan.

(2) Ensure that any tests of modified programs are performed taking into account of the range of impact of the tests.

(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.

(4) Obtain approval of the results of the tests of the modified programs from the appropriate stakeholder and personnel responsible for operations and maintenance.

(5) Ensure that the results of the tests of the modified programs are properly recorded and stored.

5. Promotion to Production (3)

(1) Define promotion procedures taking into account of the promotion conditions.

(2) Ensure that backups of the pre-modified program and data are created.

(3) Ensure that the personnel responsible for operations and the maintenance department ensure that the modified system does not affect other information systems.

6. Disposal of Old Information Systems (2)

(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.

(2) Decide the disposal measure and timing of disposal of old information systems, taking measures to prevent fraud and protect confidentiality.

VI. Common Processes (76)

1. Document Management (9)

1.1 Document Creation (5)

(1) Obtain approval for created documents from the appropriate stakeholders and responsible personnel in the information system department.

(2) Define and comply with documentation rules.

(3) Define the documentation plan.

(4) Define the type, the objective and the method of creation of documentation.

(5) Ensure that all documents are created in accordance with the documentation plan.

1.2 Documentation Control (4)

(1) Obtain approval for the contents of any modifications to documents from the appropriate stakeholders and the responsible personnel in the information department.

(2) Define and comply with documentation control rules.

(3) Update descriptions in documents and record the update history following any modification to the information system.

(4) Ensure that document storage, duplication and destruction measures are taken in accordance with fraud prevention and confidentiality protection.

2. Project Management (6)

2.1 Perform Project Management (3)

(1) Define a project management approach and structure based on the project plan, and obtain approval from the appropriate stakeholders and the personnel responsible for planning, development, operations development and maintenance development.

p. 10

(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.

(3) Ensure that the appropriate measures are taken against delays.

2.2 Assess Project Management (3)

(1) Analyze and assess project performance against the project plan at the end of each phase of the project, and obtain approval for the assessment result from the project manager.

(2) Ensure that the assessment results are properly reflected in the plan for the next subsequent phase of the project.

(3) Ensure that the assessment results are properly reflected in improvements to the approach and the structure of project management.

3. Quality Assurance (4)

3.1 Quality Management Plan (2)

(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.

(2) Define the quality management plan methodology, systems and so on.

3.2 Perform Quality Management (2)

(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.

(2) Ensure that the assessment results are properly reflected in improvements on quality management standards, approaches, and systems.

4. Human Resource Management (13)

4.1 Roles and Responsibilities (3)

(1) Define roles and responsibilities for each member of personnel in accordance with the characteristics and requirements assigned to the personnel.

(2) Verify roles and responsibilities of each member of personnel in accordance with changes in the business and the IT environment.

(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.

4.2 Job Performance (4)

(1) Ensure that each member of personnel complies with his/her assigned roles and responsibilities.

(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.

(3) Ensure that shifts are handed over carried out with error and, fraud prevention and confidentiality protection.

(4) Ensure that a reserve staffing plan is prepared for contingencies.

4.3 Education and Training (4)

(1) Develop and update the educational training plans and curriculums in accordance with the human resource management policies.

(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.

(3) Provide educational training chances to each member of personnel periodically and effectively, based on the educational training plans and curriculums.

(4) Develop a career path program for each member of personnel, and review it in accordance with changes in the business and IT environment.

4.4 Healthcare (2)

(1) Ensure that the work environment is properly managed in accordance with healthcare considerations.

(2) Carry out regular medical examinations and prepare mental healthcare programs.

p. 11

5. Consignment / Entrustment (25)

5.1 Consignment or Entrustment Business Plans (3)

(1) Develop consignment or entrustment business plans in accordance with the overall optimization plan, and obtain approval to those plans from the management.

(2) Define the objectives, scopes, budget, and structure of the consignment or entrustment business.

(3) Assess concrete effects and potential problems of the consignment or entrustment business make decisions based on the results of the assessments.

5.2 Selection of the Service Provider of Consignment Business (3)

(1) Define selection criteria of service providers.

(2) Present requirement specifications to candidate service providers.

(3) Assess proposals submitted by candidate service providers.

5.3 Contracts (8)

(1) Conclude contracts in compliance with the consignment contract rules and/or the entrustment contract rules.

(2) Define provisions concerning compliance.

(3) Define whether to allow re-commission.

(4) Define the holders of the intellectual property rights.

(5) Define the special agreement and disclaimer clauses.

(6) Define details of services and the sharing of responsibilities.

(7) Reexamine contents of the contract in case of additions to or changes in the contract.

(8) Define policies for system audit.

5.4 Consignment (7)

(1) Assess consistencies between the actual consigned business and the contracted business.

(2) Provide necessary specifications, data and other materials according to the contract.

(3) Monitor progress of the consigned business, and take necessary measures against delay of the project.

(4) Monitor the status of error prevention, fraud prevention and confidentiality protection at the consigned partners, and take measures as and when necessary.

(5) Ensure that the acceptance of deliverables is carried out based on the consignment contract.

(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.

(7) Assess and analyze results of the consigned services.

5.5 Entrustment (4)

(1) Ensure that the actual entrusted business is consistent with the contracted provisions.

(2) Monitor progress of the entrusted business, and take measures against potential risks.

(3) Implement a quality management process for deliverables.

(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 contracted business.

6. Change Management (6)

6.1 Change Management (3)

(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.

(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.

p. 12

(3) Track change management issues from the proposal to its completion, and periodically analyze uncompleted issues.

6.2 Implement Change Management (3)

(1) Implement change management issues in compliance with change management rules.

(2) Ensure that the environment of other related systems is changed simultaneously when implementing change management issues.

(3) Obtain approval of the results of change management issues from the appropriate stakeholders and the responsible personnel in the development department, the operation department and the maintenance department.

7. Disaster Recovery (13)

7.1 Risk analysis (3)

(1) Assess potential risks such as earthquakes and the range of impacts on the information system.

(2) Analyze potential damage to the organization suffered from a shutdown of the information system and so on.

(3) Assess the acceptable recovery time for each business processes and prioritize them.

7.2 Contingency Plan (6)

(1) Develop contingency plans based on risk analysis and ensure that the plan is consistent with the business continuity plan.

(2) Obtain approval for the contingency plan from the top management of the organization.

(3) Assess the feasibility of the contingency plan.

(4) Define educational training policies for employees in the contingency plan.

(5) Communicate and inform related departments of the contingency plan.

(6) Update the contingency plan regularly and ensure that the plan is kept up to date.

7.3 Backups (2)

(1) Define methods and procedures for backing up the system, data and forget necessary resources to meet the recovery objectives of the businesses.

(2) Assess and confirm the backup methods and procedures by the responsible personnel in the operations department.

7.4 Alternative Operations and Recovery (2)

(1) Define and assess alternative processing procedures and structures until resumption. This task should be conducted by the appropriate stakeholders and the responsible personnel in the operations department.

(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.

Supplementary provisions

1. It is desirable to apply the Information Security Control Standards to matters related to information security.

2. It is desirable to apply related standards for other cases.