Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure

(July 4, 2023)
Cybersecurity Strategic Headquarters
Government of JAPAN

Table of Contents

1. Purposes and Positioning

1.1. The Importance of Ensuring Cybersecurity for Critical Infrastructure (CI)

National life as well as the economy and society of Japan are underpinned by the safe and continuous provision of CI services (CISs). To realize a safe and secure society, it is vital to ensure the cybersecurity of CI and enhance its resilience based on the concept of mission assurance.

In cases where damage is caused to an organization or third party due to an inadequate cybersecurity system determined by the organization's decision-making body in consideration of the scale and contents of the organization's operations, the top management[1] shall be held accountable to stakeholders or legally responsible under provisions of the Companies Act, Civil Code, or other laws. For example, the top management can be liable for damages for breach of duty of care or negligence of their duties.

It is important for all levels, from the top management to personnel-in-charge, to fulfill their respective roles and responsibilities, and ensure cybersecurity from both aspects of proactive approaches through risk management and crisis management, such as preventing the spread of damage and achieve early recovery in the event of an outage or other problem.

1.2. What are "Safety Principles?"

CI operators engage in business in accordance with the relevant standards, under the legal systems that are related to their respective business domains. In this Guideline (hereafter, "Guideline for Establishing Safety Principles"), documents that serve as standards or references for the decisions and actions taken by CI operators in relation to ensuring cybersecurity, are named as "Safety Principles."

The Safety Principles are classified into the following four categories.

[1] Mandatory standards that are stipulated by the government based on the relevant laws

[2] Recommended standards and guidelines that are stipulated by the government in accordance with the relevant laws

[3] Industry standards and guidelines that cut across industries, stipulated by industrial organizations with the aim of fulfilling the expectations of the citizens and the relevant laws

[4] Internal regulations, etc. stipulated by CI operators with the aim of fulfilling the expectations of citizens, users, and the relevant laws

*Note that documents that correspond to Safety Principles are not limited to documents drawn up for the purpose of ensuring safety.

[1] A person with overall responsibility as the representative of the organization (CEO, Chairperson, Head, etc.), persons responsible for executing the organization's operations, and the Board of Directors or Board of Governors, if applicable.

It is desirable that items and standards related to security measures are clearly presented in the Safety Principles and they are understood by all parties that are involved in the CI business.

1.3. Positioning of the Guideline for Establishing Safety Principles

The Guideline for Establishing Safety Principles are developed to support the formulation and revision of the Safety Principles based on the Cybersecurity Policy for Critical Infrastructure Protection (decided by the Cybersecurity Strategic Headquarters on June 17, 2022) (hereafter, “the Cybersecurity Policy”).

The Guideline for Establishing Safety Principles organizes and sets out the cybersecurity measures that are required across all CI sectors. While these measures are, in principle, expected to be prescribed in the Safety Principles, measures that may be considered for adoption depending on the situation in the organization are described as recommendations using terms “it is desirable to…”.

Regarding which the Safety Principles to prescribe each measure under, it is assumed that this will be considered by each CI sector or CI operator based on factors such as the provisions of the relevant laws and regulations, and the structure of the Safety Principles.

It is desirable to refer to various relevant standards, best practices in Japan and abroad, and other reference sources so that the Safety Principles can be made more advanced and comprehensive.

The terminology used in the Guideline for Establishing Safety Principles follows that used in the Cybersecurity Policy.

2. General Provisions

The following items should be prescribed in the Safety Principles.

2.1. Purpose of Formulating the Safety Principles

Set out the following effect as the purpose of formulating the Safety Principles: To secure the resilience of CI and realize the safe and continuous provision of CISs without serious impact on national life and socioeconomic activities,[2] it is necessary to make efforts to ensure cybersecurity with reference to the contents of the Safety Principles.

2.2. Applicable Scope

List the applicable scope for the items to be prescribed in the Safety Principles based on the contents prescribed in the Cybersecurity Policy such as applicable critical information system examples in "Annex 1: Scope of CI Operators and Critical Information System Examples," as well as the CISs (including procedures), examples of CISs outages, and service maintenance levels in "Annex 2: Explanation of CI Services and Service Maintenance Levels."

2.3. Roles of Stakeholders

With regard to the stakeholders such as the responsible ministries for CI, CI operators, and supply-chain operators, provide a comprehensive and specific list, and clearly define the roles of each stakeholder in relation to the respective security measures. In particular, with respect to the role of CI operators, the efforts of the top management should also be included.

[2] Refer to "I. Introduction 1. Purpose of CI Protection" of the Cybersecurity Policy.

3. Cybersecurity in Organizational Governance

Ensuring cybersecurity of CI should be tackled from the perspective of mission assurance. The Cybersecurity Strategy (Cabinet decision on September 28, 2021), sets out the following explanation of mission assurance: “Refers to the condition in which any organization represented by companies, critical infrastructure operators, and government bodies understand the operations or services that they should carry out as their missions, and ensure necessary capabilities and resources to reliably execute such missions. This means that senior executives or managers of each organization should identify operations or services that represent their missions and take all responsibility for secure and sustainable provision, rather than making cybersecurity initiatives themselves the goal.”

It is a social responsibility for CI operators to reduce the risks of uncertainty in the safe and continuous provision of CISs to an acceptable level, and it is a duty of the top management to put this into practice. Considering that it is essential to ensure cybersecurity for the safe and continuous provision of CISs, cybersecurity should be included in existing organizational governance [3] initiatives (organizational policy, system architecture, audits, information disclosure, etc.); therefore, the following items should be prescribed in the Safety Principles.[4]

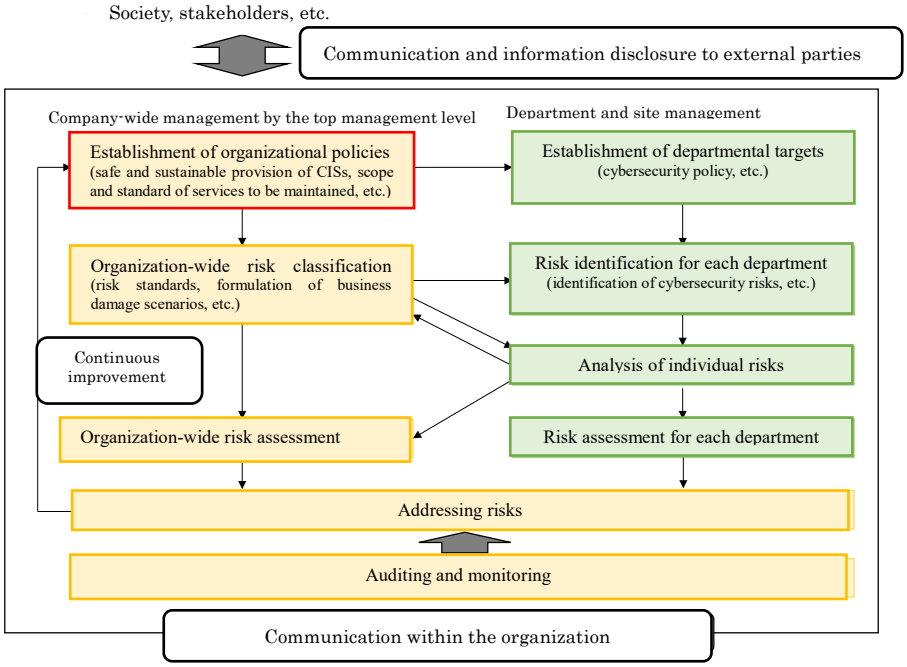

Figure: Image of organizational governance and cybersecurity

[3] In the Guidelines for Establishing Safety Principles, organizational governance refers to the systems that regulate the activities of an organization and the actions of its managers and directors, as well as the systems for preventing misconduct in an organization, and for enhancing the soundness of its finances as well as its competitiveness and sustainability. It is also important to bear in mind that the Corporate Governance Code (June 11, 2022, Tokyo Stock Exchange, Inc.) defines corporate governance as "a structure for transparent, fair, timely and decisive decision-making by companies, with due attention to the needs and perspectives of shareholders and also customers, employees and local communities," as well as the establishment of a risk management system corresponding to the scale and characteristics, etc. of the businesses operated by the company as the internal control system required under the Companies Act (Act No. 86 of 2005).

[4] Refer to METI's Cybersecurity Management Guidelines, the Q&A handbook on cybersecurity-related laws and ordinances published by the National Center of Incident readiness and Strategy for Cybersecurity (NISC).

3.1. Organizational Policy

3.1.1. Organizational Policy and Cybersecurity

Incorporate items related to ensuring cybersecurity for CI into the documents that correspond to organizational policy (such as business policy, risk management policy, etc.). For example, it is desirable to incorporate elements such as “realizing the safe and continuous provision of CISs,” “damage from threats to cybersecurity is one of the risks that hinder service provision,” and “including matters related to cybersecurity in risk management.” At the same time, it is also desirable to indicate the scope and level of services to be maintained.

3.1.2. Cybersecurity Policy

Based on the organizational policy, formulate a cybersecurity policy that contains the following elements.

- Purposes and direction of security measures
- Response to requests from stakeholders
- Commitment of the top management

3.2. Communication Within and Outside the Organization

Handle information related to cybersecurity risks, incidents, etc. in communication within and outside the organization.

As a part of communication on organizational governance, internal control, and other risk management matters, hold opportunities for regular dialogue between the top management and the personnel-in-charge on matters such as environmental changes related to cybersecurity, occurrence status of incidents and lessons drawn, implementation status of security measures and evaluation of effectiveness.

It is desirable to recognize “security by design” as a common value, and to include departments responsible for cybersecurity as a stakeholder in the internal consultation processes during product and service planning.

It is desirable to exchange opinions among stakeholders within and outside the organization on their roles, division of responsibilities, information sharing systems, and other matters related to cybersecurity.

3.3. Managing Cybersecurity Risks as Business Risks

As a part of the organization-wide risk management,[5] develop organizational systems that

[5] In addition to vertical layers such as the top management, CISO (refer to section 3.4 Assignment of Responsibilities and Authority), strategic management, and personnel-in-charge, pay attention to the lateral layers such as information system departments, business departments, and publicity departments.

enable the top management to understand and assess cybersecurity risks and their impact on business operations. In other words, based on the organizational policy, manage risks from the perspective of how the organization's information systems and businesses that utilize information, credibility as a business operator, and other business risks, can be affected by the failure to ensure cybersecurity. Also, analyze risks from the perspectives related to individual information systems and the security of information itself. In addition, pay close attention to security measures not just within one's own organization, but also across the entire supply-chain such as business partners and contractors.[6]

It is desirable for the top management to put efforts into understanding cybersecurity risks as much as possible, keeping in mind the following points: which information systems are indispensable to the provision of CISs, how those systems may be exposed to cyber threats, and what kind of security measures should be taken.

3.4. Assignment of Responsibilities and Authority

In managing cybersecurity risks, determine the departments and employees responsible for cybersecurity, and assign their responsibilities and authority.[7] In particular, personnel-in-charge of cybersecurity (CISO, etc.) should be appointed, and their appointment should be carried out under the responsibility of the top management.[8] These personnel-in-charge should be persons who have knowledge about cybersecurity, and should be positioned at a hierarchy within the organization as persons who can communicate directly with the top-level executive

---

[6] In addition to the form and scale of conventional parts procurement, etc., efforts should also be made to take an overview of the entire supply-chain, including all the connections with external parties via the digital environment, such as the use of cloud services, and to ensure cybersecurity comprehensively.

[7] Based on the premise of building an appropriate management system, specialized matters related to cybersecurity can also be complemented through external outsourcing and collaboration with industry organizations.

[8] Paragraph 4 of Article 362 of the Companies Act, and item 3 of the same, stipulate that "Board of directors may not delegate the decision on the execution of important operations such as the following matters to directors: the appointment and dismissal of an important employee including managers." There are three types of companies with board of directors: (1) Companies with (board of) auditors; (2) companies with audit and supervisory committees; (3) companies with nomination committees, etc.

Regardless of which it is, (1) to (3) above, the appointment of CISO, etc. usually falls under the category of the appointment of important employees. In such cases, in (1) companies with (board of) auditors, the appointment of the CISO, etc. must be decided by the board of directors. As an exception, in cases where the majority of the board of directors are outside directors (Paragraph 5 of the same), or if there are provisions in the articles of incorporation (Paragraph 6 of the same), the appointment of the CISO, etc. may be delegated to the director in charge. In (ii) companies with nomination committees, etc., the appointment of the CISO, etc., including decisions on the execution of duties, may be delegated to the executive officer (Paragraph 4 of Article 416 of the Companies Act). In other words, in (3), the appointment of the CISO, etc. is decided by the board of directors only when it is not delegated to such an executive officer.

On the other hand, with respect to stock companies that do not have a board of directors, the main clause of Article 348 and Paragraph 3 of the same stipulate that "the directors may not delegate the decisions on the appointment or dismissal of a manager to individual directors." Although CISOs, etc. do not normally fall under the category of "managers," considering the balance with companies that have a board of directors, even in companies that do not have a board of directors, it should be considered necessary to obtain the approval of the majority of the directors when appointing a CISO, etc. (see Paragraph 2 of the same Article).

Furthermore, in the establishment of an internal control system related to cybersecurity, matters related to the necessary internal organizations and rights should be decided by the board of directors. (NISC's Q&A handbook on cybersecurity-related laws and ordinances, March 2, 2020).

of the organization during normal times and particularly during emergency situations. It is desirable to assign them from among members of the top management.

3.5. Securing Resources

Allocate the resources (budget, human resources, etc.) necessary for security measures under the responsibility of the top management based on the concept[9] that these investments[10] are essential for reducing costs and losses in organizational activities in order to maintain and enhance the value of the organization.

3.6. Auditing and Monitoring

Implement audits such as information security audits and system audits[11] (or if there are difficulties, at least self-inspections) under the responsibility of the top management. It is desirable to implement vulnerability assessments and penetration tests to detect problems with the current systems and security measures.

Check periodically on changes to risks associated with the introduction and operation of security measures (changes in the occurrence frequency of events, changes in the impact of the consequences of events, etc.). In addition, check periodically, or corresponding to changes in the situation, on the attainment status of targets set under the cybersecurity policy, and the effectiveness and validity of the cybersecurity policy and various plans.

3.7. Information Disclosure

From the viewpoint of fostering a sense of security among the people, utilize existing information disclosure systems within the organization, and disclose information on cybersecurity efforts to the fullest extent possible.[12] It is desirable to disclose the following information related to cybersecurity.

- Organizational policy and cybersecurity policy
- Scope and level of service to be maintained
- Risk management systems
- Knowledge of personnel-in-charge of cybersecurity

---

[9] Generally, it is difficult to calculate the direct profits from investments in security measures, and it is necessary to change the way of thinking about cybersecurity.

[10] With regard to the concept of investment, definitions differ in the various domains, such as accounting and management. Here, rather than expecting direct profits (returns), it is used in the sense of means to suppress future risks and realize positive outcomes in the sum of risks and profits.

[11] Departments in charge of internal control are often established under the top management. However, even in such cases, depending on the nature of the case, the submission of reports should be separated into cases where reports are made to the top management, and cases where reports are made to the auditors, etc. (METI's Practical Guidelines for Corporate Governance Systems (June 28, 2019), page 72 and below).

[12] The disclosure of an organization's cybersecurity information not only fulfills the organization's responsibility of accountability to society, but can also be expected to be evaluated properly by stakeholders as the organization's proactive effort to implement security measures as an important issue in the management of the organization.

- Securing resources
- Understanding risks and formulating plans for addressing risks
- Emergency response systems and recovery systems
- Occurrence status of incidents

3.8. Continuous Improvement

Continuously improve the organizational governance framework, taking into account the outcomes of cybersecurity auditing and monitoring as well as the latest security trends. In departments responsible for cybersecurity, carry out continuous improvements on cybersecurity policies and various plans, based on directives from the top management, monitoring reviews, crisis management, and exercises and training.

It is desirable to make efforts to ensure that the concept of risk management, including cybersecurity, penetrates the organization and becomes established as the organizational culture through continuous improvement.

4. Utilization of Risk Management, and Crisis Management

It is important to work on ensuring cybersecurity from both aspects of proactive approaches through risk management and crisis management.

Upon identifying the characteristics and risks of one's own organization, the following items should be specified in the safety principles so that the organization can repeatedly: (1) conduct self-evaluation of the current implementation status of security measures; (2) analyze the differences from the ideal situation and requirements; (3) prioritize the measures that are insufficient for the organization based on the analysis results; (4) implement specific measures.

4.1. Understanding the Organization's Situation

Organize the status of the external environment (politics, economics, society, etc.) and internal environment (organizational structure, strategy, capabilities, etc.) in relation to CISs, including the situation in the near future. In addition, organize the requirements from stakeholders, such as obligations prescribed in relevant laws and ordinances[13] as well as contracts, and limitations set out by suppliers and contractors. It is desirable to understand the following characteristics of an organization, from the viewpoint of mission assurance.

- The roles and functions that the organization should fulfill, and the services that need to be maintained and continued based on these roles and functions
- Minimum scope and level of services to be provided
- Operations and management resources necessary for maintaining the provision of services

Furthermore, in the department related to cybersecurity, ascertain the actual implementation status of security measures at the current stage, based on an understanding of the organizational situation.

4.2. Risk Management

Identify the assets of the organization, such as information systems, software, and information. Conduct risk assessments based on the concept of mission assurance, taking into account the situation in the organization and its assets. It is desirable to draw up scenarios in which the continuous provision of CISs is uncertain, and to conduct risk analysis based on such scenarios.

- Select risk analysis methods based on the characteristics of the risks considering that risks that make the continuous provision of CISs uncertain include natural disasters, mismanagement, cyberattacks, and environmental changes surrounding CI.

[13] For example, business laws on critical infrastructure, Act on the Protection of Personal Information (Act No. 57 of 2003), Act for the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Act No. 43 of 2022), etc. Refer to NISC's Q&A handbook on cybersecurity-related laws and ordinances.

- Conduct risk assessments appropriately[14] on OT systems[15], bearing in mind that general-purpose equipment is used in OT systems, and that there are cases where they are connected to the external environment for purposes such as remote monitoring and control.[16]
- During the operation of information systems, conduct appropriate risk assessments corresponding to environmental changes, such as the occurrence of new threats related to cyberattacks.
- Review the ideal situation and requirements, and decide on the target future vision.

4.3. Addressing Cybersecurity Risks

4.3.1. Decision to Address Risks

Consider the security measures that should be implemented in order to close the gap between the target future vision and the actual conditions. Prioritize the degree of security measures based on the organization's evaluation criteria and other factors, while utilizing the maturity model.

Through addressing risks, prevent the occurrence of outages to CISs and realize the detection, response and recovery functions for limiting the socioeconomic impact of outages to acceptable ranges.

4.3.2. Formulation of Individual Policies

Formulate individual policies that compile the standards on actions and decisions to be adhered to in each security measure determined through addressing risks (for example, access control policy, information classification policy), and communicate them to the organization. In addition, communicate them to the contractors where necessary.

4.3.3. Formulation of Plans for Addressing Risks

Formulate plans for addressing cybersecurity risks. It is desirable to include the following items in the plans.

- Target future vision
- Items to be implemented
- Resources required
- Personnel-in-charge
- Deadline for accomplishment

---

[14] Refer to concrete work procedures, etc. outlines in the IPA's Security Risk Assessment Guide for Industrial Control Systems, 2nd Edition (Implementation and Utilization of Risk Assessments in Security Measures).

[15] A group of devices used to manage and control other equipment and systems in the monitoring and control of social infrastructure and factories/plants, and in production and processing lines.

[16] Generally, OT systems of critical infrastructure consist of equipment with proprietary specifications and communication protocols, and are operated in a closed environment with no external connections.

- Evaluation method for outcomes

4.4. Supply-chain Risk Management

The following are representative threats related to the supply-chain[17] that should be addressed.

- Embedding of unauthorized functions, etc.
- Supply disruption of services
- Inappropriate handling of information in external services
- Cyberattacks via overseas bases, group organizations, business partners, etc.

Understand the dependency between critical systems and functions of the organization, and its supply-chains, and grasp the status of suppliers' security measures.

Conduct risk assessments and risk responses on supply-chain risks. For overseas bases, address risks based on the local laws, regulations, and culture.

Clarify the roles and scope of responsibilities for direct suppliers to address cybersecurity risks in contracts between business operators. Furthermore, it is desirable to conduct risk management of the entire supply-chain by determining the degree of involvement of suppliers linked to direct suppliers based on risks, and by having each supplier understand the implementation status of risk management at suppliers located upstream of itself. Through support for the introduction of security measures and joint implementation, it is desirable to enhance the effectiveness of measures in the supply-chain as a whole.

4.5. Business Continuity Plan and Other Plans

Based on the impact of cyber incidents on business continuity, incorporate cybersecurity into the response policies (contingency plans, business continuity plan,[18] business recovery plan,[19] etc.) from initial response to full recovery to limit the adverse effects on business continuity to an acceptable level. Incorporate the response to supply-chain threats into the business continuity plans and other plans. Along with the business continuity plan, it is also desirable to formulate a response policy (such as IT-BCP)[20] that sets out details on the information systems. When the impact of system outages spreads to the entire organization, it is desirable to migrate

[17] A supply-chain generally refers to the process from the production of the raw materials of a certain product, to its delivery to the end consumer. In the Guideline for Establishing Safety Principles, it refers to the process of procuring and utilizing products (equipment, software) or services (cloud services, maintenance and management services, etc.) that involve external organizations, within one's own organization.

[18] A Business Continuity Plan (BCP) is a plan describing the policy, systems, procedures, etc. by which enterprises can avoid suspension of their critical business or can recover the critical business quickly if it is interrupted, even when contingencies arise, including natural disasters such as major earthquakes, communicable disease pandemics, terrorist acts, serious accidents, disruption of supply chains and abrupt changes in business environment, or they can recover business quickly if their business is interrupted. (Cabinet Office "Business Continuity Guidelines," April 2021, p. 3)

[19] The policy of working to achieve complete recovery to reach the service standard in normal times.

[20] The definition of cybersecurity in The Basic Act on Cybersecurity (Act No. 104 of 2014) includes necessary measures to ensure the safety and reliability of information systems.

smoothly from the IT-BCP to the business continuity plan.

4.6. Human Resource Development and Awareness-Raising

Based on the concept of "Cybersecurity by All," promote human resource development and awareness-raising so that all employees can deepen their understanding of cybersecurity rules and regulations, and ensure the necessary level of cybersecurity-related capabilities for each department and position.

- It is desirable to consider the design of career paths and the utilization of external human resources to secure personnel to engage in security measures.
- It is desirable to promote the acquisition of qualifications such as the Registered Information Security Specialist certificate, participation in exercises and training, and other initiatives among human resources who are engaged in security measures.
- It is desirable to raise awareness on the importance of security measures through methods such as presenting examples of the impact of inadequate security measures.

4.7. Establishment of CSIRT, etc.

Establish systems that function as CSIRT.[21] CSIRT, etc. makes agreements with the relevant departments on the division of roles and response procedures. In particular, if the organization owns OT systems, it is desirable to develop systems that can enable collaboration with departments related to the OT systems.

4.8. Operation During Normal Times

4.8.1. Introduction of Security Measures, Establishment and Implementation of Operational Processes

Introduce security measures, establish and implement operational processes, and put CSIRT, etc. into operation based on the plans for addressing risks. It is desirable to establish mechanisms for the early detection of events that could potentially lead to CIS outages (cyberattacks, abnormal conditions in information systems, etc.), as well as operational processes such as information sharing with relevant departments and triage.[22]

4.8.2. Information Sharing

Share information within and outside the organization, in accordance with the Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks (March 8, 2023, Study Group on Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks) and NISC's "Information Sharing Manual based on the Cybersecurity Policy for Critical

[21] The abbreviation for Computer Security Incident Response Team. Refers to a system that monitors information systems, etc. in companies and government agencies for security problems, and, in the unlikely event that a problem does occur, analyzes the cause and investigates the degree of impact.

[22] Assigning a degree of priority to the impact analysis and response of events such as cyberattacks.

Infrastructure Protection.”

Based on the information on threats and countermeasures that have been collected, make decisions on the need to conduct additional risk assessments and address risks.

- It is desirable to participate in information sharing activities that are highly specialized for certain fields, such as ISAC, and collect information through such activities.
- It is desirable to check if the contact system has been updated with the latest information.
- It is desirable to provide information to both inside and outside the organization, being aware of the need to provide appropriate information in order to obtain useful information.

4.9. Crisis Management

When signs of cyberattacks, etc. are detected, verify if they can be addressed by the current security measures, and where necessary, swiftly take actions such as revising the countermeasures and introducing new measures. In. addition, when outages to CISs occur, implement initial and recovery responses in line with the business continuity plan and other plans. In departments responsible for cybersecurity, provide support toward the top management in their decision-making processes related to initial and recovery responses, and share information within and outside the organization.

4.10. Exercises and Training

To validate the effectiveness of systems and initiatives from both aspects of proactive approaches through risk management and crisis management, conduct practical exercises and training regularly for identification and improvement of issues. It is desirable to conduct exercises and training across the whole of the organization,[23] involving the top management. It is also desirable to conduct joint exercises and training with other CI operators and supply-chain operators, etc., and to study past incident response cases.

[23] For example, cross-sectoral exercises organized by NISC.

5. Measures

The following security measures should be incorporated into the Safety Principles in response to the process of section 4.3.1 (Decision to Address Risks).

5.1. Organizational Measures

5.1.1. Asset Management

5.1.1.1. Responsibility for Assets

- Identify assets such as information systems, software, and information, and develop and maintain an asset inventory that clarifies the personnel-in-charge of managing, and usage restrictions (scope of permitted use) for each asset.
- In cases where information systems or their operation is replaced by external services, develop and maintain a list of external services to be used.
- Create network configuration diagrams, data flow charts, and other figures.
- Monitor and address to ensure that unauthorized assets are not connected or operated on the network.

5.1.1.2. Classification and Handling of Information

- Assign ratings to information from the perspectives of confidentiality, integrity, and availability, and manage it by labeling information media (paper, electronic).
- Implement necessary handling restrictions (for example, prohibition of duplication, taking out, and distribution) based on the life cycle of information.

5.1.1.3. Data Management

- Conduct desirable data management including appropriate protection of data and consideration of data storage locations according to the risk management of systems.
- When using new technologies such as Internet-based services (cloud services, etc.) in response to changes in the business environment, pay attention to domestic and foreign laws and regulations, evaluation systems, etc.

5.1.2. Supplier Management

- Organize the security requirements for mitigating the risks of suppliers and other sub-contractors accessing the assets of CI operators, etc., and agree on the requirements with the suppliers beforehand.
- Check periodically on the agreement items such as contracts related to service provision by suppliers, as well as review reports prepared by suppliers, and conduct audits.
- Manage changes in services provided by suppliers.
- Establish systems to promptly share information with suppliers and respond to the issues when incidents occur in the services provided by suppliers, or when vulnerabilities in

equipment are detected.

5.1.3. Operation Management

5.1.3.1. Procedures and Responsibilities of Operations

- Establish procedure manuals related to the operation of information systems, etc.
- Share the procedure manuals to deter operational errors and security standards violations.
- Establish prior approval procedures for updating information systems, etc.
- Separate the operational environment from the development and testing environments.

5.1.3.2. Protection from Malware

- Establish mechanisms for the detection and prevention of malware, as well as countermeasures and procedures for early recovery in the case of malware infection.

5.1.3.3. Backup

- Establish backup policies and procedures for system images, data, etc., and conduct backup recovery tests periodically.

5.1.3.4. Maintaining Logs

- Record and manage the event logs of information systems and work logs of operational personnel.
- Maintain logs to prevent them from intentional tampering or deletion by malicious persons or malware. For example, check for fraudulent activities on logs through periodic inspections based on the nature of the log.

5.1.3.5. Operational Software Management

- Be aware of and understand the individual configurations of software used in information systems, as much as possible, and strive to ensure their safety.
- Systematically update software to supported versions. If it is difficult to update to supported versions, take complementary measures.

5.1.3.6. Vulnerability Management

- Collect vulnerability information and confirm if it has any impact on information systems in operation.
- Conduct vulnerability scans periodically.
- Establish working policies and contents regarding the application of patches to information systems. If it is difficult to apply patches, take complementary measures such as strengthening the monitoring of information systems.

5.1.4. System Acquisition, Development, and Maintenance

- Include cybersecurity-related items in the requirements for acquisition, development, and improvement of information systems. Where necessary, utilize information systems that have received third-party certification, or products of trusted venders who have sufficient achievements in security measures and disclose the status of their measures.
- Establish procedures and prepare an environment for ensuring cybersecurity during the acquisition, development, and improvement of information systems. Conduct vulnerability assessments during acceptance verification of information systems, corresponding to the importance of those systems.
- When outsourcing system development to external contractors, check periodically with the contractors on the status of compliance with development policies that take cybersecurity into consideration.

5.1.5. Incident Management

- Appoint personnel responsible for incident management.
- Establish procedures for incident reporting within and outside the organization, evidence collecting, and other related activities.
- Establish mechanisms for utilizing the knowledge gained through addressing incidents to prepare for future incident readiness.

5.2. Personnel Measures

5.2.1. Employee Management

- Assign and manage employees involved in the development and operation of critical systems based on the results of risk assessments.

5.2.2. Contractor Management

- Incorporate requirements for the employees of the contractor[24] and items to comply with even after the end of the work consignment, into the contract with the contractor.
- Periodically check on the status of efforts by contractors and request them to make the necessary improvements.

5.2.3. Telework and Remote Control

- Implement measures to ensure cybersecurity related to telework and remote control.

5.2.4. Escalation

- Establish mechanisms for reporting promptly on security events discovered or suspected by employees through appropriate escalation.

[24] The details of requirements will be the same as those for managing employees of one's own organization.

5.3. Physical Measures

5.3.1. Domains that Require Security

- Manage domains that require security.
  - Set physical security boundaries.
  - Develop entry/exit management systems.
  - Verify and restrict items brought into the concerned domains.

5.3.2. Installation and Management of Facilities Less Likely to be Damaged by Disasters

- Implement disaster countermeasures, such as arranging facilities in a way that makes them less likely to be damaged due to disasters.

5.3.3. Device Management

- Lay out communication and power cables in consideration of the possibility of interception and damage.
- Establish systems for the prior authorization of the use, taking out, and disposal of documents and removable storage devices.

5.4. Technical Measures

5.4.1. User Access Control

- Control users and access rights to information systems and information, etc.
  - Define application routes, authorizers, workers, etc. for the official processes of registration, change, and deletion of users and access rights.
  - Periodically review user access rights.

5.4.2. Access Control of Information Systems, etc.

- Restrict access to information systems and information depending on the importance of the information and systems, based on the principles of least privilege and segregation of duties.
  - Limit the number of times of failed log-in.
  - Use strong passwords.
  - Utilize multi-factor authentication.

5.4.3. Information Management Using Cryptography

- Formulate policies for the use of cryptography and management of encryption keys.

5.4.4. Communication Security

- From the perspective of protecting the confidentiality and integrity of information, ensure network security through the use of dedicated lines and encryption technology,

implementation of security measures related to IPv6, network isolation, and detection of cyberattacks through logging and monitoring.

- When transmitting important information through means of communication, organize the policies and procedures for ensuring security, and agree on them with the recipients of the information.

5.4.5. Defense-in-depth

- Introduce defense-in-depth for terminals, networks, systems, or services that carry out important operations.
-

5.5. Measures Based on Trends

5.5.1. Ransomware Countermeasures

- Take vulnerability countermeasures by promptly applying patches.
- Manage assets, including those at overseas bases and supply-chains.
- Backup system software and data, and check periodically on the possibility of recovery from backups.
- Store backup data separately from networks.
- Segment networks based on roles, etc.
- Store logs, etc. that can be investigated after an attack.
- Build cooperative relationships with stakeholders such as vendors.
- Contact the responsible ministries and police in the event of an attack, and store information on the situation in a sequential time series.
- It is desirable to refrain strictly from the payment of money so as not to encourage ransomware attacks.

5.5.2. Measures During the Use of Cloud Services

- Review and deepen understanding of the specifications of the cloud services to be used.
- Understand Shared Responsibility Models,[25] and clarify the scope of responsibilities, etc. with cloud service providers.
- Check for errors in settings such as information disclosure.
- Verify the impact when service specifications are changed.
- Identify a wide range of stakeholders, and establish information sharing systems and incident response systems.
- Check the handling of data on the cloud service at the end of use of the cloud service.

[25] The concept that users and cloud service providers not only prescribe a point for demarcating responsibility, but also share operational responsibility.