Guidelines for the Establishment of Safety Standards of CIIP

(4th Edition)

(Tentative Translation)

May 25, 2015

Cybersecurity Strategic Headquarters

Government of JAPAN

(This Page Intentionally Left Blank)

Contents

(This Page Intentionally Left Blank)

Ⅰ. Purpose and Role

1. Significance of Information Security Measures for Critical Information Infrastructures

As is stated in the "The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)" (adopted by the Information Security Policy Council on May 19, 2014 and revised by the Cybersecurity Strategic Headquarters on May 25, 2015; hereinafter referred to as the "Basic Policy"), information security measures are essential for minimizing as much as possible the occurrence of IT malfunctions, as well as restoring the system quickly and preventing recurrence in the event of such malfunction, in order to ensure the uninterrupted provision of critical information infrastructure[1] services and thereby prevent the adverse impact of IT malfunctions[2] caused by natural disasters, cyber-attacks, etc. on people's lives and socioeconomic activities.

With regards to the implementation of information security measures, it is primarily the critical information infrastructure operators[3] who shall adequately and continuously implement and improve information security measures as their own responsibilities through PDCA cycles based on the characteristics of the relevant critical information infrastructure sectors and the operators thereof.

When implementing such measures, consideration has to be given for the consistency of actions involving risk management and information security measures[4] based on the understanding that information security measures are an important part of company-wide risk management, which is the key issue for critical information infrastructure operators to stay in business.

In particular, to maintain this consistency, the information security measures have to be regarded as part of the company-wide risk management which a management layer undertakes, and the measures are to be implemented under a company-wide framework that involves not only the personnel responsible for implementing the measures but also the management layer.

---

[1] The term "critical information infrastructures" refers to "the sector of infrastructures that is formulated by business operations which provide services that cannot be easily substituted by other means, forming the basic backbone for people's lives and socioeconomic activities. These infrastructures can potentially cause crucial impact on people's lives and the socioeconomic activities of Japan when a stoppage or deterioration of functions or an outage of service occurs, and for this reason they are designated as 'critical information infrastructures.'"

[2] The term "IT malfunction" refers to the class of IT failures that cause critical information infrastructure services to fall short of the criteria of the "service maintenance level" that is specified in "ANNEX 2.CII SERVICES AND SERVICE MAINTENANCE LEVELS" of the Basic Policy.

[3] The term "critical information infrastructure operators" refers to the service operators, and groups consisting thereof, who are categorized as the "applicable CII operators" among the operators who engage in the business sectors of critical information infrastructure in the "ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES" of the Basic Policy.

[4] The term "information security measures" is used for the general activities concerning information security, such as risk management and the implementation of measures.

Based on the recognition that the adequate and continuous improvement of information security measures will lead to the protection of the entire system of critical information infrastructures, as well as individual critical information infrastructure operators, the cooperative activities of the government and private sectors are essential for fostering the public's sense of security, achieving the growth and fortification of society, and enhancing international competitiveness.

2. Necessity of the "Safety Standards"

In pushing forward information security measures, where the effect of efforts is often not apparent, it is imperative that the critical information infrastructure operators acknowledge their own conditions correctly, review their own security measures in reference to available standards, and adequately and periodically implement and improve their own information security measures through the practice of PDCA cycles.

The "Safety Standards" are necessary for implementing and improving said measures. The "Safety Standards" clearly specify the appropriate standard of information security measures corresponding to the characteristics of the relevant critical information infrastructure sector and the operators thereof.

Note that the information security measures specified in the "Safety Standards" shall be designed so as to have a proper balance between proactive measures, reactive measures that include both measures for limiting the extent of damages as well as quick recovery after the occurrence of IT malfunctions, and preventing recurrence.

3. Definition of the "Safety Standards"

Each critical information infrastructure operator conducts business according to the various standards set by the government under the legal system generally called "industry laws".[5]

Based on these circumstances, this guideline collectively calls the following documents, which are established to serve as standards or references for the service operators in their business decisions and actions, "Safety Standards":

(1) "Enforceable standards" set by the government under the industry laws
(2) "Recommended standards" and "Guidelines" set by the government according to the industry laws
(3) Cross-industry "Industry standards" and "Guidelines" developed by industry groups to meet the expectations of industry laws and the public

[5] Local governments conduct public administration for their administrative district voluntarily and comprehensively under the Local Autonomy Act.

(4) "Internal rules" developed by the critical information infrastructure operators themselves to meet the expectation of the industry laws, the public and users

In order for the required information security measures to be implemented in a faultless manner, the purpose, scope of application, intended causes, role, required items, and level of information security measures have to be clearly described and documented in the "Safety Standards." For this reason, the four types of documents (1) – (4) above are listed together to provide comprehensive views such that all parties involved in critical information infrastructure services can refer to and identify "their own responsibilities" in each process of the relevant information security measures.

4. Role of the Guideline

The important and difficult challenge in implementing information security measures is for the critical information infrastructure operators to acknowledge their own conditions correctly and determine "what measures they should take and what level they should aim at" in reference to the "Safety Standards." Information security measures shall be designed based on the above determination, incorporate monitoring and reviews in each process, and then be implemented.

For this reason, the purpose of the Guideline is to contribute to the maintenance and improvement of the level of information security measures through the establishment and update of the "Safety Standards"; specifically, to the effective and independent efforts by the critical information infrastructure operators whose actions are currently underway, or by mid- to small-size operators.

On the presumption that the Guideline is referred to when the Safety Standards are established or updated, the listing form of required items has been changed from the one that demonstrates the concept of "Four pillars and five priorities," which was used in the 3rd edition of the Guideline. The new one in the 4th edition adopts the PDCA practice to further increase the effectiveness of information security measures.

In particular, the required items are listed in accordance with "Figure 1. 'CII Operator Measure Examples' and 'Government Activities'." (This figure is exhibited again in this Guideline as Figure 1.)[6]

For the listing of the required items, considering the following sources of risks — intentional causes such as cyber-attacks; incidental causes such as operational error of users or effects

[6]The Guideline is a document that lists the measures that accord with the stance the Cabinet Secretariat takes, not what demands compliance to international standards for each concerned body. Thus, it is the objective of the Guideline that it contributes to the further betterment of the safety standards and the advancement of information security measures that the critical information infrastructure operators have already established and applied to their systems. The Guideline does not expect service operators to introduce the PDCA cycle copied from Figure 1.

derived from IT malfunctions in other critical information infrastructure sectors; and environmental causes such as disasters or epidemics — the most highly demanded items from a cross-sectional view on multiple critical information infrastructure sectors and the items that should be referred to as innovative efforts have been selected.

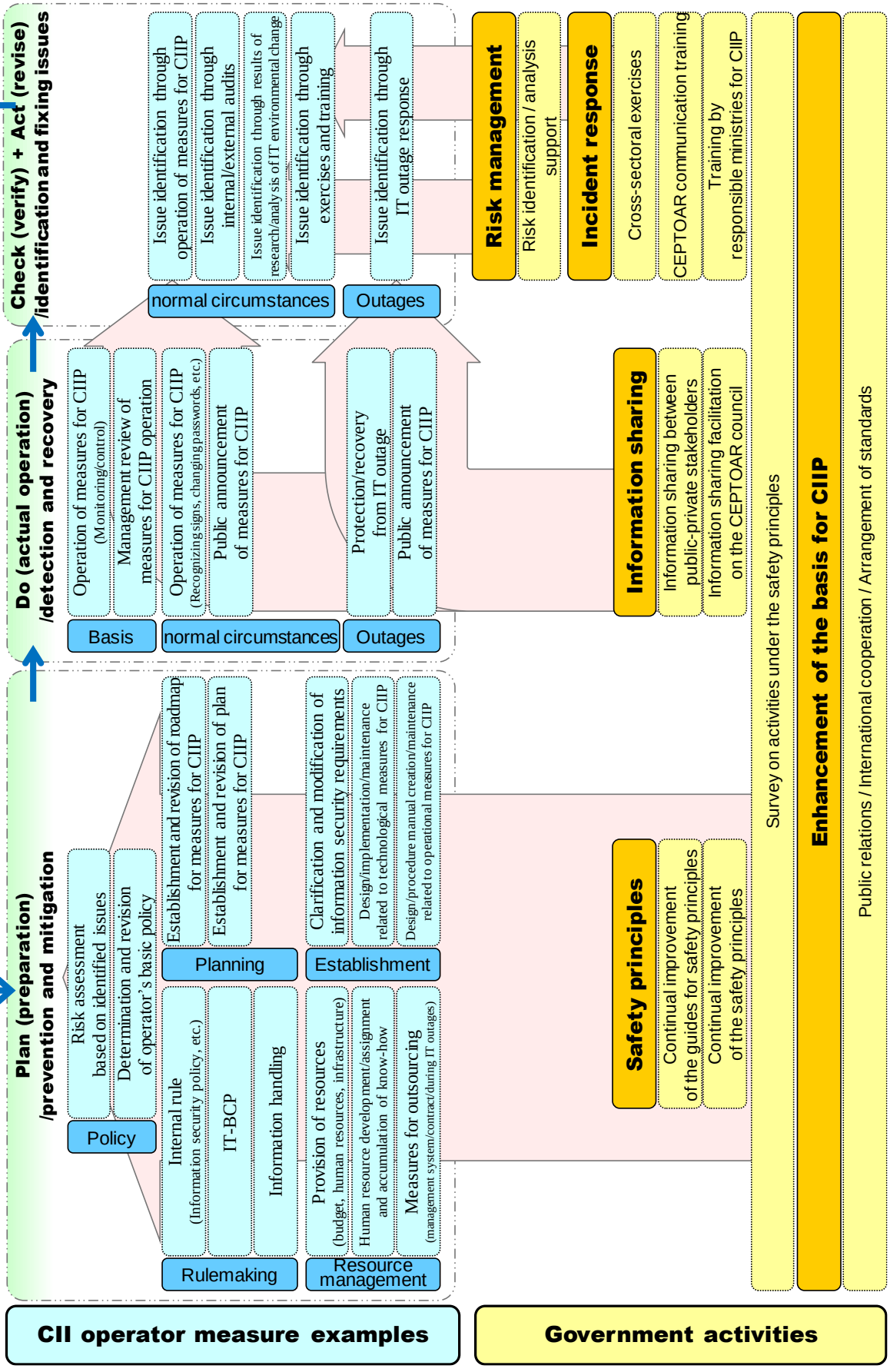
Individual critical information infrastructure operators shall ensure the continuous improvement of their PDCA practices for information security measures through the improvement efforts guided by assessment of what has been taken care of and what has not in reference to Figure 1.

Additionally, the following two points shall be understood when referring to this Guideline for the establishment and revision of the "Safety Standards":

- The items that this Guideline requests to be described in the "Safety Standards" may include items irrelevant to a particular critical information infrastructure sector or operators, depending on the manner of business involvement.
- There may be other items for certain critical information infrastructure sectors or operators than the items that this Guideline requests to be described in the "Safety Standards," depending on the manner of business involvement.

It shall be determined by individual critical information infrastructure sectors or operators thereof which of the "Safety Standards" documents specify the items and target levels that this Guideline requests, based on the industry laws and the composition of existing "Safety Standards."

Figure 1. "CII operator measure examples" and "Government activities"



5. Composition of the Guideline

The Guideline consists of the following parts: "Guidelines for the Establishment of Safety Standards Concerning Information Security Management for Critical Information Infrastructures, 4th Edition" (hereinafter referred to as the "Guideline"), which emphasizes the necessity of the "Safety Standards" and the items desirable to be specified therein; "Guidelines for the Establishment of Safety Standards Concerning Information Security Management for Critical Information Infrastructures, 4th Edition--Collection of Example Measures" (hereinafter referred to as the "Examples"), which collects examples of the information security measures specified in the Guideline; and "Guidebook for the Prioritization of Information Security Measures for Critical Information Infrastructures, 1st Edition" (hereinafter referred to as the "Guidebook"), which helps critical information infrastructure operators to develop the information security measures that best fit their own systems with respect to the items described in the Examples, and enhance the effectiveness of the protective measures by focusing on the prioritization of activities for the maintenance and improvement of security.

Note that the items to be discussed and referenced which are described in the Guideline, 3rd Edition have been removed because the approach for the prioritization of information security measures is stated in the Guidebook. Individual critical information infrastructure operators shall prioritize the measures and implement them accordingly.

The Examples and the Guidebook are treated as additional volumes of the Guideline and shall be drawn up by the CII Expert Committee.[7]

6. Expectations for the Continuous Improvement and Implementation of the Guideline Based on the "Safety Standards"

Self-verification by the critical information infrastructure operators in reference to the "Safety Standards" is essential in order for the operators to adequately and periodically implement and improve their information security measures through PDCA practice. For this reason, the "Safety Standards" shall be reviewed from time to time for continuous improvement in response to the latest knowledge, technologies, systems, new risks, etc. arising therefrom, and are expected to go beyond mechanical fulfillment of the requirements specified by the Guideline.

Additionally, the "Management Standards for Information Security Measures for the Central Government Computer Systems" and related documents shall be referred to when necessary, in

[7] The "Critical Information Infrastructures Expert Research Committee" has been established as an expert research committee that conducts research and studies on cybersecurity for the protection of Japan's nationwide critical information infrastructures. (Cited from "Establishment of the Critical Information Infrastructures Expert Research Committee", set out by the Cybersecurity Strategic Headquarters on February 10, 2015.)

addition to actively referring to best practices in Japan and overseas, such as various industry standards.

Furthermore, environmental arrangements necessary for the implementation of the measures shall be pursued for the implementation of the “Safety Standards”, in addition to the promotion of the information security measures specified in the “Safety Standards.”

Ⅱ. Items Desirable to be Specified in the "Safety Standards"

1. Purpose of the Establishment of the "Safety Standards"

The importance of the promotion and implementation of information security measures in reference to the "Safety Standards" shall be stated, in order to assure implementation of the information security measures against IT malfunctions that may cause disturbance in the continuous provision of services. Such measures are the keys for proactive measures, reactive measures that include both measures for limiting the extent of damages as well as quick recovery after the occurrence of IT malfunctions, and measures preventing recurrence.

2. Scope of the "Safety Standards"

The critical information infrastructure operators shall clearly express the services they provide and specify the intended IT systems, the data for protection within the data utilized in their IT systems, and the depth of the security measures, as specifically as possible in the "Safety Standards". This should be based on an understanding of the "ANNEX 2.CII SERVICES AND SERVICE MAINTENANCE LEVELS" of the Basic Policy, to strive for the achievement of their business objectives such as the stable provision of critical information infrastructure services[8] to the public, and for the continuation of their businesses.

All constituents that are closely involved with the uninterrupted provision of the services shall be included in the scope of the protection when considering the scope. The following are presumed examples of the items to be protected:

- Information assets (information systems and data utilized therein)
- Transactions[9] or business processes that take place in the information system networks
- Development, operation and maintenance of information systems

3. Causes of IT Malfunction Covered by the "Safety Standards"

To prevent adverse impacts on the stable provision of critical information infrastructure services and ensure continuous business operations, the critical information infrastructure operators shall specify the causes of IT malfunctions covered by the "Safety Standards" by listing the IT malfunctions that have a high probability of occurring, considering the characteristics of the critical information infrastructure sectors and operators thereof as specifically as possible.

---

[8] The term "critical information infrastructure services" indicates the services or a series of procedures necessary for using such services provided by the critical information infrastructure operators, which are developed in the "ANNEX 2.CII SERVICES AND SERVICE MAINTENANCE LEVELS" of the Basic Policy of each critical information infrastructure sector. In particular, it indicates the services to be protected as a higher priority based on the degree of impact of the interruption of services on people's lives and on socioeconomic activities.

[9] The term "transaction" is used for a number of related processes bundled into a single processing unit to control a series of operations as a single process.

The following are presumed examples of the items to be specified:

(1) Intentional causes

Receipt of suspicious e-mails, phishing for user IDs, flooding of traffic such as in DoS (Denial-of-Service) attacks, illicit obtainment of information, internal fraud, failure of proper system operations, etc.

(2) Accidental causes

User operation errors, user administration errors, execution of suspicious files, access to suspicious sites, administration errors by outside contractors, failure of devices, system vulnerability, effects derived from malfunctions in other areas, etc.

(3) Environmental causes

Disasters, epidemics, etc.

4. Role of the “Safety Standards”

To clarify the bodies responsible for each information security measure, the “Safety Standards” shall specify the roles of presiding ministries, the roles of the entire critical information infrastructure sector, and the roles of each critical infrastructure operator.

In addition, the critical information infrastructure operators shall specify the efforts to be made by their management layers toward the “Safety Standards” with reference to the contents of the “Responsibility of the Management Layers of the Critical Information Infrastructure Operators” and Figure 1. “’CII Operator Measure Examples’ and ’Government Activities’.”

The “Responsibility of the Management Layers of the Critical Information Infrastructure Operators” stated in the Basic Policy is quoted below:

> Responsibility of the stakeholders
>
> - All the stakeholders should periodically check the progress of their own measures and policies as part of relevant efforts and accurately recognize the current circumstances, and proactively determine the goals of relevant activities. In addition, stakeholders should enhance their cooperation with each other, taking into account the status of other stakeholders’ relevant activities.
> - All the stakeholders should understand the 5W1H (when, where, who, why, what and how) of IT outage response depending on the scale of IT outages and should be able to calmly address signs or occurrence of an IT outage. They should be capable to cooperate with other stakeholders and respond in a cooperative and concerted manner in addition to ensuring robust communication among various stakeholders and taking proactive measures.
>
> Responsibility of CII operator's executives and senior managers

In addition to the aforementioned measures, the executives and senior managers should recognize the need for and be able to ensure the implementation of the following measures:

- Recognize risk sources with a focus on information security for the purpose of CIIP.
- Assess risk sources and set forth measures to address those risks by identifying priorities.
- Determine plans necessary for the establishment and operation of systems and the implementation of relevant policies in addition to securing management resources (e.g. budget, human resources, etc.).
- Check the status of the implementation of relevant policies through monitoring the system operation.
- Check the status of incident response capability including information sharing among relevant stakeholders through conducting exercises and trainings.

5. Publication of the “Safety Standards”

As part of efforts for fostering the public’s sense of security through the stable provision of critical information infrastructure services which have a significant influence on people’s lives and socioeconomic activities, efforts undertaken for critical information infrastructure protection shall be demonstrated through the publication of the “Safety Standards”, as much as possible.

6. Measures to be Taken

When establishing and revising the “Safety Standards” in each critical information infrastructure sector, the adoption of the following items, which are itemized in line with Figure 1. “’CII Operator Measure Examples’ and ’Government Activities’” in the Guideline, shall be discussed.

6.1 In the Planning Phase: “Plan” (Preparation)

6.1.1 Policy making

(1) Risk Assessment Based on Recognized Issues

Based on the result of risk analysis, which is described in the section on Verification and Correction Phases below, the creation of basic information (risk assessment) concerning the risks that need to be dealt with and decision-making on the priority of actions to be taken, along with the establishment/revision of the “Safety Standards”, shall be carried out.

Based on this basic information, decisions on measures (actions against the risks) shall be made with reference to the required level of security, together with consideration of the significance of the risks, the feasibility of the measures, and the possibility of the risks

spreading from a contained state.

(2) Establishment/Revision of the Basic Policy

The basic policy is the statement of the basic stance for information security measures. The policy shall clarify the purpose of critical information infrastructure protection, the direction of efforts, and the targets to be protected by the information security measures, and shall specify how the efforts for information security are being conducted.

In addition, the controlling organizations, purpose, authorities, members involved, criteria for revision, etc. concerning the establishment/revision of the basic policy shall also be specified.

6.1.2 Rulemaking

(1) Establishment/Revision of the Internal Rules

Based on the established/revised basic policy, the method of thinking, rules, etc. concerning the implementation shall be specified through the systemization of each information security measure.

In addition, the controlling organizations, purpose, authorities, members involved, criteria for revision, etc. concerning the establishment/revision of the internal rules shall also be specified.

(2) Establishment/Revision of IT-BCPs

The IT-BCP (Information Technology — Business Continuity Plan) mentioned in the Guideline is a plan consisting of the process of actions necessary for the quick recovery and continuous provision of IT system services in the case of IT malfunctions that degrade services below the serviceable level. It shall specify the priority of actions, processes toward the determination of necessary measures, methods to continue the operation, divisions to cooperate with, etc. in the event of IT malfunctions.

When developing the plan, threats that call on action from the entire society, such as a wide-area disaster, multiple failures, new types of influenza, spread of failures from mutually dependent critical information infrastructures, etc., along with the highly dense conditions of essential data for business continuity in specific cities or areas, shall be considered as well.

Furthermore, precautions in ordinary times, education/training programs, etc. shall be included in the plan for the adequate implementation of actions in the event of IT malfunctions.

(3) Rulemaking for Information Handling

The information shall be rated (ranked) depending on the importance of the information

from the aspects of confidentiality[10], completeness[11] and availability.[12] In addition, conditions to be complied with and information security measures in each step of the lifecycle of the information, such as creation, acquisition, utilization, storage, transference, provision, erasure, etc., shall be specified.

Note that attention shall be paid to the public’s sense of security in the handling of personal data.

6.1.3 Planning

(1) Development/Revision of the Roadmap and Plan Concerning Information Security Measures

Once the specific goals are set for information security measures based on the establishment/revision of the policy, a roadmap, a rough schedule toward the accomplishment of the goal, and a plan that details the roadmap shall be drawn up and implemented.

6.1.4 Framework

(1) Securing a Budget and the Formation of a Framework (including Outside Contractors)

To implement the information security measures according to the plan, management resources such as the budget, framework, human resources, etc. necessary for the construction and operation of the system and execution of the plan shall be secured.

(2) The Development and Assignment of Human Resources and the Accumulation of Know-How

Information security measures for systems are often constructed by a combination of multiple measures. In addition, system maintenance in ordinary times requires actions to maintain the level of security measures, such as changing the organization and system users, system optimization, etc.

For this reason, the continuous development and assignment of human resources that are designed to be effective, along with the accumulation of know-how, shall aim to maintain a constant level of security measures even after a change of the personnel responsible for the security measures.

Furthermore, education about information security shall be given to all company employees,

---

[10] The term “confidentiality” in this Guideline means securing the condition where only authorized personnel can have access to restricted information. This includes the application of protection techniques on the information to prevent an adverse impact in the event that restricted information is divulged.

[11] The term “completeness” in this Guideline means securing the condition where the information is not destroyed, altered, or erased.

[12] The term “availability” in this Guideline means securing the condition where authorized personnel can have access to the information at any time necessary and without interruption.

and not limited to the personnel responsible for system operations as system users. PC users are also intended personnel.

(3) Measures for Outside Contractors (Oversight, Contracts and Actions in the Event of IT Malfunctions)

Divulging of critical information and malicious system operation could also arise from conduct inside the company which are either intentional or accidental, not only coming from the outside. Such intentional or accidental conduct within the company includes that performed not only by the employees of the critical information infrastructure operators, but also by the personnel of outside contractors.

For this reason, oversight of outside contractors shall be performed by means of outsourcing contracts that are entered into through evaluation of the adequacy for the tasks to be outsourced, clarification of the range of tasks to be outsourced, and contractor nomination with reference to the vendor selection criteria, as well as contractors' business management. Particularly, implementation of the same level of security measures and education of the contractors as that applied and given to the employees, and cooperation in the event of IT malfunctions, shall be agreed upon.

6.1.5 Structuring

(1) Clarification and Change of Information Security Requirements

In implementing information security measures into the information systems of critical information infrastructure operators, the information security functions to be installed shall be clarified with regards to the aspects of confidentiality, completeness and availability.

In this process, the information security functions that need to be installed against various threats such as security holes, malicious programs and DoS attacks, and the functions necessary for proactive measures, as well as reactive measures that include measures for limiting the extent of damages and quick recovery after the occurrence of IT malfunctions, shall be clearly specified, along with the measures needed to prevent unauthorized invasion and to prevent tangible damages[13] brought about by successful invasion.

(2) Design, Implementation and Maintenance of Information Security Measures (Technologies)

Information security measures shall be implemented into the information systems in accordance with the information security requirements. In this process, attention should be given so that the implemented information security measure functions do not disturb the performance of the original system required for business operations.

[13]The examples of tangible damages include information theft, breaking of information systems, etc.

Additionally, design documents that detail the implementation of information security measures shall be prepared for the accumulation of know-how.

(3) Design, Manual-Making and Maintenance of Information Security Measures (Operations)

Stable operations are realized through the design of operation procedures and the compilation of a procedural manual for the information system in which the information security measures are being implemented, in accordance with the information security requirements. In addition, maintenance activities such as the user registration necessary for verification shall be performed thoroughly to maintain the efficacy of the information security measures.

6.2 In the Implementation Phase: “Do” (Implementation)

6.2.1 Actions Common to Ordinary Operations and in the Event of IT Malfunction

(1) Operation of Information Security Measures (Monitoring and Control)

The managing staff responsible for information security shall constantly and periodically assess the operational status of the established information security measures.

(2) Understanding of the Operational Status of the Measures

The management layer shall assess the operational status of the information security measures.

6.2.2 Actions During Ordinary Operations

(1) Operation of the Information Security Measures (Monitoring Indicators, Changing of Passwords, etc.)

The operational condition of the information systems shall be monitored so that any abnormal conditions in comparison to ordinary conditions or to threshold values can be detected as a sign of malfunctions.

In addition, the level of security measures shall be maintained through changing registered data such as the organization and system users, system optimization, etc. in system maintenance activities.

Furthermore, education about information security shall be given to all employees of the company.

(2) Explanation of the Status of Information Security Measures Outside the Company

To contribute to the fostering of the public’s sense of security, the efforts of information security measures made for the uninterrupted provision of critical information infrastructure services shall be explained outside the company through information security reports or a company website, etc., while paying attention to the content of disclosures.

6.2.3 Actions in the Event of IT Malfunction

(1) Protection against IT Malfunction and Recovery

The developed IT-BCP shall be put in motion and business operations shall be maintained in accordance with the actions specified in the rules while efforts for quick recovery are being made. While doing so, electronic records such as journals or logs shall be collected and analyzed for the cause, so that appropriate measures against the cause of the relevant IT malfunction can be taken.

(2) Explanation of the Status of Information Security Measures Outside the Company

As to the provision of information about the status of the IT malfunction and the recovery therefrom, necessary actions such as informing users about the service availability shall be taken in accordance with the developed IT-BCP and an understanding of the 5W1H (when, where, who, why, what and how) of the information-based actions. Such actions shall be taken in a cooperative and harmonized manner with other related organizations.

6.3 In Verification and Correction Phases: “Check” (Verification) and “Action” (Correction)

6.3.1 Actions During Ordinary Operations

Any threats and vulnerability that have been identified in conducting information security measures, internal and external audits, research and analyses of changes of the IT environment, and issues found through exercises and training, all of which can be the source of risks, shall be taken into consideration together with considerations of the impact on must-be-maintained service levels and the consequences of those threats and vulnerability, for the purpose of identifying the risks (risk identification).

Qualitative or quantitative analyses (risk analyses) shall be made of the identified risks and then the concrete impact of those risks, such as the potential damages on business, shall be determined.

The results of risk identification and analysis shall be used in the risk assessment and actions taken against the risks described in section 6.1 In the Planning Phase: “Plan” (Preparation) above.

6.3.2 Actions in the Event of IT Malfunction

As issues recognized through the actions taken in the event of an IT malfunction (detection and recovery), any threats and vulnerability that have been identified as the source of risks, the must-be-maintained service levels that have been affected, and the consequences that arose from those threats and vulnerability, shall be referred to for identifying the risks (risk identification).

The damage that the identified risk has caused on the business is referred to as the result of the risk analysis and dealt with at a later time.

The results of risk identification and analysis shall be used in the risk assessment and actions taken against the risks described in section 6.1 In the Planning Phase: “Plan” (Preparation) above.