**[Provisional Translation]**

The original texts of the Guidelines are prepared in Japanese, and this translation is only provisional. The translation is to be used solely as reference material to aid the understanding of the Guidelines and is subject to any future changes.

# Guidelines on Cybersecurity for the Financial Sector

## October 4, 2024

## Financial Services Agency

## Table of contents

# 1. Fundamental Principles

## 1.1. Fundamental Principles to Cybersecurity

Under Article 3 of the Act for Establishment of the Financial Services Agency (FSA), the FSA is tasked with ensuring the stability of financial functions and protecting depositors. Given that cyberattacks pose a threat to the interests of financial service users and may undermine the stability of the financial system, it is essential for the FSA to strengthen cybersecurity across the entire financial sector to fulfill its mission. Furthermore, financial institutions[1] are required under various financial laws[2] to ensure sound and appropriate business operations, etc. From the perspective of business soundness and appropriateness, securing cybersecurity is a critical responsibility.

In light of this, the FSA has promoted the strengthening of cybersecurity in the financial sector through dialogue and collaboration with the financial industry, as outlined in the "Policy on Strengthening Cybersecurity in the Financial Sector" (including its revised versions). Additionally, the FSA has specified key points to be considered in supervisory practices regarding the cybersecurity management frameworks of financial institutions in its comprehensive guidelines for supervision and administrative guidelines, etc. Based on these provisions, the FSA has conducted inspections and monitoring, etc., engaged in dialogue with individual financial institutions, and generalized the findings to share with the broader industry, thereby promoting efforts to strengthen cybersecurity across the sector.

Now, based on the results of past inspections and monitoring, as well as changes in the internal and external environment of the financial sector, the FSA has developed this more detailed guideline, separate from the existing comprehensive guidelines for supervision, etc. This section outlines the Fundamental Principles to cybersecurity expected of financial institutions, the roles of information-sharing organizations and central industry bodies, and the positioning and supervisory application of this guideline. Section 2 provides perspectives on governance, identification, defense, detection, response, recovery, and third-party risk management from a cybersecurity standpoint. For each area, the guideline clarifies "Fundamental response measures" and "Recommended measures" for financial institutions. Section 3 discusses the Fundamental Principles to collaboration between the FSA and relevant stakeholders and organizations.

(Note) "Fundamental response measures" refer to foundational actions that financial

[1] For the definition of "financial institutions" in this guideline, refer to Section 1.4.
[2] Examples include Article 12-2, Paragraph 2 of the Banking Act; Article 35-3 of the Financial Instruments and Exchange Act; and Article 100-2-1, Paragraph 1 of the Insurance Business Act.

institutions generally need to implement, often referred to as cyber hygiene practices[3].
"Recommended measures" refer to advanced practices that are desirable for institutions with significant potential impact on local communities and economies, etc., in the event of an incident, or best practices, etc., identified through dialogue, etc., with foreign authorities or financial institutions. These are examples that major financial institutions and major financial market infrastructures (FMIs') should consider.
Given the diversity in size and characteristics of financial institutions, this guideline does not mandate uniform responses. Institutions are expected to identify and assess cybersecurity risks, etc., based on their business environment, business strategy, and risk tolerance, and implement mitigation measures accordingly—as the risk-based approach.

The FSA will continue to conduct inspections and monitoring based on the risk-based approach, tailored to the size and characteristics of each financial institution, and verify their cybersecurity management frameworks. In doing so, institutions should assess the risks they face, prioritize responses based on importance and urgency, and implement mitigation measures within the constraints of available resources. At the same time, the FSA will share common challenges and best practices identified through inspections and monitoring with the broader industry via industry associations, thereby further promoting strengthening of cybersecurity across the financial sector.

## 1.2. Required Initiatives for Financial Institutions

### 1.2.1. Cybersecurity Management Framework

In Japan, the Basic Act on Cybersecurity stipulates the fundamental principles for related policies. One of its core philosophies is that the promotion of cybersecurity measures should be actively pursued through collaboration among various stakeholders, including the national government and critical infrastructure operators, etc. Under this Act, entities such as banks, life and non-life insurance companies, securities firms, and payment service providers are designated as critical social infrastructure providers (critical infrastructure operators). These operators are responsible for ensuring the stable and appropriate provision of services and are expected to deepen their understanding of the importance of cybersecurity and proactively work to secure it.

In addition to these designated operators, all financial institutions are required under laws such

[3] Cyber hygiene refers to efforts to instill basic cybersecurity practices across the organization, such as proper IT asset management and timely application of security patches.

as the Banking Act, Insurance Business Act, and Financial Instruments and Exchange Act to ensure sound and appropriate business operations, etc.—which includes securing cybersecurity.

When financial institutions operate as part of a group (including overseas location, etc.), they are expected to establish a consistent cybersecurity management framework across the group, taking into account differences in scale and characteristics of each subsidiary and location, to ensure cybersecurity for the entire group.

Moreover, to respond to ever-evolving threats, organizations must continuously and dynamically review their technical and organizational response frameworks. This requires proactive engagement from senior management, appropriate allocation of resources, and a shift from reactive responses (i.e., reviewing frameworks only after incidents occur) to proactive, ongoing improvements during normal operations. Cybersecurity cannot be ensured solely by the cybersecurity or IT departments. It must be addressed by the entire organization, led by senior management, through the development and operation of a comprehensive framework.

Given these circumstances, financial institutions must avoid adopting a risk management approach that merely focuses on formal compliance with this guideline. Instead, they are expected to take substantive and effective actions based on the intent of relevant laws, comprehensive guidelines for supervision, etc., and this guideline, etc. In doing so, institutions should also refer to other related guidelines[4].

### 1.2.2. Engagement and Understanding of Senior Management

Business disruptions caused by cyber incidents[5] can have a significant impact on customers and may severely undermine trust in financial institutions and the financial system. Given the nature of this risk, it is clear that cybersecurity is not merely an issue for IT or systems departments—it is a matter that may entail executive accountability. To minimize the impact on customers and the financial system and to achieve the earliest possible recovery when a cyber incident occurs, cross-functional coordination is essential. This includes collaboration among departments such as operations, planning, public relations, compliance, risk management, and internal audit.

[4] (Reference) related materials include:
- "The Cybersecurity Policy for Critical Infrastructure Protection" and "Guidelines for Developing Safety Standards for Cybersecurity in Critical Infrastructure" (Cybersecurity Strategic Headquarters),
- "FISC Security Guidelines on Computer Systems for Financial Institutions" (FISC),
- NIST Cybersecurity Framework (USA),
- The Profile by the Cyber Risk Institute (CRI, USA)

[5] The term "cyber incident" here is synonymous with "cybersecurity incident" as defined in comprehensive guidelines for supervision.

Moreover, proactive involvement by executive management is required—not just from frontline staff. In addition, coordination with external stakeholders such as customers, law enforcement agencies, information-sharing organizations, and regulatory authorities, etc., is also necessary. To enable such a comprehensive organizational response, strong governance must be established, and leadership from senior management is indispensable.

Directors and other executives bear responsibilities under the Civil Code, Companies Act, and various financial laws, etc. If inadequate cybersecurity management leads to damage to their organization or third parties, they may be held liable for breach of duty of care or neglect of duty, resulting in claims for damages.

### 1.3. Roles of Industry Associations and Central Organizations, etc.

When it comes to gathering threat intelligence and understanding the latest attack techniques, etc., in cyberspace, relying solely on individual financial institutions may not always be efficient or effective. This is particularly true for smaller institutions or those with limited business scope, which may face challenges in accumulating sufficient information and expertise to respond appropriately.

From the perspective of strengthening the overall cybersecurity posture of Japan's financial sector, it is desirable for industry associations and central organizations, etc., to play a central and leading role. By collaborating with authorities as needed, these entities can promote mutual assistance initiatives such as sharing reference information and case studies, supporting the development of cybersecurity frameworks, conducting exercises, scenario analysis[6], and human resource development. These efforts help improve the capabilities of financial institutions across the sector.

Accordingly, financial institutions are encouraged to actively utilize the expertise provided by mutual assistance organizations such as Financials ISAC Japan[7], which offer support in addressing technical challenges, sharing best practices, and analyzing trends in cyberattacks and vulnerabilities. Collaboration with other industries outside the financial sector is also recommended.

[6] Scenario analysis refers to the evaluation of cyberattack scenarios and their potential ripple effects, etc., used in risk assessments, testing, and exercises, etc.

[7] Financials ISAC Japan (Information Sharing and Analysis Center) is a mutual assistance organization established in August 2014 to promote cybersecurity information sharing and analysis among Japanese financial institutions, with the aim of enhancing the safety and security of the financial system.

For example, many cooperative financial institutions outsource the development and operation, etc., of core systems to shared centers or entrust the construction and operation, etc., of network systems—connecting to intra-industry or cross-industry systems—to central organizations or industry-specific centers. Similarly, networks including internet environments, etc., websites, and internet banking services are often jointly used through services provided by these centers. Given this shared infrastructure, the role of industry associations and central organizations, etc., becomes especially important in responding to system failures caused by cyberattacks. Therefore, each cooperative financial institution should leverage the business support functions of central organizations, etc., while central organizations, etc., themselves should work to consolidate and enhance their cybersecurity support services. This will help strengthen mutual assistance within each industry segment.

In addition, FMIs must manage risks posed by their participants, etc., to ensure stable service provision. From this perspective, these institutions may refer to this guideline when establishing reasonable participation, etc., requirements based on the risk environment.

### 1.4. Scope and Applicability, etc., of This Guideline

This guideline applies to all financial institutions and related entities subject to comprehensive guidelines for supervision, etc., with cybersecurity management. These include major banks, etc., regional and small and medium-sized financial institutions, insurance companies, small amount and short term insurance agents, financial instruments business operators, credit rating agencies, money lending business operators, prepaid payment instrument issuers, electronic money claim recording institutions, designated credit bureau, funds transfer service providers, financial market infrastructures , financial service intermediaries, funds transfer transaction analysis service providers , crypto-asset exchange service providers, bank agents, electronic payment service providers, electronic payment handling service providers, electronic payment instruments service providers, agricultural and fishery cooperative financial institutions, and financial instruments exchanges (collectively referred to as “financial institutions, etc.” in this guideline).

Unless otherwise specified, the definitions of terms used in this guideline should follow those provided in the comprehensive guidelines for supervision, etc., applicable to each type of business.

(Note) Provisions related to cybersecurity management within comprehensive guidelines for supervision, etc., are part of the broader framework for system risk management.

Therefore, in order to fully understand this guideline, it is recommended to also refer to the relevant sections of the comprehensive guidelines for supervision, etc., concerning system risk management as needed.

## 2. Cybersecurity Management Framework

### 2.1. Establishing a Cybersecurity Management Framework, etc.

#### 2.1.1. Formulation of Basic Policies and Regulations, etc.

*Fundamental response measures*

(1) The board of directors, etc., should recognize cybersecurity risks as part of the organization-wide risk management and formulate a basic policy for cybersecurity management. The basic policy should include, for example:
- Objectives and direction of security measures
- Responses to requirements from stakeholders, etc., (e.g., customers, local communities, shareholders, authorities) and legal/regulatory compliance, etc.
- Commitment from senior management

(2) The board of directors, etc., should acknowledge the increasing sophistication of cyberattacks and recognize the importance of cybersecurity in achieving business objectives. Based on stakeholders, etc., requirements and the internal/external regulatory environment, etc., the board of directors, etc., should establish an appropriate cybersecurity management framework. In addition, the cybersecurity management framework should undergo comprehensive evaluation and deliberation, such as through formal reviews conducted at least once per year[8] (with external expert reviews as necessary).

(3) Senior management should establish a cybersecurity management framework, including response measures such as:
- Systems for collecting, sharing, and analyzing early warning information through information-sharing organizations, etc.
- Monitoring systems such as Security Operations Center (SOC)[9], etc., including use of external resources
- Crisis management systems, etc., designed for cyberattacks, including reporting and public relations structures, emergency response such as internal CSIRTs (Computer

[8] Where appropriate, organizations are encouraged to refer to the Cyber Risk Handbook for Directors published by the Japan Business Federation (Keidanren).

[9] A Security Operations Center (SOC) is an organization that monitors networks, servers, and other devices to detect and analyze cyberattacks.

Security Incident Response Teams), etc., and early warning mechanisms

(4) Based on the basic cybersecurity policy, senior management should formulate a cybersecurity strategy and implementation plan[10] (including multi-year plans), ensuring their effectiveness and adequacy. These plans should be reviewed annually or when significant changes occur.

(5) When introducing financial products or services or promoting digital transformation, senior management should simultaneously promote cybersecurity initiatives, including "security by design"[11].

(6) Senior management should position cybersecurity as a key issue in management policy, demonstrate leadership in fostering a cybersecurity-conscious organizational culture, and promote measures based on an understanding of critical operations[12] and risks. This includes managing progress, directing additional measures, and allocating necessary resources.

(7) Senior management should clearly define the roles, responsibilities, and authority of cybersecurity departments and related personnel. Personnel arrangements should ensure continuity of operations despite sudden resignations or transfers, etc. A person responsible for overseeing cybersecurity (e.g., CISO) should be appointed under the responsibility of senior management.

(8) Senior management should require the relevant departments, etc., to report at least once a year on:
- The status of cybersecurity risks surrounding the organization (e.g., incidents within the organization, industry-wide incidents, critical vulnerability information)
- Results of cybersecurity risk assessments (including external expert evaluations as necessary)
- Progress of the implementation plan

(9) Senior management should continuously improve the cybersecurity management framework based on audit results, stakeholders(e.g., customers, local communities, shareholders, and regulatory authorities) requirements, and changes in the domestic/international regulatory environment, etc.

---

[10] The implementation plan should include specific measures, schedules, and execution frameworks. Examples of measures that may be included are:
- Risk responses developed based on the results of risk assessments
- Human resource development
- Incident response (e.g., conducting drills and training)
- Strengthening third-party risk management

[11] This refers to the concept of incorporating security requirements from the planning and design stages of financial products and services.

[12] In this guideline, "critical operations" refer to financial services whose disruption could cause significant adverse effects on the operations of financial institutions, users, or the financial system.

*Recommended measures*

(a) To ensure appropriate governance over cybersecurity, which is essential for sound management decisions, have senior management access to sufficient cybersecurity knowledge, including the use of external experts. This includes clarifying the roles and responsibilities of each department involved in cybersecurity[13] under the commonly adopted three lines of defense model—business units, risk management, and internal audit—and establishing mechanisms for verification through external experts.

(b) The board of directors, etc., positions cybersecurity risk as part of integrated risk management and define the organization's risk appetite[14] and risk tolerance[15].
(Reference) FSA, "Discussion Paper on Ensuring Operational Resilience", (April 2023)

(c) Senior management, to the extent possible, publicly communicates the significance of the organization's cybersecurity initiatives to internal and external stakeholders, while carefully considering the potential risk of encouraging attackers. Possible items for disclosure include:
- Basic policy on cybersecurity management
- Scope and level of services maintained
- Risk management framework
- Expertise of cybersecurity officers
- Resource allocation
- Risk identification and response planning
- Emergency response and recovery systems
- Status of cybersecurity incidents

(d) Senior management requires relevant departments, etc., to report at least twice a year on the following:
- Key Performance Indicators (KPIs) [16] and Key Risk Indicators (KRIs)[17] related to cybersecurity

(e) Senior management appoints a person with sufficient knowledge and experience in cybersecurity as the Chief Information Security Officer (e.g., CISO) or equivalent position, who is in a position to report directly to senior management on a daily basis. Establish a relationship that enables direct communication between the CISO and top management

[13] Refer to Sections 2.1.4 and 2.1.5.
[14] Risk appetite refers to the types and total amount of risk that an organization is willing to proactively accept within its risk capacity, in order to achieve its strategic goals and business plans.
[15] Risk tolerance refers to the minimum level of service that must be maintained for financial services identified as critical operations, assuming that service disruptions will inevitably occur despite all preventive measures, and based on the organization's established risk appetite.
[16] Examples of KPIs: reporting rate for targeted email training, vulnerability response rate, progress rate of information asset inventory, training participation rate, etc.
[17] Examples of KRIs: number of attempted cyberattacks, number of audit findings, number of incidents, number of unresolved vulnerabilities, etc.

during both normal operations and emergencies. To that end, senior management provides the CISO with the necessary support, authority, and resources to fulfill their role. Additionally, business units appoint responsible personnel with sufficient cybersecurity knowledge and experience to facilitate smooth coordination with the CISO.

### 2.1.2. Development of Policies and Business Processes, etc.

*Fundamental response measures*

(1) Senior management should establish regulations and operational processes related to cybersecurity and conduct reviews at least once a year. These regulations, etc., should include, for example, the following items:
- Information asset management
- Risk assessment
- Vulnerability management
- Vulnerability assessment and penetration test
- Exercises and training
- Authentication and access control
- Education and training
- Data management
- Logging and log management
- Security by design
- Technical measures (e.g., physical security, network security)
- Incident response and recovery
- Third-party risk management

(2) Senior management should establish organization-wide reporting, communication, consultation channels, and command structures for cybersecurity risk management, including risks originating from third parties[18].

### 2.1.3. Securing Resources and Developing Human Talent

[18] A third party refers to another organization with which the entity has a business relationship or contractual arrangement for the purpose of providing its services. Examples include system subsidiaries, external contractors such as vendors, cloud service providers, money transfer service partners, and API integration partners. An external contractor refers to an organization to which operations are outsourced. This includes vendors of systems outsourced by financial institutions to provide financial services (including shared centers). Even in cases where no formal outsourcing contract exists, if the actual arrangement is equivalent to outsourcing, or if the outsourced operations are conducted overseas, such cases are also considered to fall under the definition of external contractors.

*Fundamental response measures*

(1) Senior management should allocate appropriate resources by assigning personnel with specialized expertise to departments responsible for cybersecurity, etc., and by providing necessary budget allocations, based on the importance of cybersecurity.

(2) Senior management should formulate plans for the development and retention of human resources that are consistent with the basic policy on cybersecurity management. These plans may include human resource development plans, recruitment plans, and education/training programs. A sustainable personnel policy should be established, taking into account factors such as succession planning for retirees. Personnel assignments should be made from a medium- to long-term and strategic perspective to avoid transfers that hinder human resource development for employees with the necessary aptitude and motivation. In addition to recruiting and utilizing external talent, organizations should also consider the development of internal personnel by providing educational opportunities both within and outside the organization.

(3) Senior management should actively participate in training and exercises, etc., aimed at acquiring the skills and knowledge necessary to enhance governance over cybersecurity and foster a cybersecurity-conscious organizational culture. This may include awareness programs and training sessions conducted by internal departments or external organizations specifically designed for executives.

(4) Regarding human resource development, the organization should systematically secure personnel—including external experts—such as:
- Personnel capable of assessing cybersecurity risks associated with the introduction of new digital technologies
- Personnel responsible for planning and formulating cybersecurity strategies and implementation plans
- Personnel engaged in cybersecurity-related training and human resource development
- Personnel involved in system design and development from a cybersecurity perspective
- Personnel responsible for collecting threat and vulnerability information and implementing vulnerability countermeasures
- Personnel engaged in log monitoring and surveillance
- Personnel responsible for responding to cybersecurity incidents
- Personnel conducting forensic investigations[19], etc.
- Personnel performing vulnerability assessments and penetration testing
- Personnel conducting cybersecurity audits

[19] This refers to an investigative method that analyzes electronic data stored in electronic devices or digital media to uncover evidence of misconduct or other illicit activities.

### 2.1.4. Oversight by Risk Management Department

*Fundamental response measures*

(1) The risk management department should monitor and provide oversight of whether the cybersecurity management framework is functioning effectively, from a position independent of the business units, etc.
(2) The risk management department should report on the execution status of cybersecurity management to the executive in charge of risk management (e.g., the Chief Risk Officer, CRO) and to the board of directors, etc.

*Recommended measures*

(a) Assign personnel with appropriate knowledge and expertise in cybersecurity, etc., to the risk management department.

### 2.1.5. Internal Audit

*Fundamental response measures*

(1) The internal audit department should, from an independent standpoint and based on a risk-based approach, formulate an internal audit plan related to cybersecurity and conduct internal audits on cybersecurity—including the status of cybersecurity system implementation and operation, incident response and recovery, compliance with laws and regulations, and third-party risk management—utilizing external experts as necessary.
(2) The internal audit department should promptly report any significant findings identified through internal audits to the President and the Board of Directors, etc., and accurately monitor the status of improvements made in response to those findings.

*Recommended measures*

(a) Assign personnel with appropriate knowledge and expertise in cybersecurity, etc., to the internal audit department.

## 2.2. Identification of Cybersecurity Risks

### 2.2.1. Information Assets[20] Management

*Fundamental response measures*

(1) Procedures for managing information assets according to their lifecycle, etc., (acquisition, use, storage, and disposal) should be established and reviewed as necessary.
(2) Information assets should be classified and managed based on their level of importance (Confidentiality, Integrity, Availability) to determine appropriate protection priorities.

For information asset management, refer also to item[21] "Management of information security" in the comprehensive guidelines for supervision, etc., for each business type.

#### 2.2.1.1. Information Systems and External System Services

*Fundamental response measures*

(1) The organization should establish and maintain ledgers, etc., to appropriately manage information systems and external system services, and define maintenance procedures to ensure comprehensive and up-to-date oversight. This should include information systems managed by individual departments. These ledgers, etc., should be cross-referenced with those specified in Sections 2.2.1.2 and 2.2.1.3.

#### 2.2.1.2. Hardware, Software, etc.

*Fundamental response measures*

(1) Establish procedures and ledgers, etc., (including organization's assets managed by external contractors) to appropriately manage hardware (including network devices and appliance products [22]) and software (including virtual machines),etc., and define maintenance

[20] Information assets refer to: (i) information systems and external system services (such as external contractors and cloud services); (ii) their components, including hardware, software, etc. and stored information (data); and (iii) networks.
[21] For example, in the Comprehensive Guidelines for Supervision of Major Banks, etc., refer to item III-3-7-1-2-(4) "Management of information security".
[22] Refers to products designed for specific purposes, in which dedicated software is permanently embedded into the device.

procedures to ensure comprehensive and up-to-date oversight. The ledgers, etc., should include the following items:

- Support period (planned end-of-support date, possibility of extension)
- For software, version information

*Recommended measures*

(a) Include multifunction printers and specialized-purpose devices[23] as items to be managed in the ledgers, etc.
(b) Where necessary, include third-party assets as items to be managed[24].
(c) When classifying information assets related to hardware and software, etc., ensure that risk management takes into account dependencies on third parties for critical operations.
(d) Identify and appropriately address information assets, etc., that are currently unmanaged, such as personally owned devices and unauthorized cloud services (e.g., shadow IT), by either including them in the management scope or discontinuing their use.
(e) Prepare a Software Bill of Materials[25] (SBOM) for the following:
    - Software developed in-house
    - Services in use (if the service provider offers an SBOM)

#### 2.2.1.3. Information (Data)

*Fundamental response measures*

(1) Establish ledgers, etc., tools to appropriately manage customer information, confidential information, and other data, and define maintenance procedures to ensure comprehensive and up-to-date oversight.

#### 2.2.1.4. Data Flow Diagrams and Network Diagrams

*Fundamental response measures*

[23] In accordance with the definitions provided in the "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies" this refers to components of information systems used for specific purposes—such as video conference, IP phone, network camera, entry control systems, facility management systems, and environmental monitoring systems—that are either connected to communication networks or equipped with built-in electromagnetic recording media.
[24] Note that the inclusion of third parties should be considered based on a risk-based approach (refer to Section 2.6).
[25] Refers to a machine-readable list that includes software components and their dependencies.

(1) Create data flow diagrams and network diagrams to appropriately manage data flows and networks from a comprehensive perspective, and define maintenance procedures to ensure up-to-date visibility. (These should include mobile connections, external connections, third parties connected to the network, and internal systems.)

### 2.2.2. Risk Management Process

#### 2.2.2.1. Collection and Analysis of Threat and Vulnerability Information

*Fundamental response measures*

(1) In addition to collecting threat information specific to the organization (e.g., cybersecurity incidents), gather threat information on cyberattacks (including those caused by negligence or internal misconduct) and vulnerability information (including vulnerabilities identified through exercises and training, etc.) from public institutions, information-sharing organizations, and third parties.
(2) Organize and analyze the collected information, and assess the impact of such cybersecurity risks on the organization's business and information assets.
(3) Review the sources and methods of information collection and analysis at least once a year, and make improvements as necessary.

*Recommended measures*

(a) Actively participate in specialized information-sharing activities such as Financials ISAC Japan, as well as cross-industry and international organizations, etc., to collect and share threat and vulnerability information relevant, etc., to the organization's operations.
(b) When conducting threat analysis, include serious but plausible cyberattack scenarios, even if they have not occurred in the past.
(c) When collecting information, take into account the broader context surrounding the organization, including emerging technologies (e.g., AI, quantum computing), geopolitical developments, disinformation, and industry trends.

#### 2.2.2.2. Identification and Assessment of Risks

*Fundamental response measures*

(1) Establish procedures for identifying and assessing cybersecurity risks.
(2) Based on threat and vulnerability information, assess cybersecurity risks at least once a year by considering both the likelihood of cyberattacks and their potential impact on the organization's business and information assets. Additionally, conduct evaluations when significant threats or vulnerabilities are identified, or when launching new products or services.
(3) In conducting risk assessments, consider threats such as the risk of perimeter-based security being breached and internal misconduct, and include risks to systems located within internal network segments.

*Recommended measures*

(a) In conducting risk assessments, identify critical operations and consider the interdependencies among internal personnel, facilities, systems, and third parties necessary to maintain those operations.
(b) Use scenario analysis, tabletop exercises, or stress testing, etc., to identify vulnerabilities within the organization and assess potential impacts on critical systems and operations. Scenarios should include a diverse range of serious but plausible cyberattack scenarios.

#### 2.2.2.3. Risk Response

*Fundamental response measures*

(1) Based on the results of risk assessments, prioritize risks and formulate a risk response plan (including risk avoidance, risk mitigation, risk acceptance, and risk transfer).
(2) Procedures should be established for handling risk response exceptions and for the acceptance of certain risks. Obtain approval from senior management, etc., when implementing such procedures.
(3) Report the risk response plan (including evaluation of residual risks) to senior management on a regular basis (or confirm that the plan is within the risk appetite set by the board of directors, etc.).

#### 2.2.2.4. Efforts Toward Continuous Improvement

*Fundamental response measures*

(1) Evaluate the cybersecurity risk assessment process at least once a year in response to changes in internal and external environments, and implement continuous improvement activities.
(2) Assess and improve the effectiveness of the cybersecurity risk management framework and its operational status at least once a year.
(3) Improve procedures, etc., in accordance with relevant processes based on recommendations, findings, and lessons learned from exercises and training, vulnerability assessments and penetration testing, audits, risk assessments, and actual incidents.

*Recommended measures*

(a) Evaluate and improve procedures related to monitoring and detection at least once a year, in response to changes in the threat landscape, technological advancements, and lessons learned.
(b) Establish a mechanism for measuring and evaluating performance indicators (KPIs) and risk indicators (KRIs), and reporting them to senior management. Set specific goals and achievement metrics, and identify progress and challenges in improvement efforts.

### 2.2.3. Vulnerability Management of Hardware and Software, etc.

*Fundamental response measures*

(1) Establish and periodically review procedures, etc., for managing vulnerabilities in hardware and software, etc. These procedures, etc., should include the following elements:
- Sources of vulnerability information and the process for obtaining such information (including public institutions, information-sharing organizations, and third parties)
- Evaluation of the severity, impact, and scope of the obtained vulnerabilities
- Determination of response methods and deadlines, and management of response status
- Decision-making process for exceptional handling

(2) Determine whether a response is necessary based on the procedures, etc., for managing vulnerabilities in hardware and software.
(3) Organizations should establish deadlines for implementing patches and other remedial measures based on the criticality of systems, the level of risk, and the severity of vulnerabilities, and should maintain records of implementation status. (For systems with high-risk configurations—such as those lacking network segmentation between business and internet-facing environments—patch impact assessments should be conducted, and

patches should be applied either promptly or within a defined timeframe.) In cases where patching or other remedial actions are exceptionally not carried out, formal approval must be obtained from senior management, etc., along with a documented assessment of the associated risks.

(4) When a highly severe vulnerability is identified, promptly identify affected systems based on asset inventories of information systems, hardware, and software, etc., and take appropriate action (Refer to sections 2.2.1.1 and 2.2.1.2.).

(5) Systems managed by group companies and overseas offices must also be included within the scope of vulnerability response, particularly in cases involving high-severity vulnerabilities.

(6) For critical vulnerabilities, manage vulnerability responses for systems owned by critical third parties[26] (including shared systems). Consider utilizing third-party assurance reports (e.g., SOC 2) or contractual documents, etc., for management purposes.

*Recommended measures*

(a) For serious vulnerabilities, manage systems owned by third parties including cloud service providers (excluding the third party mentioned in (6) above) to address the vulnerabilities.In managing such matters, it may be appropriate to utilize third-party assurance reports and contractual documentation, etc.

### 2.2.4. Vulnerability Assessment and Penetration Testing

*Fundamental response measures*

(1) Regularly conduct vulnerability assessments and penetration tests to identify and improve system vulnerabilities and security issues, taking into account factors such as risk level and system importance. Additionally, establish and periodically review related procedures, etc. These procedures should consider the following points:

- Define the scope of vulnerability assessments (including devices directly connected to external networks, such as VPN equipment), frequency, timing (including pre-release of systems), and implementation steps.
- For publicly accessible websites (e.g., corporate websites, internet banking sites, and

[26] "Important third parties" refers to third-party entities that the organization recognizes as critical to its business operations.

public APIs), conduct both platform assessments[27] and web application assessments[28].
- Conduct vulnerability assessments for mobile applications.
- In high-risk configurations (e.g., when business networks and internet-facing networks are not separated), perform vulnerability assessments on critical internal systems (e.g., Active Directory servers and file servers).
- Prioritize identified issues, determine response methods and deadlines, and manage the status of responses.

  Findings of significant importance from vulnerability assessments and penetration tests should be promptly reported to senior management, etc.

*Recommended measures*

(a) Include VPN networks and internal environments that are not directly connected to the internet in the scope of vulnerability assessments and penetration tests.

(b) Regularly conduct threat-led penetration testing (TLPT). When conducting TLPT, consider the following points:
- Select vendors with the necessary experience and skills (including background checks on testers' qualifications and career history, etc.).
- Use techniques that reflect the level of sophistication employed by real-world attackers, based on threat intelligence.
- Consider serious but realistic threat scenarios in the test plan that could impact services provided to stakeholders, etc.
- The testing process should include an evaluation of the incident response capabilities of the defensive team (Blue Team).(e.g., their ability to detect, report, contain, and mitigate threats, etc.)
- Conduct tests in the production environment without prior notice to the defense team (Blue Team).
- Report identified issues to senior management and carry out improvement activities.

  (Reference) FSA, "Report on TLPT in foreign countries" (May 2018), FISC, "The Guide for Financial Institutions to Implementing TLPT" (September 2019), FSA, "Analytical Report on Financial Institutions' IT System Failures" (June 2024), Appendix 1: Column on TLPT best practices and challenges in financial institutions

(c) Conduct penetration tests by internal personnel who are well-acquainted with the organization's system environment, including tests by Red Teams (attackers in TLPT).

[27] This refers to the investigation of potential flaws on the server that forms the foundation of a web application, such as the presence of easily guessable passwords or misconfigurations in the operating system or middleware.

[28] This refers to the investigation of potential flaws arising from the design and implementation of a web application, such as SQL injection or cross-site request forgery (CSRF).

(d) Periodically review the methods and results of penetration tests, and consider changing test vendors to gain fresh and independent perspectives.

### 2.2.5. Exercises and Training

*Fundamental response measures*

(1) Regularly conduct exercises and training (including participation in exercises and training hosted by other organizations)[29] to verify the effectiveness of the organization's cyber incident response plan and contingency plan, identify issues, and continuously improve them. Where necessary, consider involving external contractors in the exercises and participating in cross-industry exercises.
(2) Ensure that senior management, the person responsible for overseeing cybersecurity (e.g., CISO), and heads of business departments are directly involved in cyber exercises and training, etc., and are informed of the results.
(3) Include scenarios in exercises and training that could realistically occur and have a serious impact on customers.
(4) Through exercises and training, regularly verify the effectiveness of the cyber incident response plan and contingency plan from a business continuity, etc., perspective, and revise them based on the issues and lessons learned.
(5) Review the methods and scenarios, etc., of exercises and training in accordance with the latest threat trends, etc.

*Recommended measures*

(a) In recovery training using actual equipments, etc., include verification of the appropriateness of system and data recovery procedures, as well as the validity of recovery objectives such as the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
(b) Conduct exercises and training using scenarios in which incidents have a large-scale and prolonged impact on the organization, or cause connection failures, etc., with exchanges, clearinghouses, or settlement institutions—resulting in serious ripple effects across the entire financial system.
(c) For improvements based on issues identified through exercises and training, either conduct follow-up exercises, etc., to verify their effectiveness or obtain approval from senior

[29] Participants and other related parties of financial market infrastructures should also be included in the scope of exercises and training.

management, etc., to accept any residual risks.

(d) Combine various types of exercises and training (e.g., internal drills, vendor-provided training, industry-specific exercises, and those hosted by authorities) taking into account their respective scale and characteristics.

## 2.3. Cyberattack Defense

*Fundamental response measures*

(1) Implement Defense in Depth by combining various countermeasures, including perimeter network protections to prevent unauthorized intrusions, internal network controls to prevent misuse of systems, and measures to prevent information leakage to external parties.

### 2.3.1. Authentication and Access Management

*Fundamental response measures*

(1) Establish and regularly review policies and procedures, etc., related to authentication and access rights. These should take into account the following considerations:
   - Restrict user (including system) access privileges to the minimum necessary, considering separation of duties.
   - Manage the account lifecycle (establishment, active use, termination), conduct regular account inventories and activity reviews, and prevent unauthorized use of accounts.
   - Strictly control and manage the use of privileged accounts (e.g., multi-factor authentication, dual-control for operations, time-based access restrictions).
   - Appropriately manage access rights granted to external contractors.

(2) Grant system access rights only to individuals who have a legitimate business need, have received approval, have undergone appropriate training, and are properly managed. Access rights to devices and systems should be granted based on the importance of the system and information.

(3) Properly manage device IDs and authentication credentials (including embedding credentials in APIs). (e.g., changing default passwords, enforcing password strength requirements, automatically expiring unused IDs, and conducting regular access reviews by system administrators, etc.)

(4) Verify the appropriateness of user access rights before authenticating IDs and granting system access. Implement measures to identify users who access the system, log processing

activities, and correlate user actions with system responses.

(5) Authentication requirements (e.g., multi-factor authentication, risk-based authentication, etc., and other risk mitigation measures at the time of authentication) should be determined based on the criticality of systems and information assets. Use multi-factor authentication for remote access to critical systems.

(6) Utilize mechanisms and initiatives to prevent unauthorized activities by third parties, such as email domain authentication (SPF/DKIM/DMARC), secure file exchange functions, and customer support and awareness activities (e.g., alerts and seminars).

(7) Ensure confidentiality, integrity, and authenticity in authentication and authorization across systems and security boundaries, including single sign-on and external authentication integrations, etc.

(8) Manage, protect, and record physical access to high-security areas and critical rooms, such as computer rooms and data storage facilities.

### 2.3.2. Education and Training

*Fundamental response measures*

(1) Regularly provide cybersecurity awareness education and training to all officers and employees, including senior management, tailored to their roles and responsibilities.

(2) Ensure that personnel from third-party organizations receive the necessary cybersecurity education and training to perform their duties appropriately[30]. This may include content related to incident response and recovery plans specific to financial institutions. This requirement may also be fulfilled by the financial institution confirming that the third party conducts internal education and training.

(3) Implement initiatives to raise customer awareness of cybersecurity threats and promote cybersecurity awareness, as needed (e.g., posting phishing alerts on the website).

(4) Regularly provide education and training to personnel in IT and security departments to maintain up-to-date knowledge and skills regarding evolving threats and countermeasures, etc.

(5) Ensure that all employees have access to necessary education and training, etc., opportunities to respond appropriately if they become involved in an incident. Additionally, regularly provide training to relevant personnel on their roles and operational procedures in incident response and recovery plans.

[30] It should be noted that the third parties to be covered must be considered based on risk. (Refer to Section 2.6)

*Recommended measures*

(a) If forensic investigations, etc., are conducted internally, ensure that the relevant personnel maintain and enhance their skills and knowledge.
(b) If vulnerability assessments or penetration tests are conducted internally, ensure that the relevant personnel maintain and enhance their skills and knowledge.

### 2.3.3. Data Protection

*Fundamental response measures*

(1) Establish data management policies based on the importance of the information and the inherent risks of the technological environment in which it is used. These policies should include data handling and storage practices, adoption of appropriate encryption methods, lifecycle management and protection of encryption keys and digital certificates, and procedures for responding to key compromise.
(Reference) CRYPTREC "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)" (Last updated: May 2024)
(2) Classify data according to its importance and protect it in accordance with the relevant management policies (e.g., encryption, authentication, data masking, and access control).
(3) Establish and implement management procedures for the protection and use of external storage media, including usage restrictions, encryption, and malware scanning.
(4) Appropriately manage data throughout its entire lifecycle (e.g., disposal of media, secure data deletion, and the process of acquisition, return, and disposal of data by external contractors).
(5) Develop and implement backup policies, etc., based on the importance of systems and information, including requirements for backup, isolation and protection of backup data, integrity verification, and recovery testing, etc. For clearing and settlement institutions, establish agreements with relevant parties regarding data sharing, as necessary, to ensure the integrity of backup data.
In particular, considering the risk of ransomware attacks, review the duration and frequency of backups. Given that some types of ransomware search for and delete backup files within the same network, implement tamper-resistant backup systems and store, etc., backups in multiple environments or media that are isolated from the internal network.

For information asset management, refer also to the "Management of information security" section in comprehensive guidelines for supervision, etc., specific to each business sector.

*Recommended measures*

(a) Implement Data Loss Prevention (DLP) [31]solutions or equivalent measures to monitor and protect against data leakage (including theft or destruction of confidential data) by employees or external parties.
(b) Establish policies and procedures, etc., for data governance based on legal responsibilities and the importance of information as an organizational asset.

### 2.3.4. System Security Measures

#### 2.3.4.1. Hardware and Software Management

*Fundamental response measures*

(1) Configure systems to provide only the necessary functions, such as ports, protocols, and services.
(2) Establish procedures to ensure cybersecurity during system maintenance, including approval processes for remote and on-site maintenance personnel, work procedures, tools used, and replacement parts.
(3) Plan and safely execute the decommissioning or upgrading of hardware and software upon the end of support. If updating software to a supported version is difficult, implement compensatory measures and develop a transition plan to systems and business processes that use software with readily available support—and execute the plan steadily.
(4) Protect systems from malware infections. For example, consider the following measures:
    - Deployment of anti-malware software and automatic updates of malware signatures and behavior-based detection profiles.
    - Enabling protective features against malicious code (e.g., JavaScript, ActiveX, VBScript, PowerShell).
    - Detection, isolation, and blocking of malware or links to malicious website within email messages.
    - Restrictions on access to malicious websites, unauthorized use of social networking services, file-sharing services, etc.

*Recommended measures*

[31] DLP (Data Loss Prevention) is a tool designed to identify, monitor, and protect sensitive information.

(a) When using third-party libraries, middleware, or hardware in systems, select secure products provided by vendors that incorporate secure development practices, such as security by design and security by default[32], to ensure they do not contain backdoors or other intrusion paths.
(b) Include cybersecurity risks related to hardware (e.g., risks of unauthorized firmware installation) in the supply chain risk assessment.
(c) Ensure the authenticity of hardware (e.g., devices, firmware, UEFI or BIOS) and implement measures to prevent unauthorized modifications, such as tamper detection mechanisms.
(d) Establish secure procurement standards, etc., for hardware acquisition. Within procurement and transaction standards, require suppliers or business partners to comply with applicable laws, internal security or ethical standards. Create and maintain supplier or sanction lists based on laws, internal policies, and international sanctions (e.g., UN sanctions), and conduct procurement accordingly.

#### 2.3.4.2. Logging and Log Management

*Fundamental response measures*

(1) Establish and regularly review procedures for log collection, monitoring, and storage. These procedures should include, for example, the following items:
- Contents to be recorded in logs
- Scope of logging (e.g., monitored hardware, software, services)
- Access control for logs
- Monitoring methods
- Measures to prevent log tampering
- Retention period
- Storage methods

(2) Regularly or as needed, verify the appropriateness of event logs from information systems and operation logs from system administrators.

#### 2.3.4.3. Security by Design

*Fundamental response measures*

[32] Security by default refers to the concept that users (including customers) can use IT products—especially software—safely immediately after purchase, without incurring additional costs or effort.

(1) Implement “Security by Design” by incorporating security requirements from the planning and design stages of financial products and services. Throughout the entire service flow, assess risks and implement countermeasures, including those involving critical third parties.
(2) Verify that critical third parties providing systems to your organization have the capability and structure to implement Security by Design.
(Reference) Digital Agency “Security by Design Guidelines for Government Information Systems” (January 2024)

*Recommended measures*

(a) Establish and operate a management process for Security by Design, taking into account the following points:
- Define and implement secure coding standards.
- Clearly specify security requirements such as data confidentiality, access control, and event log collection.
- Develop design standards for security technologies and architectures.
- Conduct vulnerability assessments of application software both before and after release on a regular basis.
- Utilize tools (e.g., source code analysis tools) to prevent and detect vulnerabilities early in the development process.

### 2.3.4.4. Infrastructure (e.g. Network) Technical Measures

*Fundamental response measures*

(1) To prevent unauthorized access, implement appropriate intrusion prevention measures (e.g., physical or logical separation) at the connection points between external networks (e.g., open networks and remote access) and internal networks. Also, apply intrusion prevention measures to data transfers between external and internal networks.
(2) Regularly inspect and update network device configurations (e.g., firewall policies, ports, protocols), including during system environment updates. Firewalls should be configured to allow only necessary communications.
(3) Ensure network security by using, etc., dedicated lines or encryption technologies to protect the confidentiality and integrity of information, etc.
(4) Implement proper authentication and access control mechanisms for wireless LAN networks to prevent unauthorized use.
(5) Restrict and properly manage systems subject to remote access, such as those used for

remote work or vendor maintenance. This includes session timeouts, user authentication, and logging (collection, storage, and monitoring, etc., of access and communication data). For critical systems, use multi-factor authentication and encrypted connections.

*Recommended measures*

(a) Enhance the resilience of organizational communications and network services through measures such as protection against DDoS/DoS attacks, cybersecurity for DNS, and control of alternative communication routes.
(b) Separate development and testing environments from the production environment, and prevent unauthorized access or tampering with information assets.
(c) Micro-segment the network to prevent lateral movement of malware and contain the spread of damage from cyberattacks.

#### 2.3.4.5. Measures When Using Cloud Services[33]

*Fundamental response measures*

(1) Review and understand the specifications of the cloud services being used.
(2) Understand the shared responsibility model [34] and clearly define the scope of responsibilities, etc., between your organization and the cloud service provider.
(3) Verify that there are no misconfigurations related to information disclosure settings. When confirming the appropriateness of configurations, consider using system audits by experts or diagnostic services that automatically detect misconfigurations, etc., as needed.
(4) Assess the impact of any changes in service specifications according to the division of responsibilities.
(5) Identify all relevant stakeholders and establish frameworks for information sharing and incident response.
(6) Confirm the handling of data stored on cloud services upon termination of service usage, including logical data disposal.

### 2.4. Detection of Cyberattacks

*Fundamental response measures*

[33] (Reference) Also refer to the "Guidelines for Appropriate Configuration in the Use and Provision of Cloud Services" published by the Ministry of Internal Affairs and Communications.
[34] The shared responsibility model refers not only to the delineation of responsibilities between users and cloud service providers, but also to the concept of jointly sharing operational responsibilities.

(1) Establish and, as necessary, review procedures, etc., for monitoring, analyzing, and reporting indicators of cyberattacks, such as anomalies and Indicators of Compromise (IoCs). These procedures should also include monitoring of cloud services, in consideration of the risk that such services may become entry points for cyberattacks, and in accordance with the shared responsibility model. Monitoring of cloud services should include reviewing reports, etc., provided by cloud service providers regarding their system monitoring status.
(2) Implement appropriate monitoring and analysis measures in response to cyber threat levels to reduce associated risks. If these measures are outsourced, ensure that the organization understands the specific countermeasures implemented by the service provider. If any areas lacking sufficient countermeasures are identified, take appropriate action to address them.

### 2.4.1. Monitoring

*Fundamental response measures*

To detect signs of cyberattacks, continuously monitor the following:
(1) Hardware and software, such as:
- Connection of unauthorized hardware or hardware that violates internal policies to the network
- Installation of unauthorized software
- Tampering of software or firmware during updates, etc.
- Suspicious behavior on servers or endpoints
- Status of software patch application

(2) Networks, such as:
- Unauthorized intrusions into internal networks (e.g., using IPS[35] or IDS[36])
- Anomalous network flows or traffic caused by DDoS attacks, etc.
- Unauthorized or unusual network connections and data transfers
- Connections to malicious websites, unauthorized social networking services, or file-sharing services, etc.

(3) Regarding access to systems by personnel, including executives and staff, appropriate monitoring mechanisms should be established, such as the following:
- Suspicious behavior such as access patterns that deviate from normal usage

[35] IPS (Intrusion Prevention System) refers to a system equipped with functionality to automatically block detected unauthorized communications.
[36] IDS (Intrusion Detection System) refers to a system that monitors network traffic and detects and alerts on suspicious communications, such as unauthorized intrusions or malware.

(4) Access to systems by external service providers (e.g., for maintenance)
(5) Analyze whether signs of cyberattacks constitute an incident, including assessment of impact and severity, and promptly report to the appropriate responsible personnel.
(6) Regularly verify the validity of alert thresholds and criteria, etc., used to detect signs of cyberattacks.
(7) Monitor entry and suspicious activity in data centers and server rooms.

*Recommended measures*

(a) Implement mechanisms to detect early-stage attacks using decoy accounts or servers.
(b) Conduct continuous monitoring (24/7) based on the nature of customer services provided.
(c) Utilize tools such as SIEM[37] to aggregate multiple sources of monitoring information (including external sources such as social media and the dark web), and analyze correlations in real time to determine whether signs of cyberattacks constitute incidents.

## 2.5. Response and Recovery from Cyber Incidents

### 2.5.1. Formulation of Incident Response and Contingency Plans

*Fundamental response measures*

(1) Develop incident response plans and contingency plans (including recovery plans) for each type of cyberattack[38]. These plans should define response priorities, Recovery Time Objectives (RTO), and Recovery Level Objectives. Review these plans regularly or as needed.

*Recommended measures*

(a) In contingency planning, prepare for large-scale cyber incidents, such as those affecting financial settlement infrastructure, payment systems, or services, etc., provided by third parties (including data centers and cloud services) that may become unavailable for extended periods

[37] SIEM (Security Information and Event Management) refers to a system that centrally aggregates logs and data from sources such as firewalls, IDS/IPS, and proxies, and performs correlation analysis to monitor networks and detect incidents such as cyberattacks or malware infections.
[38] Examples of cyberattacks include DDoS attacks, website defacement, targeted attacks such as malware infections (where malicious programs are delivered via email or website browsing to compromise systems or data), ransomware, exploitation of vulnerabilities (attacks that steal information by exploiting weaknesses in systems or software), and attacks that result in unauthorized fund transfers.

### 2.5.2. Incident Response and Recovery

The following items should be taken into consideration when developing incident response and contingency plans[39].

#### 2.5.2.1. Initial Response (Detection, Reception, Triage)

*Fundamental response measures*

(1) Detect incidents through various means, including system monitoring as outlined in Section 2.4, inquiries from customers, etc., and notifications from external organizations such as cybersecurity response agencies.
(2) Based on the information collected at the time of detection or intake, verify the facts and determine whether incident response is necessary.
(3) Prioritize incidents according to their impact on business operations, etc., and report them to the incident response team manager, the person responsible for overseeing cybersecurity (e.g., CISO), and senior management, in accordance with predefined criteria.

#### 2.5.2.2. Analysis

*Fundamental response measures*

(1) For incidents determined to require a response, analyze the attack methods, causes and entry points, impact on systems, current business disruptions, and potential future impacts, etc. Prior to conducting analysis, preserve evidence such as logs, and perform the analysis using the preserved data.
(2) Maintain records throughout all phases from detection and intake to recovery, including details of the incident, actions taken during the response, and lists of logs collected during investigation, etc.

[39] (Reference) Also refer to Section IV "Considerations for Cyberattacks and Information Leaks" in the "Manual for the Development of Contingency Plans in Financial Institutions Guidelines for Developing Contingency Plans (Emergency Response Plans) for Financial Institutions," published by The Center for Financial Industry Information Systems Center (FISC).

### 2.5.2.3. Customer Response, Internal and External Coordination, Public Communication

*Fundamental response measures*

(1) Ensure that responsible personnel such as the CISO and other designated individuals, as well as stakeholders involved in contingency plans (including third-party representatives, etc.), are familiar with their roles, necessary contact points, and required response procedures[40] as defined in the incident response and contingency plans (including recovery plans).
(2) If an incident such as a data breach results in secondary damage or other impacts to customers, communicate the scope of the impact, precautions, and response measures, etc., to the affected customers.
(3) Report incidents promptly to regulatory authorities and other relevant bodies in accordance with applicable laws and regulations, etc.
(4) If public disclosure is required by law, etc., or deemed appropriate for preventing secondary damage or protecting customers, etc., disclose known facts—such as the nature of the cyberattack, response status, and recovery outlook—promptly and appropriately, while considering the security risks to customers and the organization, etc.
(5) Share relevant attack technique information, such as TTPs (Tactics, Techniques, and Procedures), with information-sharing organizations such as Financials ISAC Japan or JPCERT/CC, as needed, excluding confidential information.
(Reference) Cabinet Cybersecurity Center "Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks" (March 8, 2023))

### 2.5.2.4. Containment

*Fundamental response measures*

(1) To prevent the spread of damage caused by a cyberattack, consider the following points in advance when implementing containment measures:
- Clearly define the authority responsible for deciding whether to take actions such as disconnecting communications or shutting down systems. When making such decisions, prepare considerations such as the timing and duration of the shutdown, the scope of affected services, potential business impact, alternative operations, and communication

[40] This includes coordination and communication with participants and other related parties in the event of an incident involving financial market infrastructures.

routes.

(2) When containment is carried out and there is concern about recurrence or secondary damage due to information leakage, implement measures to prevent further incidents. Consider the following points:
- When disconnecting communications or shutting down systems, etc., determine—based on the incident situation and organizational policy—whether containment or evidence preservation should be prioritized.
- Engage external experts to assist with containment, if necessary.

(Reference) The Center for Financial Industry Information Systems "Manual for the Development of Contingency Plans in Financial Institutions" 4th Edition, January 2024, Section 2. (3) d Containment).

*Recommended measures*

(a) During containment, appropriately notify any third party who may be affected by the response.

### 2.5.2.5. Eradication

*Fundamental response measures*

(1) Eliminate the cause of the damage caused by the cyberattack (e.g., removing malware, applying patches, etc., to fix vulnerabilities).
- Evaluate and implement measures to enhance security, such as increasing network monitoring levels, installing firewalls and security appliances, and enforcing proper access controls.
- Engage external experts to assist with eradication, if necessary.

(Note) Refer to Section 2. (3)e Eradication in the "Manual for the Development of Contingency Plans in Financial Institutions" published by The Center for Financial Industry Information Systems.

### 2.5.2.6. Recovery

*Fundamental response measures*

(1) In recovery planning, it is essential to clearly define the authority responsible for deciding

when recovery is complete and operations can resume, as well as to organize the criteria for making that decision. Resuming operations without identifying and addressing the root cause of the incident may result in repeated attacks and further damage. Therefore, the decision criteria for resuming operations should include confirmation that appropriate measures have been taken to address the cause of the incident.

(2) During recovery operations, restore affected systems to normal operating conditions, including reinitializing compromised devices and rebuilding systems, and confirm that they are functioning correctly.

(3) When restoring from backups, consider the possibility that backup data, etc., may have been tampered with or infected with malware, etc., depending on the nature of the attack.
In the case of financial market infrastructures, if there are instructions from participants, etc., that were not successfully processed, etc., request the resubmission of those instructions.

(4) Before reconnecting the recovered system to other systems, confirm that the system is operating normally and that connections are functioning properly.

(5) During recovery, confirm—together with the system owner—that critical business operations have been properly restored and are functioning as expected.

(6) After recovery, analyze the root cause, etc., of the incident and any factors that contributed to the spread of damage. Evaluate the response and, based on the findings, revise and improve the incident response plan, contingency plan, and overall cybersecurity management framework.

## 2.6. Third-Party Risk Management

As financial institutions increasingly rely on third parties, their supply chains have expanded and become more complex, making risk management more challenging. In this context, there have been cases where cyber incidents originating from the supply chain had a significant impact on financial institutions. Given these circumstances, financial institutions must appropriately manage cybersecurity risks across their supply chains. In addition to this guideline, comprehensive guidelines for supervision, etc., provide general perspectives on outsourcing (including multi-tiered outsourcing) and key considerations for managing system risks related to outsourcing[41]. As noted in Section 2.6 (4), it is important to recognize that third-party risk management requires a risk-based approach.

Furthermore, third parties that provide services, etc., to financial institutions should offer necessary support to enable appropriate cybersecurity risk management. This includes ensuring

[41] Example: Comprehensive Guidelines for Supervision of Major Banks, etc., Section III-3-3-4.

that financial institutions can access relevant information about cybersecurity risks associated with those third parties. In relation to this, the FSA, under applicable laws[42], has the authority, etc., to issue reporting orders and conduct on-site inspections of outsourced entities when deemed necessary.
Comprehensive guidelines for supervision, etc., outline the methods and approaches for such oversight.

*Fundamental response measures*

(1) When formulating cybersecurity strategies and action plans, financial institutions should consider the entire supply chain. A cybersecurity management framework should be established that covers all business processes, including those involving third parties.
(2) Establish a framework to manage cybersecurity risks arising from third parties throughout the entire lifecycle of third-party relationships, and formulate a policy for third-party risk management.
(3) Develop an organizational structure for managing third-party risks, including the establishment of a central department for unified oversight, clarification of roles and responsibilities across relevant departments, and the development of internal regulations.
(4) Identify third parties and assess their risks based on their role, importance in business operations, handling of sensitive information (e.g., personal data, trade secrets), and system connectivity (e.g., ease of external access via the internet). Implement appropriate measures based on the level of risk.
(5) Maintain and organize a ledger or equivalent documentation to manage third parties. Example items to be managed include: the name of the third party, the products, services, and functions they provide, the level of access they have to the organization's systems, and the types, sensitivity, and location of the organization's data that they retain or process.
(6) In cyber incident response plans and contingency plans, establish a framework that includes third parties involved in incident response and related activities[43].
(7) Prior to initiating transactions with third parties, conduct due diligence based on predefined criteria. In the due diligence process, evaluate, for example, the following items. Note that due diligence may also include the use of external evaluations, such as third-party assurance reports or certifications:
    - Assessment of potential cybersecurity risks and vulnerabilities associated with the transaction with the third party
    - Evaluation of the extent to which the third party meets the cybersecurity requirements expected by the organization (e.g., those stipulated in contracts)

[42] For instance, Article 24, Paragraph 2 and Article 25, Paragraph 2 of the Banking Act.
[43] For further details, refer to Section 2.5

- Review of past incidents, including the occurrence of such incidents, the third party's response, recovery efforts, and measures taken to prevent recurrence, etc.

For particularly important third parties, evaluate their cybersecurity management framework, cyber incident response plans, and contingency plans.

(8) Clearly define the cybersecurity requirements that third parties must comply with, and depending on their importance, explicitly state items such as the following in contracts or service level agreements (SLAs), etc.:
- Roles and responsibilities between the organization and the third party
- Audit rights
- Procedures for subcontracting
- Required security measures
- Rules to be followed by the third party's officers and employees
- Response and reporting procedures in the event of an incident
- Implementation and reporting of vulnerability assessments, etc.
- Response and reporting procedures when serious vulnerabilities are identified
- Implementation of cybersecurity exercises and training (including participation in joint exercises)
- Agreements regarding data location, storage, retention, transfer, and disposal
- Conditions for contract termination and arrangements upon termination
- Implementation of external evaluations, etc. (including submission of third-party assurance reports and acquisition of third-party certifications)

(9) Continuously monitor the cybersecurity risks posed by third parties and their products/services, as well as the status, etc., of contract fulfillment, in accordance with the severity of the risks.

(10) Establish a management process for the termination of transactions with third parties, including measures such as data disposal and revocation of access to internal systems.

*Recommended measures*

(a) Assign personnel with appropriate knowledge, etc., and expertise to the department responsible for overseeing third-party risk management.

(b) In third-party risk management, give consideration to dependencies on third parties for critical operations, concentration risks associated with third parties, the impact of geopolitical risks, and the influence of fourth parties (i.e., subcontractors of third parties).

(c) Regularly monitor the ability of critical third parties to manage their own third parties (including two or more third parties, such as fourth, fifth, and Nth parties from the perspective of the organization), as well as risks related to their supply chains and concentration, etc.

(d) In preparation for the withdrawal from business, suspension of operations, or termination of contractual relationships involving critical third parties, formulate appropriate contingency plans and exit strategies in advance, and test, etc., alternative measures periodically.

(e) In accordance with the Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures, when a Specified Social Infrastructure Service Provider intends to outsource the introduction or critical maintenance, etc., of Specified Important Equipment, implement risk management measures as required in the notification. These measures aim to reduce the risk of such equipment being used as a means of specified acts of disruption.
(Reference) FSA website: "Economic Security Measures to be taken in the Financial Sector" (https://www.fsa.go.jp/news/r5/economicsecurity/231117infrastructure.html)

## 3. Strengthening Collaboration Between FSA and Related Organizations

### 3.1. Enhancing Information Sharing and Analysis

In order to promptly identify and share vulnerability information, and to encourage financial institutions to respond to vulnerabilities—thereby preventing damage from cyberattacks or minimizing their impact—the FSA maintains and strengthens its collaboration with the National Cybersecurity Office (NCO), which serves as the command center for cybersecurity, the Bank of Japan, the Financials ISAC Japan, The Center for Financial Industry Information Systems (FISC), and each CEPTOAR[44], etc. (Capability for Engineering of Protection, Technical Operation, Analysis and Response)

Furthermore, as the actors and objectives of cyberattacks diversify and it becomes increasingly difficult to grasp threat trends, the Agency promotes information-sharing with organizations such as the Public Security Intelligence Agency (PSIA) to further enhance its intelligence capabilities for information collection and analysis.

### 3.2. Collaboration with Investigative Authorities, etc.

While new financial services leveraging emerging technologies continue to be developed, in the realm of financial crime, there has been a growing trend of criminal activities that exploit these new services and technologies. In addition to traditional unauthorized money transfers via

[44] CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) refers to organizations responsible for information sharing and analysis functions among critical infrastructure operators and related entities.

internet banking, criminals are increasingly misusing anonymization technologies related to crypto-asset transactions, such as demanding ransom payments in crypto-assets through ransomware attacks. Furthermore, it has been pointed out that an ecosystem has been established in which malicious actors without advanced technical skills are systematically provided with tools such as malware and methods for unauthorized fund transfers, enabling them to illicitly generate profits. To reduce the incentives for criminal behavior and support the efforts of investigative authorities in deterring cyber attacks, the FSA closely monitors changes in criminal methods used in financial crimes, and works in cooperation with the police and industry associations, etc., to carry out activities aimed at preventing such crimes and minimizing the damage through awareness-raising and education.

### 3.3. Deepening International Cooperation

To appropriately address cross-border issues such as transnational threats, incidents with international impact, third-party and supply chain risks, AI and the potential compromise of cryptographic technologies due to quantum computing, the FSA actively participates in international discussions and collaborates with overseas authorities. In addition, the insights gained through such international collaboration are utilized in domestic monitoring activities and in coordination with industry stakeholders.

### 3.4. Public-Private Collaboration

Cybersecurity must be strengthened across the entire ecosystem, including users of financial services, financial institutions, authorities, and other relevant stakeholders. To this end, the FSA promotes sector-wide initiatives in collaboration with mutual aid organizations and financial institutions, while also working to enhance the capabilities of individual financial institutions and the industry as a whole through monitoring and other means.
In addition, the Agency further encourages private-sector efforts to foster mutual support and cooperation.

| | |
|---|---|
| October 4, 2024 | Issued |
| July 4, 2025 | Revised |