Research Report on "Strengthening the Management of Third-Party Cybersecurity Risks by Financial Institutions"
(Provisional Translation)

Deloitte Tohmatsu Cyber LLC

February 27, 2026

Table of Contents

I. Executive Summary

Relationships between financial institutions and third parties have become increasingly diverse, resulting in the growing complexity of risk management. Under such circumstances, incidents have occurred in which customer information and other data held by financial institutions are leaked due to cyberattacks targeting third parties. In light of the rising importance of third-party cyber risk management (hereinafter referred to as "TPCRM"), this research examines advanced management practices employed by financial institutions in the United States, the European Union, and the United Kingdom, where such initiatives are considered to be progressing, and discusses implications for TPCRM at Japanese financial institutions.

As a result of this research, it was found that major financial institutions in the US, EU, and UK have established cyber security risk related to third parties as one risk domain to be managed within the framework of third-party risk management (hereinafter referred to as "TPRM"). Specialized departments, such as cyber security departments, are incorporated as responsible units for these risk domains and are promoting corresponding measures. Based on this premise, the following responses were observed.

- Third parties are classified based on the importance of the services they provide to the financial institution and the inherent risk level associated with each third-party arrangement. Furthermore, third parties subject to management include all third parties, such as cloud service providers, in accordance with the relevant laws, regulations, and guidelines of each country. The management approach is determined based on risk, with varying degrees of control applied. Nth parties are also included in the scope of management; however, from the perspective of operational effectiveness, many financial institutions limit their visualization and management to fourth parties. Additionally, the mitigation of Nth party risks is ensured by evaluating the third party's ability to manage its own subcontractors.
- The criteria for determining critical third parties differ depending on the region. For financial institutions in the EU and UK, critical third parties are selected from the perspective of operational resilience to ensure regulatory compliance; specifically, those third parties whose failure would immediately affect the financial institution's business continuity and ability to provide services are designated as critical. In the US, financial institutions also consider operational resilience but tend to designate those

third parties that pose extremely high inherent risks as critical, depending on the business activities for which they are used and the purpose of those activities.

- With regard to concentration risk among third parties, financial institutions manage this from the perspective of operational resilience by assessing the extent of their dependence on third parties, whether the provision of third-party services is concentrated in specific regions, and whether critical third parties are relying on Nth parties for key operations. Third party-related data is effectively visualized and managed by using TPRM tools.
- For ongoing monitoring, as cyber threats continue to evolve and become more sophisticated year by year, financial institutions not only use cyber threat intelligence tools, such as risk scoring tools and dark web monitoring, to continuously assess the status of critical third parties, but there are also cases where all third parties are monitored. Additionally, some financial institutions improve operational efficiency by utilizing frameworks for sharing industry questionnaires.
- As initiatives to secure audit rights over third parties, all financial institutions include clauses regarding audit rights in their basic contracts with third parties. In addition, contractual provisions also stipulate the minimum security control requirements that third parties must comply with, as well as the authority to conduct onsite inspections.
- With regard to exit strategies and exit plans for third parties, these are formulated with priority given to critical third parties. The basic policy, such as whether to terminate the contract or switch to an alternative in the event that the services provided by the third party are discontinued or interrupted, is outlined in the exit strategy. The exit plan details procedures for transitioning to alternatives. Additionally, exit plans are regularly tested through tabletop testing and updated as necessary to maintain their effectiveness.
- In anticipation of cyber incidents occurring at third parties, financial institutions have established detailed procedures, such as reporting flows from the third party to the institution and within the organization, and, if there is a network connection with the third party, steps for network disconnection. They have also formulated response policies for cyber incidents. To ensure effectiveness in the event of an incident, a collaborative structure is in place in which the department responsible for contracts with third parties works together with the specialized cyber security incident response team.
- It was often observed that intermediaries (insurance agents, brokers) have traditionally been managed outside the framework of TPRM. On the other hand, there were some

cases where intermediaries (insurance agents, brokers) access policyholders' information for activities such as insurance renewals. In these cases, although the intermediaries (insurance agents, brokers) were managed under a different program from TPRM, insurance companies also evaluated and managed the security measures of them. There were also examples where the scope of TPRM was extended to intermediaries (insurance agents, brokers) by unifying the assessment of inherent risks, management standards, and the databases used for management between TPRM and intermediaries (insurance agents, brokers) management.

II. Introduction

1. Background and Purpose

As outsourcing destinations and other third parties[1] for financial institutions' IT systems diversify and become multilayered[2], the configuration and procurement relationships of devices and software that make up IT systems are also becoming more complex[3]. Amid such circumstances, incidents in which customer information of financial institutions is leaked[4] or at risk of being leaked due to cyberattacks on third parties of financial institutions have been occurring frequently, and strengthening TPCRM at financial institutions has become an urgent issue. Regarding TPRM/TPCRM, in Japan, for the 2023 administrative year, an investigation into management methods at major US financial institutions was conducted, and a report was published[5] with the aim of providing information useful for risk management at domestic financial institutions. In August 2024, key points regarding the "Consultative Document Principles for the sound management of third party risk"[6] published by the Basel Committee on Banking Supervision in July 2024 were summarized and published. Furthermore, in the "Guidelines on Cybersecurity for the Financial Sector" formulated in October 2024, perspectives on responses related to TPCRM are included. In recent cases, issues such as identifying critical third parties and services, concentration on specific third parties, and ensuring not only the availability but also the confidentiality of information have become apparent, and it is necessary to strengthen responses to these issues. TPRM/TPCRM is not a problem unique to Japan. For example, it is addressed in the "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector"[7] (formulated in October 2018, revised in October 2022), and in various foreign countries, comprehensive systems related to TPRM/TPCRM in the

---

[1] 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." Financial Service Agency, "Guidelines on Cybersecurity for the Financial Sector" (October 4, 2024).

[2] Software vendors build services on cloud vendors' platforms and provide cloud services as SaaS, etc.

[3] Software vendors incorporate open-source software (software whose source code is publicly available and which, in principle, may be modified and redistributed free of charge) and provide software as packages, etc.

[4] Such as when the external service provider to which the processing of the company's important information has been entrusted is subjected to a cyberattack, resulting in the leakage of the company's information, etc.

[5] Financial Service Agency, Research Report on "the Management of Third-Party Supply Chain Cybersecurity Risks by Financial Institutions" (December 20, 2023)

[6] The Basel Committee on Banking Supervision（BCBS）, "Principles for the sound management of third-party risk" (December 2025)

[7] G7 Cyber Expert Group, "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" (October, 2022)

financial sector are being newly introduced. Based on this situation, this research aims to grasp the actual conditions of such systems in foreign countries and examples of initiatives to comply with such systems, and to consider suggestions for improving risk management at domestic financial institutions.

2. Basic Approaches to TPCRM in Foreign Countries

In this research, based on issues of TPCRM expected at domestic financial institutions, we investigated topics such as classification of third parties, concentration risk, and audit rights of third parties, which will be described later. In order to understand the background and research results of these topics, it is useful to grasp the general framework of TPCRM. Therefore, as an overview, we will supplement here with information on TPCRM structures, processes, tools, and services.

- ✧ TPCRM Structure
  - ➢ Under the TPRM/TPCRM frameworks, the contract management department and other relevant business units act as the first line, conduct the TPRM program, and bear ultimate responsibility. The cybersecurity department is responsible for assessing third-party cybersecurity risks, while the procurement department or risk management department as a second line oversee the TPRM/TPCRM program. These departments collaborate to execute TPRM/TPCRM. In addition, committee organizations and meeting bodies in which both divisions participate are established, and reporting to management is conducted. The basic approach to the division of roles in TPCRM in foreign countries is organized in the table below.

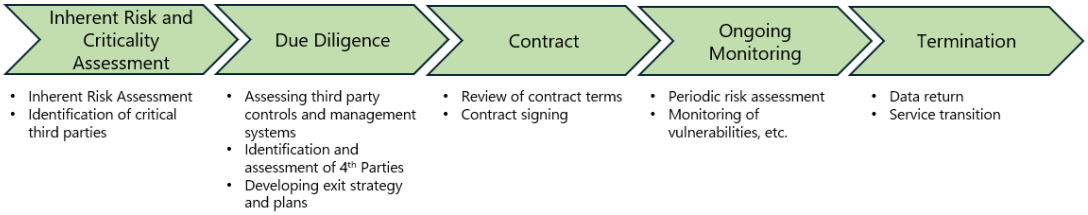
Table I-1. Basic Division of Roles in TPCRM

Examples of Responsible Departments	Examples of Responsibilities
Risk Management Departments/ Procurement Department as a TPRM Section	・ Establishes and reviews the TPRM framework in accordance with the organization's risk appetite, strategy, procedures, etc., and promotes its operations ・ Develops and promotes the implementation of TPRM rules not limited to cybersecurity

	・ Compiles and reports to management on the status of TPRM operations (number of third parties, changes in the number of risk assessments conducted, trends, monitoring, etc.)
Specialized Departments for Each Risk (Risk Experts)	・ Specialized departments for each risk in TPRM (such as the compliance department, procurement department, cybersecurity department, etc.) participate as experts and are involved in the design of risk assessment items for third parties and in the review of risk assessment results conducted by the operational departments ・ In the execution of TPCRM, there are cases where personnel from the cybersecurity department are assigned to conduct evaluations of third parties from a cybersecurity perspective, including onsite investigations, remote investigations, and risk assessments
Operational Departments	・ The operational departments that utilize third parties conduct actual third-party risk assessments, formulate response policies based on the results, and make decisions regarding risk acceptance ・ Any department within the financial institution that enters into contracts and utilizes third parties may fall under this category

✧ Basic Processes of TPCRM

➢ Various laws, regulations, and guidelines require risk management throughout the entire lifecycle of relationships with third parties in TPCRM, including processes such as risk assessment at the time of selection, contracting, ongoing monitoring during the contract period, and termination of third-party use. Many overseas financial institutions also implement this process. The overall image of the lifecycle is summarized in the diagram below.



➢ In the initial stage, financial institutions evaluate the inherent risks of the

transactions and whether the services provided by the third party support the provision of important functions, taking into consideration the details of the services used by the third party. Based on the results of the inherent risk and importance assessments, the areas where controls over third parties are necessary and the depth of control evaluation are determined, and the prioritization for post-contract monitoring, as well as its depth and frequency, are decided. The results of the inherent risk and importance assessments are important as the starting point for risk-based management.

- ✧ Tools and External Services Used in TPCRM
  - ➢ In TPCRM, tools and services are used to centrally manage ledgers of relationships, contracts, and risk information with third parties, and to execute risk management workflows effectively and efficiently throughout the entire lifecycle of third parties. For example, due to the large number of third parties and related management information, as well as the wide variety of stakeholders involved in business processes, managing all of this with Excel has its limitations, and many companies use tools and services. In addition, tools and services tend to be used to obtain near real-time risk information, such as third-party ongoing monitoring. Examples of tools and external services used in TPCRM are summarized in the table below.

Table I-2. Examples of Tools and Services

Type of Tool/Service	Overview
TPRM Tool	● Provides mechanisms for efficient storage and updating of key data related to relationships and risks with third parties, including ledger management and workflow functions ● Includes features for sending, collecting, and aggregating questionnaires to third parties ● May be offered as a function within Governance, Risk, and Compliance (GRC)[8] tools

[8] Frameworks or processes for companies and organizations to efficiently and centrally manage adherence to management policies and rules, risk management, and compliance with laws and regulations, and to strengthen controls.

Intelligence	● External data is used to identify risks that cannot be detected solely from third-party responses ● There are research firms that provide highly specialized information on third parties, focusing on areas such as cybersecurity, corporate investigations, and sustainability ● Some services provide the scanned results of negative news about third parties found on the internet
Risk Scoring Tool	● Tools and services that regularly assess the cybersecurity status of companies and organizations from the outside, visualizing the results as scores or rankings ● This is a form of intelligence utilization mentioned above

3. Hypothesis on Challenges of TPCRM in Japanese Financial Institutions

Japanese financial institutions have implemented outsourcing management programs based on regulations such as the Banking Act, Financial Services Agency's Supervisory Guidelines, and Act on the Protection of Personal Information. However, with regard to broader TPCRM initiatives, including entities beyond outsourcing, as promoted in some foreign countries, it was observed that many institutions are considering reviewing their current frameworks, including compliance with the "Guidelines for Cybersecurity in the Financial Sector"[9] issued by the Financial Services Agency. Accordingly, the current challenges faced by financial institutions were organized as the following hypotheses, and this research was conducted.

1. Classification of Third Parties

Financial institutions where specific methods for classifying third parties under TPCRM have not yet been established are facing difficulties in determining the scope of third parties and Nth parties to be managed. In addition, with respect to "critical third parties," as referenced in the Financial Services Agency's "Guidelines for Cybersecurity in the Financial Sector"[10], it was noted that there is no clear definition or criteria for identification, and that management methods for critical third parties have not been clearly established, which may pose challenges for risk management. Furthermore, direct management of Nth parties is difficult due to the

[9] Financial Service Agency, "Guidelines on Cybersecurity for the Financial Sector" (October 4, 2024), p.32, "2.6 Third-Party Risk Management," which indicates that financial institutions and similar entities, in light of recent trends in the occurrence of cyber incidents attributable to third parties, should appropriately manage cybersecurity risks in the supply chain.

[10] Financial Service Agency, "Guidelines on Cybersecurity for the Financial Sector" (October 4, 2024), p.17

absence of direct contractual relationships between financial institutions and Nth parties, and that institutions are also struggling to determine the scope (e.g., cloud service providers, IT vendors, and areas outside of system outsourcing) and methods for managing Nth parties utilized by third parties.

2. The Risk of Concentration of the Provision of Important Services or Functions in Specific Third Parties (hereinafter referred to as "concentration risk")

There are opinions that visualization and management of concentration risk in specific third parties or Nth parties are not being sufficiently conducted, and that the assessment of concentration risk regarding cloud service providers and similar entities, as well as the positioning of exit strategies and exit plans for business continuity according to their risk, are also unclear. In addition, it has been recognized that methods for conducting joint training for business continuity with third parties are also unclear. In light of these circumstances, there may be challenges in fleshing out concentration risk management and enhancing response policies.

3. Ongoing Monitoring after Contracting with Third Parties (hereinafter referred to as “ongoing monitoring”)

As cyberattacks are changing and becoming more sophisticated year by year, timely risk monitoring and continuous response to threats have become necessary. Therefore, it is considered important not only to evaluate third parties at the time of their selection, but also to continuously assess the status of their contract fulfillment and responses to threats. On the other hand, although a certain level of expertise is required for cybersecurity risk assessment, onsite personnel responsible for contracts with third parties often lack specialized knowledge, and there are also resource constraints within cybersecurity departments. As a result, there may be challenges regarding the methods for conducting ongoing monitoring and standardizing the quality of risk assessments.

4. Securing Audit Rights over Third Parties and Methods for Doing So

There are concerns that the minimum necessary security measures may be insufficient because cybersecurity-related contract clauses are not included in contracts and other documents. In addition, due to a lack of knowledge among those in charge of TPCRM and insufficient cooperation from cloud service providers and others regarding risk assessment, there are cases where third-party risk management may be inadequate. For effective management, it is expected that examples from foreign institutions will provide references on

how audit rights are secured through contracts or other means. Furthermore, the selection, specific usage, and effectiveness of complementary management methods not limited to contracts, such as intelligence functions utilizing external information sources or the use of AI, are also considered future issues to be examined.

III. Research Methods

1. Scope and Approach

The main research items regarding TPCRM at financial institutions in the US, EU, and UK were: (1) classification of third parties and management policies, (2) concentration risk, (3) ongoing monitoring, and (4) securing audit rights and methods for third parties. First, relevant elements were organized based on laws, regulations and guidance related to TPCRM in the financial sector.

Next, several major financial institutions in the US, EU, and UK were asked to respond to a questionnaire and participate in interviews regarding the frameworks they have implemented and their actual approaches. In addition to the items above, the research also included (5) exit strategy and exit planning, and (6) incident response as main research items. Supplementary research was also conducted on "cyber threat intelligence," "use of AI in TPRM," "frameworks for sharing questionnaires within the industry," and "contractual clauses related to cybersecurity." Furthermore, (7) additional research was conducted on third parties specific to the insurance industry, such as intermediaries (insurance agents, brokers), as well as third parties linked to insurance products and services.

The research period was from June 17, 2025, to February 28, 2026.

2. Disclaimer

This research was conducted for the purpose of extracting advanced initiatives at major financial institutions in the US, EU, and UK, and obtaining insights for Japanese financial institutions. The research targets were primarily organizations with global operations and employee numbers ranging from tens of thousands to several hundred thousand. While this report refers to practical operations at these financial institutions, especially regarding organizational structure and human resources, please note that these are based on the assumption of such scale and may not necessarily be applicable to financial institutions of all types and sizes.

This report presents the results of research conducted based on the business outsourcing agreement concluded between the Financial Services Agency and our company dated June 17, 2025, and was not performed as an assurance engagement. The acceptance and usage of its contents shall be determined at the discretion and responsibility of the readers of this report.

The information contained in this research report is current as of the time of the research and, except for publicly available information, is based on information provided by the interviewed institutions. The validity or accuracy of the information obtained are not the responsibility of our company.

IV. Regulatory Supervision Trends by Authorities

1. Document Review Results

To extract research items regarding management methods at major financial institutions in the US, EU and UK, we conducted a review of the scope and content of management required or recommended in existing laws, regulations, and guidelines. Here, we present an overview of the results of our research on laws, regulations, and guidelines related to TPCRM issued by authorities and international organizations in each country and jurisdiction.

- Overview of Research Results
  - The laws, regulations, and guidelines do not limit their scope to traditional outsourcing contracts but also include third parties that have broader business agreements and arrangements that are not considered outsourcing in nature[11]. For financial institutions to manage risks related to third parties, these documents describe the fundamental concepts necessary for engaging in TPCRM, such as the approach to evaluating which third parties should be managed and their level of importance, as well as monitoring of contracts and arrangements with third parties. All laws, regulations, and guidelines require financial institutions to assess and manage risks inherent to third parties, as the risks arising from relationships with third parties differ for each financial institution. To supplement the fundamental concepts for implementing TPCRM, these documents provide reference information such as examples of third-party management methods and items, thereby encouraging financial institutions to adopt TPCRM measures. Additionally, in the US, guidelines have been issued primarily for small and medium-sized banks (community banks)[12], providing examples of considerations and reference sources for those implementing TPCRM for the first time.
  - We have organized useful information found in the laws, regulations, and guidelines and illustrated this information below under the categories of "Classification of Third Parties," "Concentration Risk," "Ongoing Monitoring," and "Securing Audit Rights over Third Parties and Methods for Doing So."

[11] For example, the EBA published the "Guidelines on outsourcing arrangements" in 2019, and in July 2025 published the consultation paper "CP on Draft Guidelines on sound management of third-party risk," which extends the scope of management to third parties.

[12] November 27, 2025, Office of the Comptroller of the Currency (OCC) carried out a solicitation of comments for community banks regarding challenges and barriers in third-party risk management for community banks.

- Classification of Third Parties and Management Policies
  - ✧ Entities/firms and individuals that provide services to financial institutions are defined as service providers, and are classified and defined as follows:
    - ✓ Third Parties / Nth Parties:
      Refers to service providers that have direct transactions with financial institutions or indirect service providers
    - ✓ Critical/Material Third Parties:
      Refers to service providers whose suspension of services would have a significant impact on the operations of financial institutions
    - ✓ Intra-group Service Providers:
      Indicates whether the third party is an affiliate within the same group as the financial institution
    - ✓ The distinctive points in each document are as follows:
      - In the US documents, all business arrangements are subject to regulation regardless of whether a contract exists between the financial institution and other entities. It is noted that relationships with third parties may exist even without contracts or compensation. Examples of these business arrangements include:
        outsourcing services, use of freelance consultants, referral agreements, merchant payment processing services, services provided by affiliates or subsidiaries, and joint ventures.
      - In the UK documents, including service providers that do not qualify as outsourcing under the definition are classified as non-outsourcing, the financial institutions are expected assess the materiality and risk of all third party arrangements, and should implement proportionate, risk-based, suitable controls. Examples of such arrangements include:
        purchase of ICT products such as hardware and software, design and construction of on-premises IT products, purchase of data collected by service providers, pre-developed machine learning models by service providers, etc.

  - ✧ All laws, regulations, and guidelines indicate that third parties subject to management should not be limited to the scope of outsourcing contracts. It is necessary to identify, assess, and appropriately manage the risks associated with arrangements with third parties.
    - For example, the Basel Committee on Banking Supervision (BCBS) guidelines

state that financial service transactions conducted between a bank and its customers, employees, or counterparties (e.g., accepting deposits from consumers, lending to consumers, providing insurance to policyholders, providing or receiving services related to financial market infrastructure (FMI) such as clearing and settlement to/from other banks) are not included in the definition of third-party arrangements. However, arrangements made with third parties to support these operations (e.g., outsourcing of back-office operations that support the above-mentioned activities) are indicated as subject to management.

- ✧ All laws, regulations, and guidelines define third parties that support high-risk activities or critical operations of financial institutions as critical third parties. The criteria for determining critical third parties are described as follows:
  - ✓ Soundness of the third party's financial condition
  - ✓ Tolerance for interruption of services, etc.
  - ✓ Nature of data and information shared with the third party
  - ✓ Availability of alternative services

    and others
    - In addition, laws, regulations, and guidelines in the EU and UK provide examples of evaluation items for determining whether an activity is critical, such as whether the third party is directly involved in the provision of regulated activities like banking, investment, or payment services.

- Concentration Risk
  - ✧ All laws, regulations, and guidelines indicate the management of concentration risk from the perspective of operational resilience. For example, the Basel Committee on Banking Supervision (BCBS), as well as laws and guidelines in the EU and UK, define concentration risk as the risk arising from a financial institution's dependence on services provided by a single or limited number of third parties, where disruption or failure of those services may potentially impact the institution's critical operations. Examples of concentration include concentration of multiple services with a single third party, concentration in the geographic regions where third parties provide services, and cases where multiple third parties rely on the same subcontractor for service provision. Identification, assessment, and management of such concentration risks are required.

- ✓ On the other hand, the Financial Stability Board (FSB) notes that dependence on a single third party can have benefits, such as enhancing internal expertise within the financial institution, creating synergies when developing business models, and improving efficiency in risk management. Such characteristics are also indicated as strengthening the resilience of financial institutions and increasing operational efficiency and flexibility.
- ✓ The distinctive points in each document are as follows:
  - In the EU and UK documents, similar to the BCBS, identification, assessment, and management of service concentration, geographic concentration, and Nth-party concentration risk are required. It is also stated that authorities should evaluate concentration risk in the financial sector through a risk-based approach, and if concentration risk is identified, its trends should be monitored and the potential impact on other financial institutions, payment institutions, and the stability of financial markets should be assessed.
  - In the US documents, although concentration risk is not explicitly defined, it is common to require confirmation of dependence on specific third parties for operations and situations where multiple activities rely on a particular subcontractor. Additionally, reporting the status of dependence on third parties to the board of directors is required[13].

■ Ongoing Monitoring

- ✧ All laws, regulations, and guidelines require the establishment of processes for ongoing monitoring.
  - ✓ Continuous evaluation and monitoring of the performance and risks related to the provision of services in accordance with arrangements such as contracts with third parties, regular reporting to the board of directors and management, and the establishment of processes for reporting and responding to senior management when significant issues are identified, or incidents occur
  - ✓ More comprehensive and frequent monitoring for arrangements with critical third parties
  - ✓ The distinctive points in each document are as follows:
    - The EU and UK documents require maintaining expertise in risks related to

[13] Although it is not included this survey, the U.S. Department of Treasury, in "The Financial Services Sector's Adoption of Cloud Services" issued on February 8, 2023, mentions the potential impacts of market concentration in the provision of cloud services

third parties in order to continuously manage third-party operations.

- For the US, guidance for small and medium-sized banks (community banks) indicates that banks can conduct ongoing monitoring efficiently by utilizing external resources and by referencing suitability assessments and certifications.
- The EU documents require ongoing risk-based monitoring for all arrangements with third parties.

✧ Specific examples to be implemented as ongoing monitoring are as follows:

✓ Confirmation of third-party performance (such as the status of third-party operations and fulfillment of SLAs), as well as the occurrence of significant issues or concerns:

E.g., Monitoring of indicators showing the manifestation of risks, such as serious or repeated findings, deterioration of financial condition, data loss or leakage, service interruptions, incidents, compliance violations, concentration, and other risks

✓ Periodic visits and meetings with third-party representatives to discuss performance and operational challenges

✓ Confirmation that the availability, integrity, and confidentiality of data and information are ensured

✓ The distinctive points in each document are as follows:

- In the EU and UK documents, if the risk, nature, or scale of outsourced functions changes significantly, it is required to re-evaluate the importance of those functions and to establish a framework that allows for contract termination, when necessary, without compromising service continuity or quality.

■ Securing Audit Rights over Third Parties and Methods for Doing So

✧ All laws, regulations, and guidelines require that the audit rights of financial institutions be stipulated in contracts.

✓ Rights and obligations between the financial institution and the third party

✓ The financial institution’s right to audit the third party and access information, etc.

✓ Obligation to cooperate with authorities and the right of authorities to access information, etc., at the third party

- ✓ Obligation to retain and disclose timely, accurate, and comprehensive information to the financial institution and authorities

✧ Specific examples to be included as contract provisions are as follows:

- ✓ Audit rights and rights to obtain information from third parties, rights to access the service provider's relevant facilities (such as headquarters and operation centers), equipment used for service provision (systems, networks, and data), and performance benchmarks or KPIs for services
- ✓ The right of financial institutions to receive accurate information on critical services in a timely manner
  E.g., information on incidents, service content, and significant changes
- ✓ Provisions related to operational resilience
  E.g., business continuity, emergency response plans, maximum allowable downtime, Recovery Time Objective (RTO), and Recovery Point Objective (RPO)
- ✓ Obligation to notify the financial institution in the event of compliance violations, law enforcement actions, regulatory procedures, or incidents that pose significant risks to the financial institution or its customers
- ✓ Obligation to notify regarding mergers, acquisitions, business transfers, major changes in personnel, and other significant changes that may affect the activities involved
- ✓ Types and frequency of reports to be received from third parties
  E.g., business reports, financial reports, security reports, control assessment results, etc.
- ✓ Right to ongoing monitoring
- ✓ Conditions stipulating the use of subcontractors
- ✓ The right for authorities to obtain the above-mentioned rights and to share information with authorities in a timely manner
- ✓ In addition, the laws, regulations, and guidelines in the EU and UK specify the following:
  - Requirements such as specifying the location (region or country) where functions provided by third parties (e.g., data processing or storage) are performed, notification obligations if there are planned changes in the service delivery location, ensuring the availability, authenticity, integrity, and confidentiality of data including personal data, and the obligation for third parties to fully cooperate with the competent authorities as designated.

- Even if the functions provided by the third party are not critical functions, it is required that the possibility of these functions becoming critical over time be considered. Through a risk-based approach, it is recommended to consider the nature of the functions, related operational risks, reputational risk, potential impact on business continuity, contract term, etc., and to consider including the above-mentioned access and audit rights in the contract.

✧ Supervisory authorities are expected to conduct reviews of financial institutions' third-party risk management status.

✓ In the EU and US, examples of review activities include the following:

- Evaluation of the ability of the financial institution's management to oversee relationships with third parties
- Assessment of the impact that relationships with third parties have on the financial institution's risk profile and key aspects of financial and business operations (including compliance with applicable laws and regulations)
- Conducting transaction tests on activities performed by third parties, or reviewing test results, and assessing compliance status with relevant laws and regulations
- Consultation with management or the board of directors regarding significant risks or deficiencies in the financial institution's risk management processes as necessary, and evaluation of identified issues
- Evaluation of whether the financial institution has developed appropriate and sustainable corrective measures for deficiencies related to audits of third parties involved in particularly critical activities
- Assessment of whether the financial institution has identified and managed all relevant risks
- Assessment of whether the financial institution has identified, evaluated, and appropriately managed conflicts of interest related to outsourcing arrangements

✓ If concerns are identified that a financial institution does not have a robust governance framework or is not in compliance with regulatory requirements, the competent authority should take appropriate measures, which may include restricting or reducing the scope of outsourced functions or requiring the termination of outsourcing arrangements.

■ Other

✧ In the EU and UK, documents regarding the designation of critical third parties by authorities have been published[14].

✓ The purpose of these documents is to manage the risks that disruptions or outages in services provided by critical third parties to financial institutions may pose to the stability and reliability of the financial system. They describe the supervisory framework and obligations of designated critical third parties.

✓ Both the EU and UK documents also cover the management of concentration risk as well as ongoing monitoring.

2. List of Summaries of Referenced Laws, Regulations, and Guidelines

■ The overview of the laws, regulations, and guidelines in scope of this research is as follows. For detailed summaries of each law and guideline, please refer to the Appendix.

Table III-1. Laws, Regulations and Guidelines on TPCRM Covered in the Research

Issuer (Effective date)	Jurisdiction	Document Title	Summary
Basel Committee on Banking Supervision (December 10, 2025)	International Organization	Principles for the sound management of third-party risk	・ This document sets forth principles for the sound management of third-party risk in the banking industry, intended for banks and supervisory authorities. ・ Specifically, Principles 1 to 9 provide guidance on effective third-party service provider risk management for banks, while Principles 10 to 12 present guidance for supervisory authorities.

[14] EU Digital Operational Resilience Act (DORA) and UK SS6/27 Operational resilience: Critical third parties to the UK financial sector. In the UK, at this stage of the survey, the designation of important third parties is underway.

			The document is structured to include both the principles and detailed commentary on each principle.
Financial Stability Board (December 4, 2024)	International Organization	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities	・ This is a toolkit for third-party risk management and supervision intended for financial authorities, financial institutions, and service providers. ・ Specifically, Chapter 1 defines common terminology, Chapter 2 outlines the basic concepts of the toolkit, Chapter 3 provides tools for identifying critical services and managing risks throughout the entire lifecycle, and Chapter 4 addresses financial authorities' oversight of financial institutions' third-party risk management.
Financial Conduct Authority (Final revision: January 1, 2021)	United Kingdom	FCA Handbook - SYSC 8 Outsourcing	・ This is one of the sections comprising "SYSC" in the FCA Handbook, which summarizes the laws and other provisions of the Financial Conduct Authority. This section stipulates how financial institutions (such as banks, securities firms, and

			investment firms) should design and operate their outsourcing arrangements and systems. Within this section, there are rules imposing obligations, as well as guidance providing examples and recommendations, and the legal effect differs depending on the item.
Bank of England Prudential Regulation Authority (November 15, 2024)	United Kingdom	Supervisory Statement | SS2/21 Outsourcing and third party risk management	• This document sets out the expectations of the Prudential Regulation Authority regarding how financial institutions should comply with regulatory requirements and expectations related to outsourcing and third-party risk management. • Specifically, Chapter 1 provides an introduction and overview; Chapter 2 defines outsourcing; Chapter 3 discusses the application of the proportionality principle; Chapter 4 covers governance and record-keeping; Chapter 5 addresses pre-outsourcing requirements; Chapter 6 specifies the minimum requirements for written

			agreements for material outsourcing; and Chapters 7 to 10 detail data security, access/audit/information rights, sub-outsourcing, business continuity, and exit planning.
Bank of England Prudential Regulation Authority Financial Conduct Authority (November 12, 2024)	United Kingdom	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector	• This document sets out the expectations of the regulators regarding how critical third parties (CTPs) should comply with the obligations and responsibilities (collectively referred to as "CTP duties") imposed by the Financial Services and Markets Act 2000 (FSMA, as amended) and the rules of the regulatory authorities. • Specifically, Section 1 provides an introduction and overview; Section 2 defines terminology; Section 3 addresses the potential impact of CTPs on the financial system; and Section 4 outlines the CTP supervisory framework. Sections 5 to 11 describe how CTPs should comply with their obligations and responsibilities, and

			Section 12 explains transitional arrangements.
European Banking Authority (February 25, 2019)	EU	Final Report on EBA Guidelines on outsourcing arrangements	• This document is an updated version of the "GUIDELINES ON OUTSOURCING" issued by the Committee of European Banking Supervisors (CEBS) in 2006. It sets out governance frameworks and related management expectations and processes concerning outsourcing arrangements for all financial institutions within the EBA's remit, including credit institutions and investment firms subject to the Capital Requirements Directive (CRD), as well as payment institutions and electronic money institutions. • Specifically, after presenting the executive summary and background, the document explains, as outsourcing guidelines, the assessment of outsourcing arrangements, governance frameworks, and specific requirements along the outsourcing process.

European Banking Authority (July 8, 2025)	EU	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk	• This document has been developed as an updated version of the previous EBA "Guidelines on outsourcing arrangement." Unlike the previous version, which mainly focused on outsourcing arrangements, this document covers a broader scope, including outsourcing, regarding agreements with third parties. It sets out the risk management methods, standards, and roles that financial institutions and competent authorities should implement for these arrangements. • Although the details differ, the overall structure remains largely the same as the previous version.
European Parliament European Council (December 14, 2022)	EU	Digital Operational Resilience Act (DORA)	• This regulation was introduced with the aim of strengthening the digital resilience of financial institutions by integrating requirements related to ICT risk, which had previously been addressed individually by various EU laws. • It applies from January 17, 2025, and aims to enable

			financial institutions such as banks, insurance companies, and investment firms to respond to and recover from ICT (Information and Communication Technology) disruptions, such as cyberattacks and system failures. Unlike previous regulations, which did not sufficiently stipulate qualitative rules for defense, detection, containment, recovery, and remediation capabilities against ICT incidents, as well as incident reporting and digital testing capabilities, this regulation clearly defines rules regarding ICT risk management capabilities, incident reporting, operational resilience testing, and monitoring of ICT third-party risks. • Based on this regulation, a list of critical ICT third parties was published on November 18, 2025.
FRB、FDIC、OCC (June 9, 2023)	United States	Interagency Guidance on Third-Party Relationships: Risk Management	• This guidance is intended for banking organizations regarding risk management in

			relationships with third parties. ・ Specifically, after outlining the purpose and scope, it presents the fundamental principles and considerations for implementing risk management, followed by required activities and considerations for each stage of the lifecycle, organizational oversight and responsibilities, and the supervisory framework of the authorities.
FRB, FDIC, OCC (May 3, 2024)	United States	Third-Party Risk Management A Guide for Community Banks	・ This guidance was developed for community banks based on the "Interagency Guidance on Third-Party Relationships: Risk Management." ・ Although the details differ—such as the lack of reference to the supervisory framework of the authorities—the overall structure is largely the same as "Interagency Guidance on Third-Party Relationships: Risk Management," and relevant content from the Interagency Guidance is excerpted and included.

European Parliament, European Council (from November 25, 2009)	EU	Solvency ii Directive	• This is a prudential regulation for insurance and reinsurance companies in the EU, established by the European Parliament and the European Council. The regulation aims to ensure that policyholders and beneficiaries are adequately protected and sets out various requirements applicable to insurance and reinsurance companies within the EU. • The regulation adopts a risk-based approach, enabling the assessment of the "overall solvency" of insurance and reinsurance companies through both quantitative and qualitative methods.
IAIS (July 1, 2025)	International Organization	Draft Application Paper on operational resilience objectives and toolkit	• This document provides guidance on the objectives of operational resilience for insurance companies and the practices and toolkits that support these objectives. • This document provides guidance on the objectives of operational resilience for insurance companies and the practices and toolkits that support these

			objectives.
NAIC (Q4 2017)	United States	NAIC Insurance Data Security Model Law	・ This is a model law at the state level regarding the establishment of information security programs and related matters for insurance companies and others licensed by state insurance departments in the United States. ・ This is a model law at the state level regarding the establishment of information security programs and related matters for insurance companies and others licensed by state insurance departments in the United States. ・
NYDFS (October 21, 2025)	United States	Industry Letter：Guidance on Managing Risks Related to Third-Party Service Providers	・ This guidance is addressed to financial institutions such as banks and insurance companies under the supervision of the New York State Department of Financial Services. It does not impose new regulatory requirements, but aims to promote compliance with Section 500.11 of the Cybersecurity Regulation

			(23 NYCRR Part 500) by exemplifying best practices for appropriately managing cyber risks associated with the use of third-party service providers. ・ Specifically, it is structured to indicate the required management items and considerations for each stage of the third-party risk management lifecycle.

V. Practices Among Overseas Financial Institutions

Findings and Insights from Interviews with Major Overseas Financial Institutions

This section presents the results of the research conducted on financial institutions in the US, EU, and UK. A summary of the research findings and insights obtained from there is provided below.

As a premise, as described in the previous section, TPRM-related laws, regulations, and guidelines in each region are fundamentally principle-based. These documents only present perspectives and points that financial institutions should consider when designing their own TPRM frameworks, along with reference examples. This approach is based on the expectation and policy of the authorities in each country that the ultimate responsibility for managing third-party risks via the TPRM framework lies with the financial institution and that the design of each framework should be aligned with each institution's risk appetite. Various laws, regulations and guidance referenced by overseas financial institutions do not provide rule-based information that institutions can directly adopt, such as specific instructions or frequency criteria regarding who should conduct the periodic risk reassessments in third-party ongoing monitoring, what should be reviewed, and which items should be used for risk evaluation during periodic risk reassessments. As a result, differences in scope and management methods, as well as unique initiatives were observed in the TPRM frameworks implemented by financial institutions in each country.

Third-party cybersecurity risk is established as one risk domain[15] to be managed within the TPRM framework. In terms of the management structure, all overseas financial institutions interviewed established an organization dedicated to overseeing the TPRM framework as a whole, and within that organization, specialized departments such as cybersecurity were incorporated as risk domain experts. The cybersecurity department does not oversee or manage the TPRM framework itself. Overseas financial institutions have long established frameworks for third party management, and while these frameworks and their operations have become increasingly sophisticated, cyber incidents originating from third parties still occur

[15] In addition to cybersecurity risks, the risk domains managed under the TPRM framework included compliance, ESG, operational resilience, data privacy, Nth-party risk management, and other elements.

abroad. As a result, it was noted that overseas financial institutions have a very high level of risk awareness regarding third party cyber risk management.

(1) Classification of Third Parties and Management Policies

■ Method of Third Party Classification

Financial institutions in the US, EU, and UK subjected to this research classify third parties along multiple axes according to their intended use. Broadly, these classifications can be divided into those for clarifying the scope and criticality of third parties to subject to management under TPRM, those for differentiating risk levels determined based on risk assessment results, and those for reporting purposes aimed at improving the efficiency of ongoing management.

Table IV-1. Purpose, Classification Axes, Uses, and Examples of Third-Party Classifications

Purpose	Classification axis	Use of TP classification (examples)	TP classification (examples)
Scoping	Contractual relationship with the institution	● Used to determine whether there is a direct relationship or if the third party is an indirect service provider	● Third party ● Nth party
Scoping	Intra-group or external transaction	● Used to determine whether the third party is an affiliate of the institute ● Used to determine the required due diligence and other such responses	● Intra-group third party ● External third party
Scoping	Subjected or not subjected to TPRM	● Used to determine whether the third party should be subjected to the institution's TPRM	● Third party subjected to TPRM ● Third party not subjected to TPRM
Scoping	Criticality of the third party	● Used to determine the impact on the institution if the third-party's service is suspended	● Critical third party ● Other non-critical third party
Risk assessment	Risk classification (inherent/residual risk)	● Used to evaluate third-party risk, determine need for subsequent procedures, and consider countermeasures	● High, medium, low, or no risk

Management/ reporting	Categories in expense/purchasing systems (common third-party categories)	● Information from purchasing systems and TPRM tools are integrated to conduct expenditure management and analysis by category ● Used as a unit for concentration risk evaluation (e.g., total number of transactions/expenditures for specific categories)	● Supplier: Florist, office supply vendor, hardware/IT component supplier, software provider, etc.
Management/ reporting	Type of service provided by third party	● Used to categorize services provided by third parties ● Used as a basis for adjusting TPRM risk evaluation procedures (e.g., making omissions or additions) ● Used as a basis for aggregating outsourced operations in TPRM tools	● Technology: Cloud services, data centers, application developers, software developers, network providers, etc. ● Non-technology: Call centers, BPO such as payment management operations, information provision services, consulting, etc. ● Others: Government bodies (e.g., regulatory authorities), FMIs such as clearing houses, card networks, agent banks, brokers, etc.

■ Third Parties Excluded from the TPRM Framework

Differences were observed between the EU/UK and the US financial institutions regarding third parties excluded from TPRM management. For example:

✧ In the EU and UK, it was noted that FMIs such as exchanges and clearing houses under regulatory supervision are often explicitly excluded from the TPRM framework by many financial institutions interviewed. This exclusion was because FMIs are under regulatory oversight and their risks are considered to be mitigated to some extent.

✧ On the other hand, it was observed that interviewed US financial institutions included FMIs such as clearing houses, card networks, and agent banks under regulatory supervision within the scope of TPRM.

Furthermore, it was observed across all financial institutions interviewed that the categories of third parties excluded from the scope of TPRM are determined based on the institution's risk assessment results, risk tolerance, and the degree of control that can be exercised over the third party. It was confirmed that third parties that can be pre-identified as low risk, such as office supplies providers or florists, whose inherent transaction risk is low and who are managed under other processes such as procurement, are defined as a whitelist and excluded from the scope of TPRM.

➢ Critical Third Party

■ Regulatory Stance

In the EU and UK, critical third parties are presented from both the perspective of systemic risk affecting the entire financial sector (macroprudence) and the perspective of risk management at the individual financial institution level (microprudence)[16]. Among these, systemic risk is positioned as an area that should be supervised by the authorities, while risks at the individual financial institution level are to be managed by each institution itself. Regarding the former, the authorities in the EU and UK have begun initiatives to designate and supervise critical third parties with potential systemic risks. Entities subject to this regulatory supervision includes service providers, such as cloud service providers, where concentration risk is recognized across the sector, and which may impact the resilience of the financial system as a whole.

■ Situation in Overseas Financial Institutions

It was observed that there are differences between the EU/UK and the US regarding the criteria for selecting critical third parties.

Among the EU and UK financial institutions interviewed, many established their criteria and selected critical third parties based on the perspective of operational resilience in response to regulatory requirements and the stance of the authorities. Selection was based on whether the services provided by the third party to the financial institution could potentially affect the critical operations by the institution (e.g., whether the services are considered critical in terms of operational resilience: whether the survival of the institution could be impacted, which

[16] BoE/PRA/FCA, Operational resilience: Critical third parties to the UK financial sector Supervisory Statement | SS6/24 (November 2024), p.6 "2. Key terms">"critical third party" and p.8 "systemic third party service"

includes how quickly recovery is required in the event of a service interruption [RTO perspective]; whether an interruption would have an unacceptable impact on customers [customer protection]; and whether the survival of the institution could be impacted, such as whether a significant financial impact to the financial institution could occur or whether the institution's licensing status could be affected). An inherent risk assessment was conducted to confirm the nature of the service (such as the type of service provided or data handled) and determine its criticality from an operational resilience perspective. For services where confidential data is entrusted to third parties, the determination of criticality was made not so much from the perspective of information leakage risk, but rather from the perspective of whether an inability to access the entrusted data due to service interruption would have a significant impact on continuous service provision. The perspective of cybersecurity risk alone was confirmed as part of the inherent risk assessment.

At many US financial institutions, the determination of whether a third party is considered critical is made using inherent risk levels. Inherent risk assessments were conducted to confirm items such as the following and determine whether or not to classify third parties as a critical third party based on the overall risk level that the services provided by them may pose to the institution's operations, with operational resilience included as a key assessment component.:

- ✧ Whether the arrangement involves critical operations for the institution
- ✧ The amount spent on the transaction
- ✧ Whether service interruptions would impact customers or clients (for example, whether customers directly use the service or have direct contact)
- ✧ Whether service interruptions would constitute a violation of laws and regulations or affect the institution's licensing status
- ✧ How quickly continuous service provision must be recovered, and whether alternatives are difficult (whether it constitutes a single point of failure or transitioning to an alternative would be challenging)
- ✧ What types of data are shared or accessed, where such data is stored, and whether the services involve systems or applications that process confidential data
- ✧ Whether the third party service involves any access or connection to the systems/networks of the financial institutions

Furthermore, some US financial institutions answered that they select critical third parties with consideration for compliance with regional laws and regulations such as those in the EU and use these criteria in parallel.

Additionally, at some financial institutions, there were cases in which criticality was assessed

not only based on decisions made in accordance with predetermined criteria, but also by adopting more flexible approaches. Specifically, there existed financial institutions that determined the scope of critical third parties through processes such as voting at committees composed of senior management responsible for each function of due diligence.

Regardless of the different approaches used, many financial institutions interviewed keep the number of critical third parties to approximately 1 to 10% (several dozen to several hundred entities) of their total third parties. This was also the case for financial institutions that utilize more than 10,000 third parties overall. It was noted that this is done in order to implement more detailed risk measures for extremely critical third parties, and that only a limited number of third parties are used for the provision of critical operations at the institution so that in-depth risk management is therefore placed on these top-tier third parties.

Regarding the in-depth management of critical third parties, it was confirmed that all financial institutions, in addition to conducting risk assessments and periodic reassessments for all third parties using a common questionnaire, also implement the following additional measures:

- ✧ Establishment of exit strategies and exit plans
  - ・ Availability of alternative options (in-house or alternative providers)
  - ・ Procedures and testing for transition to alternatives (scenarios under stress and non-stress conditions)
- ✧ Concentration risk monitoring (see "(2) Concentration Risk of Third Parties" for details on approach)
- ✧ Onsite assessments (or detailed evidence-based risk assessments)
- ✧ Highly frequent risk reassessments
  - ・ Re-performing risk assessments on an annual basis at the minimum
- ✧ Risk monitoring
  - ・ OSINT[17]
  - ・ ASM[18]
  - ・ Risk score monitoring[19]

[17] An investigative method that examines legally obtainable information, primarily from internet sources, to collect, correlate, and analyze data that may reveal organizational vulnerabilities or serve as potential avenues for attack.

[18] Identifying and managing an organization's attack surface. A framework for investigating information on IT assets accessible from external (internet) sources and continuously assessing them for vulnerabilities.

[19] A tool or service that periodically evaluates an organization's cybersecurity posture from an external perspective and visualizes the results as scores or rankings.

- Dark web monitoring
- Negative news monitoring

✧ Periodic reporting to senior management (board members, CxOs, etc.)

- Performance of critical third parties
- Incidents, service details, changes in key personnel, and other events related to critical third parties

➢ Types of Cloud Service Providers Being Used

Many financial institutions in the US, EU, and UK responded that they do not prohibit the use of cloud service provider. For example, public cloud service providers are assessed in the same manner as other third parties, with risk evaluated according to the intended use and inherent risk, corrective measures required as necessary, and decisions regarding usage made accordingly.

✧ Some financial institutions also performed evidence-based evaluations for cloud service providers, such as verifying evidence that supports controls. Some financial institutions commented that they conduct onsite assessments as well. Furthermore, many financial institutions commented that SOC 2 reports and similar documents were used only as reference and were not directly used as an appropriate response to risk assessments.

➢ Nth Parties

All financial institutions in the US, EU, and UK manage Nth parties under TPRM, complying with applicable regulations and guidelines. The scope of management includes service providers that support the performance of some or all services or activities provided by third parties.

✧ Many financial institutions, considering the effectiveness of operational management of service providers without direct contractual relationships, manage up to fourth parties. In some institutions, the scope is further narrowed from fourth parties to only those that support critical operations.

The methods for managing Nth parties include visualizing Nth parties used by third parties at each financial institution, adding audit rights to contractual provisions with third parties, and evaluating the third party's ability to manage Nth parties.

✧ During the due diligence process, third parties are requested to list the Nth parties they utilize and the information is registered in TPRM tools, enabling centralized

management of relationships with third parties and risk levels.

- ✧
- ✧ Contract clauses with third parties include agreements to grant financial institutions audit rights, as well as to recognize supervisory and oversight rights of regulatory authorities. In addition, third parties were contractually required to impose on their own third parties (i.e., Nth parties from the financial institution's perspective) management and protection standards equivalent to those required by the financial institution. These measures ensured that financial institutions were able to manage and oversee risks associated with Nth parties.
  - Additionally, clauses regarding approval for the use of Nth parties are included to make prior approval by the financial institution mandatory if a third party wishes to use an Nth party.
- ✧ Financial institutions manage risks associated with Nth parties that do not have direct contractual relationships with the institutions by evaluating the third party's ability to manage Nth parties.
  - This approach is based on the logic that risk management of Nth parties used by third parties is the responsibility of the third party, which has a direct contractual relationship with the financial institution. Furthermore, security control requirements demanded by financial institutions to third parties are also contractually applied to Nth parties, where compliance with the financial institution's security control requirements is mandated under the responsibility of the third party when the Nth party is involved.
  - If deficiencies or issues regarding the third party's ability to manage Nth party risks are identified, financial institutions instruct corrective actions or escalate the issue within the institution for further examination, potentially resulting in the termination of the relationship.
  - Some financial institutions with more advanced initiatives request third parties to obtain evidence from fourth parties, and conduct direct assessments of fourth parties.
  - Furthermore, at some financial institutions, initiatives were observed in which management of Nth parties was not limited to indirect management via third parties but involved more direct engagement. Specifically, with respect to fourth parties and subsequent Nth parties, financial institutions obtained, through written confirmations, consent for the financial institution to conduct direct audits of the relevant Nth parties, and conducted direct audits, including on-site visits

as necessary.

- Management of IT Assets Used by Third Parties

None of the financial institutions in the US, EU, and UK interviewed contractually required third parties for which they do not possess management authority or responsibility to submit IT asset inventories. IT asset management and vulnerability management are included as security standard's items to be observed by third parties, and during risk assessments of third parties, the existence of rules, organizational structures, and processes related to IT asset management and vulnerability management by the third party is verified to ensure that risks are mitigated.

- SBOM[20]

Among the overseas financial institutions interviewed, US financial institutions were relatively more advanced in their SBOM initiatives; however, even in the US, these efforts were still in the trial or pilot phase. Specifically, third parties are required to submit an SBOM for software developed for financial institutions. The financial institution specifies the SBOM format, and third parties prepare and submit the SBOM accordingly. The SBOM also includes items corresponding to crypto inventory[21], making it possible to utilize the information for migration to post-quantum cryptography.

- ✧ It was noted that obtaining an SBOM makes it possible to identify open-source software included in software and is thus useful for vulnerability management.
  - Currently, it was observed that SBOMs provided by third parties were manually reviewed and that the evaluation of third-party IT asset and vulnerability management was also conducted using the results of assessments such as penetration tests performed by third parties.
- ✧ There are considerations to expand the scope in the future to include not only an SBOM, but also an AI BOM and hardware BOM (HBOM).
- ✧ Some financial institutions are considering expanding SBOM submission requirements to third parties such as SaaS and software vendors. However, it was also noted that institutions are facing challenges in, for example, obtaining SBOMs from these third parties due to lack of consent or cooperation, indicating that collaboration

[20] A machine-readable inventory that lists all software components, along with information about their dependencies.

[21] A document or management ledger for systematically listing and managing the cryptographic technologies (such as cryptographic algorithms, keys, certificates, and protocols) used by an organization.

with government authorities would be necessary to address these issues.

(2) Concentration Risk of Third Parties

All financial institutions interviewed in the US, EU, and UK monitor and address service concentration, geographic concentration, and concentration of critical Nth parties, mainly from the perspective of operational resilience in accordance with the applicable regulatory guidelines in each region.

- Measurement Methods for Concentration Risk
  - ✧ Indicators are set for each type of concentration and concentration risk is measured accordingly. Examples are shown in the table below.
  - ✧ Financial institutions use TPRM tools to manage third party concentration risks by utilizing data registered through the TPRM activities. For example, such data is used to raise and send out alerts when thresholds are exceeded, visualize third party concentration on dashboards for fixed-point observation. There were also comments that the use of such tools enables efficient visualization of data according to the needs of institutions, as concentration could also be identified and assessed from perspectives such as by business unit and by geographic region.

Table IV-2. Types of Concentration and Example Measurement Methods

Type of Concentration	Description	Example of Measurement Method
Service Concentration	・ Concentration risk arising from dependence on a single third party ・ If the third party suspends services, a large portion of the financial institution's operations are affected	✧ Total expenditure for specific categories (categories used for management and reporting in in expense/purchasing systems (common third-party categories)) ✧ Proportion of expenditure or number of transactions with a specific third party relative to the total

		expenditure and the total number of transactions
Geographic Concentration	・ Concentration risk arising from dependence on a single country or region ・ If there are multiple third parties in the same country or region, events such as natural disasters, political instability, sanctions, or regulatory changes in that region can affect many of the financial institution's operations	✧ Number of third parties in specific countries or regions classified as high-risk
Concentration of Critical Nth Parties	・ Concentration risk arising when critical third parties with whom the institution has direct transactions with, even if diversified, rely on the same Nth party (fourth party, etc.) ・ Has similar impact as service or geographic concentration ・ If the Nth party (fourth party, etc.) also has transactions as a third party, that information can also be used for risk management	✧ Total expenditure for a specific category, or proportion of expenditure or number of transactions with a specific Nth party (fourth party, etc.) relative to the total expenditure and the total number of transactions

The following initiatives were observed in the utilization of concentration risk information:

- ✧ When entering into a contract with a new third party results in an increase in total expenditure for a specific category and raises the level of concentration, the second line takes note of this situation and analyzes the potential scope of impact.
  - ・ Mechanisms that allow such situations to be detected have been implemented using TPRM tools to raise alerts.
- ✧ The status of concentration risk management is regularly reported to management and risk committees.
  - ・ The concentration risk status of third parties is visualized through dashboards in TPRM tools and utilized for fixed-point observation.
- ✧ When concentration risk metrics exceed established thresholds, third parties are evaluated and reviewed from a concentration risk perspective as part of the third-party selection process.

- Specifically, the concentration status is confirmed and then a determination is made on whether the third party can be replaced (i.e., whether alternative service providers are available). If the third party can be replaced, a transition plan including transition to an alternative service provider (who are listed in advance) or switching to an internal resource is developed.
- There were also comments indicating that concentrating on certain third parties may, for example, lead to improvements in operational resilience and efficiency as well as more flexible resource allocation and enhanced quality through strengthened relationships with third parties, resulting in decisions being made from such perspectives.

➢ Regarding Data Concentration

While concerns may arise that concentrating data with a specific third party could lead to a large-scale information leakage in the event of a cyberattack, no cases were identified in which information leakage risk was managed as a form of concentration risk among those overseas financial institutions interviewed. It was confirmed that each institution monitors data concentration from the perspective of operational resilience.

(3) Ongoing Monitoring

➢ Monitoring Through Cyber Threat Intelligence

Ongoing monitoring includes due diligence being repeated on an annual or similar basis; however, such frequency is understood to be insufficient for identifying risk in a timely manner and thus may increase exposure to cyber risks, therefore, cyber threat intelligence are utilized to confirm the true state of third-party risks in a timely manner. The following introduces advanced ongoing monitoring initiatives among financial institutions in the US, EU, and UK:

- ✧ All financial institutions in the US, EU, and UK conduct cyber risk monitoring of third parties utilizing cyber threat intelligence.
- ✧ The use of cyber threat intelligence enables objective and timely monitoring that does not rely on responses from third parties, and this effect was highly valued. In addition, the technology was also utilized not only as an additional input during pre-contractual risk assessment, but also to confirm whether there have been any significant changes with third parties cyber security risk. Furthermore, in cases where deficiencies such as vulnerabilities were identified as a result of monitoring, examples were observed in which third parties were requested to submit corrective action plans. Although specific methods differ among institutions, approaches such as risk scoring tools,

open source intelligence (OSINT), attack surface management (ASM), and dark web monitoring were utilized.

- Among these methods, risk scoring tools (including ASM functions) are used by the majority of financial institutions interviewed, and ASM is often implemented as a function of risk scoring tools. The reasons cited include expectations that the use of these tools will automate the risk assessment process, reduce workload, and expand the range of third parties subject to monitoring.
- On the other hand, there were also comments indicating that risk scoring tools tend to generate a large number of false positives (i.e., excessive detections), necessitating appropriate tuning and the ability to discern useful outputs. This therefore makes specialized talents a requirement to effectively utilize these tools. Some institutions emphasized manual cyber threat intelligence activities over a reliance on risk scoring tools due to the high incidence of false positives.
- As a use case for threat intelligence, there are examples where organizations monitor small and medium-sized third parties who find it difficult to implement thorough security measures. This helps with early detection of risks, such as the sale of credentials by cybercriminals on the dark web or vulnerable remote access devices and other attack surfaces. Organizations use this information to strengthen the defense of third parties.

✧ Overseas financial institutions have established dedicated cyber threat intelligence teams within their cybersecurity departments. These institutions also conduct these cyber threat intelligence activities through a combination of in-house resources and outsourcing, or in-house. In some cases, specialized teams focusing on third party and supply chain cyber threat intelligence have also been set up.

✧ Monitoring to detect whether information related to themselves as well as their third parties is being leaked on the dark web was also conducted by many financial institutions. In cases where the institution had a policy that prohibits direct access to the dark web, these institutions would utilize external vendors to conduct such activities.

✧ It was observed that the scope of third parties subject to monitoring through cyber threat intelligence varies among financial institutions. Examples are as follows:

- Case where all third parties are monitored:
  Monitoring is conducted for all third parties, and only those for which risks are detected are subjected to further detailed investigation. These detailed

investigations are outsourced to external vendors.

- Case where the scope of monitored third parties is limited:
  Monitoring is limited to third parties with high inherent or residual risk level or critical third parties. Monitoring and detailed investigations are conducted directly by the institution's internal intelligence team.

✧ In order to strengthen their internal intelligence capabilities, some institutions have enhanced their frameworks by hiring personnel with intelligence experience from government agencies, such as the UK's MI6 or US's CIA.

✧ Negative news monitoring

- As another example of advanced ongoing monitoring initiatives beyond cyber threat intelligence, some financial institutions conduct negative news monitoring for third parties by using services based on AI to conduct real-time monitoring of information available on the internet for risk indicators of third parties. For example, financial institutions used services that used keywords provided such as third party names, related geographic locations, and risk domains to automatically identify relevant public information and notify pre-designated members who are in charge of monitoring activities.
- For those financial institutions conducting negative news monitoring, the department overseeing TPRM operations is primarily responsible for this activity. A process to escalate the issue to the relevant contract managers or responsible personnel, depending on the level of potential impact, is implemented in case news containing information that could potentially have significant impact is detected.

➢ Utilization of AI in TPRM

✧ It was confirmed that many financial institutions are studying and preparing for the use of generative AI in ongoing monitoring, other TPRM processes, and its application is still in the research phase. Examples were observed of initiatives below:

- Examples were observed of initiatives that utilize AI to efficiently assess the status of the development of regulations and other arrangements when engaging third parties from different regions or language systems.
- Cases were also identified in which third parties had introduced mechanisms to improve the efficiency of responding to questionnaires from financial institutions by utilizing publicly available web-based platforms. Specifically, on these platforms, third parties disclose various types of security-related information in

advance, such as SOC 2 reports and responses to standard questionnaires, and financial institutions obtain the necessary information from third parties using these platforms in order to conduct evaluations of third-party controls. In addition, these platforms are equipped with mechanisms that accept questionnaires from customers (including financial institutions) via the web, generate draft responses using AI, and provide final responses after human review and revision, indicating that the use of AI for the purpose of operational efficiency is also progressing on the third-party side.

- Framework for Sharing Questionnaires within the Industry
  - ✧ Industry-standard questionnaire templates developed by industry associations as well as frameworks for sharing assessment results through industry-wide platforms or communities exist overseas. It was observed that, among the overseas financial institutions interviewed for this research, some institutions utilized such frameworks for purposes such as operational efficiency. Even in such cases, financial institutions did not rely entirely on these frameworks and instead exercised their own judgment independently.
    - The methods of utilizing industry-standard questionnaire templates varied by financial institution. The following cases were confirmed: using the questions in the common questionnaire template only as a reference; directly using the common questionnaire template in the institution's own TPRM processes; or customizing the template by adding their own questions to meet the institution's own standards and requirements. For those institutions utilizing the common questionnaire template as-is, it was confirmed that this was done from the perspective of making the development of their own institutions' questionnaire templates as well as evaluation processes more efficient.
    - Regarding the framework for sharing assessment results, examples were observed in which financial institutions that are members of industry-wide community-based platforms utilize the most recent third party risk assessment results conducted by other participating organizations using the common questionnaire template on a risk basis. For example, cases were confirmed in which such frameworks were used to improve efficiency in due diligence processes for lower risk third parties, while higher risk third parties are assessed using the institution's own questionnaire template. Furthermore, financial institutions who are also members of such platforms but use internally developed

questionnaires commented that they do refer to the questions and responses as necessary, if a high level of alignment with their own assessment perspectives can be confirmed.

- ✧ For those financial institutions that do not utilize any of these frameworks, the following reasons were cited: the financial institution has already developed their own questionnaire that comprehensively covers control requirements specified by cybersecurity and information security standards such as NIST and ISO; the institution is aware of industry-standard questionnaires but the control requirements and evidence requested for third parties by this institution differ from the perspectives of the industry-standard questionnaires; or the benefits relative to the cost of implementing such frameworks has not yet been identified.

(4) Securing Audit Rights over Third Parties and Methods for Doing So

The following initiatives related to securing audit rights over third parties were observed among the overseas financial institutions interviewed:

- ➢ Contractual Provisions
  - ✧ All financial institutions have obtained audit rights over third parties through contractual provisions.
    - ・ Contracts require access to information and facilities necessary for risk management (for example, access to information on the third party's internal controls, as well as to facilities, systems, and network environments related to the services provided by the third party). In addition to audit rights over third parties, contractual provisions also cover obligations such as incident reporting in the event of information leakage, management responsibility for Nth party use, business continuity planning/disaster recovery (BCP/DR), vulnerability management, and cooperation with authorities.
    - ・ All financial institutions have prepared standard contract templates. These templates include requirements defined by the financial institutions for minimum security controls that third parties must establish as obligations in the contract. For example, requirements that the third party must observe may include data encryption, data leakage prevention, network security requirements, access control, vulnerability management, IT asset management, and physical security measures based on the nature of the third-party arrangement.
    - ・ In certain cases, some financial institutions publicly disclose the minimum cybersecurity control requirements for third parties on their websites in advance.

In actual operations, adjustments to the clauses were sometimes made through negotiations with third parties. In such cases, the legal department was also involved in adjusting the contract clauses, and it was confirmed that personnel in charge of the cybersecurity domain were assigned to the legal department, enabling the organization to negotiate provide explanations to third parties and respond appropriately during the contract process.

- ✧ These requirements aim to ensure that the third party's controls and risk management systems and processes are at a level equivalent to those of the financial institution. It was also confirmed that, at all institutions, third parties refusing audit rights are escalated as high residual risk and may be deemed ineligible for transactions. Responses were also given that stated such third parties are centrally managed and flagged in TPRM tools.

- ➢ Audit Rights and Onsite Assessments
  - ✧ Many financial institutions in the US, EU, and UK secured audit rights to facilities related to services provided by third parties through contractual provisions and conducted onsite assessments of third parties.
    - Responses were given that stated the background for conducting onsite assessments included not only the ability to directly verify the controls of third parties, but also to use face-to-face interactions to build relationships with stakeholders, deepen understanding of facilities, and establish escalation routes in the event of a cyber incident.
  - ✧ In many cases, on-site assessments were conducted on third parties that were considered higher-risk. The purpose of this approach was to narrow down the scope based on risk, assign expert resources to the necessary third parties, and conduct more in-depths evaluations. It was also noted that, in some cases, the implementation of onsite assessments was outsourced to external experts.
    - It was confirmed that, in onsite assessments, the evaluation process was conducted in the same manner as standard risk assessments by reviewing responses and evidence to determine whether the third party's control processes and technological requirements were being met. In addition, onsite assessments included supplementary elements such as observation of controls (for example, requesting actual machine operation on site and observing the facility environment) to confirm the design and operating effectiveness of controls in place.

Due to the impact of the COVID-19 pandemic, some financial institutions had temporarily conducted assessments remotely; however, as challenges were recognized in terms of limitations on collecting more in-depth evidence and accurately assessing the maturity of controls and processes, cases were observed in which financial institutions resumed on-site reviews. Such financial institutions cited, as benefits of on-site reviews, not only the ability to directly verify physical security and similar matters, but also the ability to gain a more accurate understanding of actual processes by conducting face-to-face interviews that allow for deeper, on-the-spot inquiries beyond pre-defined questions.

- ✧ On the other hand, there were also cases where a physical visit was not always deemed necessary if onsite assessments could be replaced by virtual walkthroughs (such as reviewing control evidence or observing facilities remotely via screen sharing). In fact, it was observed that some financial institutions had already removed onsite assessments from their TPRM frameworks. The rationale for this was that, particularly in the post-Covid era, it has been confirmed over the past few years that evidence-based risk assessments conducted remotely could also provide sufficient assurance of third-party controls. For example, confirmation of third-party policies, rules, and processes, as well as confirmation of server configurations and security settings via actual machines, could be confirmed via screen sharing.
  - Under such circumstances, when onsite assessments were actually conducted, the main scope was often limited to verification of physical security controls that required direct inspection. Data centers were cited as examples of third-party categories subject to such assessments.
  - Furthermore, although publicly available information that could be referenced such as SOC 2 reports was referenced by financial institutions, such information does not fully align with each institution’s assessment items and could not be solely relied upon, and therefore, assessments were not omitted.
- ✧ For major cloud service providers (CSPs), it was observed that joint audits were sometimes conducted in cooperation with industry associations, and the results were shared with financial institutions belonging to those associations.

(5) Exit Strategies and Exit Plans

Differences in the use of the terms "exit strategy" and "exit plan" were observed among various overseas financial institutions:

- ✧ In financial institutions that clearly distinguished "exit strategy" and "exit plan," each

term was clearly defined and used accordingly.

- ✧ In financial institutions that do not clearly distinguish "exit strategy" and "exit plan," it was noted that this was only a matter of terminology; when ensuring business continuity in the event of termination or interruption of services provided by third parties, both elements of "exit strategy" and "exit plan" were considered necessary. For example, the term "exit strategy" may be used to include elements of "exit plan."

Although the precise definitions of exit strategy and exit plan differed among the overseas financial institutions interviewed, similar trends were observed as follows (examples of items included in each are as follows):

- ✧ Exit Strategy: A document summarizing the basic policy and overall approach for how the financial institution will respond in the event of termination or interruption of services provided by third parties (including response policies, options, and activation conditions):
  - ・ Activation conditions for the exit plan:
    (Normal circumstances) At the end of the contract period or when planning a transition to a new third party
    (Emergency) When it is determined that the relationship with the third party must be terminated due to force majeure
  - ・ Policy for deciding on the termination or continuation of services dependent on third parties
  - ・ Policy for switching to alternative plans (transition to in-house operations or to alternative providers (which includes listing up alternative provider candidates))
- ✧ Exit Plan: A document summarizing the detailed transition plan to ensure the continuity of operations and services (examples below):
  - ・ Schedule for switching to alternative plans
  - ・ Roles, responsibilities, and resources for switching to alternative plans
  - ・ Costs for transition to alternative plans
  - ・ Internal and external communication strategies
  - ・ Interoperability with alternative providers
  - ・ Transition procedures
  - ・ Procedures for returning or disposing of data, etc.

In some cases, mechanisms were also implemented in the process to ensure that exit strategies

and exit plans are always developed and approved at the time of the initial contract and during contract renewal with critical third parties. It was observed in many cases that the third parties subject to the development of exit strategies and exit plans were often limited to critical third parties.

- ✧ In the case of critical third parties providing services with no alternatives, more detailed strategies and plans are required due to the significant impact on a financial institution's business operations. Among the financial institutions interviewed in this research, there were cases where the exit strategies and exit plans developed for services highly dependent on critical third parties exceeded 100 pages in volume. Frameworks were implemented in which exit strategies and exit plans were escalated to senior decision-making bodies, such as expert committees, even at their development stage if there was a significant dependence on critical third parties, and their contents were required to be approved by senior management.
- ✧ At those financial institutions requiring the development of exit strategies and exit plans even for low-risk third parties, it was noted that the level of detail for each item is reduced, and only an outline-level exit strategy and exit plan are prepared.
  - ✧ Exit plans developed in advance are also subject to periodic testing, and at present, most financial institutions are examining how to implement these plans through tabletop testing.
  - ✧ Although some financial institutions conduct these tests, there were also comments indicating that periodic testing has become a routine process focused only on checking whether the included items comply with laws and regulations, and its effectiveness is being reviewed.

(6) Incident Response

- ➢ Establishment of Regulations, Systems, and Conditions for System Reconnection in Anticipation of Cyber Incidents
  - ✧ All financial institutions in the US, EU, and UK have developed detailed cyber incident response procedures (playbooks) in anticipation of cyber incidents occurring at third parties. Examples of items included are as follows:
    - ・ SLAs that include reporting, RTO/RPO
    - ・ Reporting flow in the event of a cyber incident
    - ・ Escalation flow to authorities (confirmed through interviews with EU and UK financial institutions)
    - ・ Submission of event logs maintained by third parties

- Reporting procedures that include the results of confirming the cause of the incident and the information leaked
- Reporting frequency
- Response procedures in the event of network disconnection (if applicable)
- Procedures for switching to insourcing, alternative providers or plans, and the approval process (cyber contingency plan)
- Conditions and procedures for reconnecting to the network
- Third-party risk assessment and approval process for reconnection

✧ The conditions for reconnection are determined by confirming the impact of the cyber incident and results of the response measures implemented by the third party and conducting a risk assessment regarding reconnection to the third party. Reconnection is only carried out if it is judged and approved that there are no issues. In some cases, third party evaluation results are utilized in the decision-making process for reconnection, although these were not mandatory at all institutions interviewed.

✧ Cyber incident response plans are reviewed at least annually through tabletop testing and cyber simulation drills, and these are conducted for critical third parties.

✧ Furthermore, in the event of a cyber incident, the responses given stated that a specialized cybersecurity incident response team works in cooperation with the contracting department, with the technical response handled by the cybersecurity incident response team and departments such as the contracting and legal affairs departments addressing the incident from a business perspective. In addition, there were also cases where organizations have established frameworks that enable the necessary procedures, such as network disconnection, to be carried out in the event of a cyber incident for third parties connected to the organization's systems and networks, regardless of the type of third party involved such as external contractors or partners.

✧ In the event of a cyber incident at a third party, some financial institutions were observed to require the third party to develop measures to prevent recurrence and to review the content of those measures as part of their operational practices. In addition, there were cases in which financial institutions terminated their contracts with the third party when the recurrence prevention measures were deemed not to be sufficiently effective.

(7) Management of Insurance Agents and Similar Entities and TPRM

➢ Management Policies for intermediaries (insurance agents, brokers), and Similar Entities

- ✧ Intermediaries (insurance agents, brokers) have so far been managed outside the framework of TPRM. Due to differences in business practices overseas, insurance agents mainly function as intermediaries and do not retain policyholder information, resulting in many cases where the inherent risk is considered as "low."
- ✧ On the other hand, since there are some intermediaries (insurance agents, brokers) who have access to policyholder information retained by insurance companies, in these cases, although the intermediaries were managed under a different program from TPRM, insurance companies also evaluated and managed the security measures of them. It was also observed that some overseas insurance companies expand the scope of TPRM and Cyber Threat Intelligence monitoring to include intermediaries. In this case, insurance companies classify intermediaries (insurance agents, brokers) as a type of third party category in their policies, and in addition to cases where TPRM and the management program of intermediaries are integrated into a single framework, it was also observed that implementing a hybrid approach that the management programs of intermediaries and TPRM are partially integrated (e.g., evaluating and visualizing inherent risks such as system access and the possession of critical data and managing them on a risk-based approach, and the databases used for management between TPRM and intermediaries management).
- ✧ It was observed that some insurance companies manage third party administrators (TPAs), which handle contract management and insurance claim payments, within the TPRM framework.

➢ Management Policies for Service Providers Associated with Insurance Products

- ✧ How service providers associated with insurance products (such as second opinion services) were managed varied among insurance companies. There were cases where insurance companies limit their involvement to mediating between the service provider and the policyholder, with the policyholder directly contacting the service provider (thus, the information is not handled as part of the insurance company's data) and therefore exclude such providers from TPRM management. Conversely, there were cases where, because the service provider handles the insurance company's policyholder information through mediation, the provider is managed within the TPRM framework.
- ✧ In cases where the service provider provides IoT devices (e.g., cameras) and collects/processes customer data themselves, it was confirmed that such service providers were managed under the TPRM framework. However, there were also comments where insurance companies have revisited their service structure and

shifted to receiving data directly from policyholders as well as processing and storing such data in-house, instead of handling them in an external environment, from the perspective of personal information protection.

VI. Insights for Japanese Financial Institutions

In this section, implications for the hypothesis on challenges on Japanese financial institutions are considered based on research into relevant laws, guidelines, and best practices of financial institutions in the US, EU, and UK.

(1) Classification of Third Parties and Management Policies

➢ Method of Third-Party Classification and Third Parties Subjected to Management

① Challenges

- ✧ In Japan, the Financial Services Agency's "Guidelines on Cybersecurity for the Financial Sector" defines third parties as "*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*" and indicates that third parties should also be managed. Against this background, Japanese financial institutions have begun to expand the classification of entities subject to management beyond traditional outsourcing vendors and cloud service providers, but they are facing challenges regarding the method of classification.
- ✧ There is a need among Japanese financial institutions to understand reference cases regarding the following points when considering the expansion of the scope of third parties to be managed:
  - Which third parties should be included or excluded from the scope of third-party risk management
  - How to classify third parties

② Considerations for Japanese Financial Institutions

Through research with overseas financial institutions, it was confirmed that the widely shared view in TPRM was that, in principle, all third parties should be included within the scope of management. In the EU and UK, however, there were cases in which regulated third parties such as Financial Market Infrastructures (FMIs) and card networks, were excluded from the scope of TPRM. As an overall trend, the mainstream approach is to cover all third parties engaged in transactions with financial institutions and to respond on a risk-based basis according to the importance of the risks. Overseas financial institutions have gradually implemented TPRM based on guidelines and other standards, and recently, new regulations such as DORA in Europe have been introduced to further enhance its management frameworks.

It is considered difficult for Japanese financial institutions to reasonably explain narrowing down the scope of third parties considering cybersecurity incidents involving third parties have occurred in recent years. Many Japanese financial institutions currently only manage outsourcing, and the classification and management frameworks for all third parties are not sufficiently developed. It was noted that initiating management of all third parties under TPRM at once may not be realistic and that a phased approach was required.

Given this situation, when expanding the scope of third parties subject to management at Japanese financial institutions, it is important first to identify all third parties with which the institution has relationships. Based on the characteristics of those third parties, institutions should then determine the appropriate criteria for classifying third parties and clarify the extent to which they should be included within the scope of TPRM. With respect to the scope of TPRM, it is also considered practical to prioritize higher-risk third parties within each classification category and to include them in the scope of management in a phased manner. Based on the interviews with overseas financial institutions, the perspectives shown in the table below can be considered as classification methods.

Examples of criteria for classification based on risk levels include considerations of inherent risks associated with the nature of the services provided, such as whether confidential information of the financial institution is shared with third parties or whether third parties are connected to the financial institution's information systems, as well as considerations of residual risk, which is assessed by analyzing whether the third party has implemented sufficient controls to address the identified inherent risks. It was also noted that, in considering such classification methods, utilizing existing categories of business partners used by Japanese financial institutions (for example, report classifications used in the master data in procurement systems) can facilitate internal understanding when implementing new frameworks.

Table V-1. Purpose and Examples of Third-Party Classification

Purpose	Examples of Third-Party Classification
Distinction inside/outside the scope of TPRM	➢ Third parties / Nth parties ➢ Intra-group / external third parties ➢ Third parties subject to TPRM / outside the scope of TPRM
Classification based on risk assessment results	● Critical third parties, other non-critical third parties ● High, medium, low risk

Categorization for management/ reporting	[Examples based on expense/purchasing categories] ● Suppliers: Stationery, office supplies, hardware, IT parts, etc. [Examples based on third-party services] ● Technology: Cloud services, data centers, software, etc. ● Non-technology: Call centers, BPO, information services, etc. [Others] ● Government, regulatory authorities, FMI, etc.

➢ **Nth Parties Subjected to Management**

① **Challenges**

✧ While Japanese financial institutions have traditionally managed subcontractors as part of their outsourcing management practices, it is considered that, as the scope of management expands to encompass third parties more broadly, it has become unclear to what extent and in what manner Nth parties should be managed.

✧ There is a need among Japanese financial institutions to understand reference cases regarding the following points:

- Which Nth parties are included as management targets in TPRM
- How those Nth parties are managed from a risk management perspective

② **Considerations for Japanese Financial Institutions**

It was confirmed that all overseas financial institutions recognized the existence of risks arising from Nth parties, and therefore, subjected Nth parties to management as well. Regarding the scope of Nth party management, it was observed that service providers related to services offered by third parties were included.

At Japanese financial institutions, similar to the practices observed at overseas financial institutions, outsourcing partners are required to manage their subcontractors, including conducting capability assessments and exercising controls through contractual arrangements. In addition, Japanese financial institutions also sometimes required outsourcing partners to either list all subcontractors down to the lowest tier or limit the number of tiers of subcontractors used by outsourcing partners, thereby implementing stricter controls. However, it was observed that, among Japanese financial institutions, the measures were sometimes insufficient when outsourcing work such as administrative operations and the scope of third party management being limited. Therefore, one possible approach is to conduct comprehensive assessments and reviews from the perspective of whether Nth-party risks exist, without limiting the scope to specific outsourcing partners and including administrative service

providers and similar entities.

- **Third party, Nth-party IT Asset Management**

① **Challenges**

- ✧ At Japanese financial institutions, while there have been advancements in the management of their own IT assets—such as not only using traditional system ledgers but also automatically collecting IT asset information with tools and promptly identifying as well as addressing vulnerabilities linked to those assets—direct management of third-party IT assets is difficult, except for cases such as the outsourcing of system operations to an external provider. Furthermore, due to reasons such as third parties refusing requests to provide information due to internal regulations, there are cases where confirmation is limited to verifying, via checklists, that third parties are managing their IT assets. As a result, there are challenges regarding management of vulnerabilities in third-party IT assets and the actions taken by third parties in response to vulnerabilities after a cyber incident.
- ✧ Therefore, there is a need to understand reference cases regarding how overseas financial institutions collect information on how third-party IT assets and associated risks are managed.

② **Considerations for Japanese Financial Institutions**

It was confirmed in this research that, as shown in the table below, initiatives requiring third parties to submit IT asset inventories and financial institutions to directly manage third-party IT assets were limited even among overseas financial institutions. Basically, it was observed that financial institutions evaluated the management capabilities of third parties by confirming whether regulations were in place regarding third-party IT asset and vulnerability management, and by requesting evidence of the execution of specific control measures, such as system configuration diagrams, for systems where third parties store or process data belonging to the financial institution.

Additionally, it was noted that some major overseas financial institutions have started to experimentally utilize SBOMs, and further deployment is expected in the future due to requests for cooperation to cloud vendors and automation using tools.

Table V-2. Cases for Verifying Controls Related to TP IT Asset Management at Overseas Financial Institutions

Cases at Overseas Financial Institutions	
Methods for Verifying IT Asset Management	➢ Direct management, such as requiring an IT asset management ledger, has not been implemented. ➢ The control status of third parties is confirmed by checking relevant policies and regulations.
Methods for Verifying Third-Party Use of Cloud Services	➢ Cloud services used by third parties are managed as Nth parties, and the control status of third parties is verified and monitored. ➢ For global cloud providers that are also managed directly by the financial institution itself and whose control status is already understood, a separate assessment is not conducted; instead, the focus is on confirming how the third party manages and controls their use of the cloud services.
Status of SBOM Utilization	➢ Some institutions are conducting pilot projects for SBOM management. Even within these efforts, management using dedicated tools is limited; the process is still in a trial phase, with manual reviews of SBOMs provided by third parties. ➢ There are still cases—such as some SaaS vendors—where SBOMs are not yet being provided.

For Japanese financial institutions as well, it is expected to be difficult to directly manage third-party IT assets, such as by requiring the submission of IT asset inventories. On the other hand, for third party's system that store or process financial institution data, it is possible to request information about the third party's control environment, but also, when necessary, to communicate specific details from relevant policies or requirements via IT or cybersecurity personnel and confirm these with the third party. This approach could encourage the submission of necessary information and help verify the status of IT asset management.

➢ **Criteria for Determining Criticality and Management Methods for Critical Third Parties**

① **Challenges**

✧ In this research, both overseas and Japanese authorities required intense management of critical third parties. While the concept that critical third parties should be managed intensively is understood among Japanese financial institutions, perspectives of what constitutes a "critical" third party differ depending on the department or individual, and a unified view has not been established.

✧ There is a need among Japanese financial institutions to understand reference cases for the following points when identifying critical third parties in TPRM:

・ On what criteria critical third parties should be selected

- How to manage critical third parties

② Considerations for Japanese Financial Institutions

The guidelines issued by regulatory authorities in the EU and the UK emphasize operational resilience as a key criterion for identifying critical third parties.

In line with these approaches, it was observed that financial institutions in the EU and the UK interviewed in this research tended to designate third parties whose problems would immediately affect the business continuity or service provision capabilities of the financial institution as critical third parties from the perspective of operational resilience. At US financial institutions, it was noted that critical third parties were selected based on operational resilience and whether inherent risks associated with the business or purpose for which the third party was used were extremely high. It was also confirmed that, in some US financial institutions, multiple categories of critical third parties were established to comply with EU and UK regulations. Specifically, it was observed that, apart from identifying third parties as critical based on the perspective of inherent risk, a separate category of critical third party was defined based on the perspective of legal compliance, and those important for business continuity were managed under this category.

Furthermore, it was observed that all overseas financial institutions interviewed conducted more intensive management of critical third parties. For example, additional measures included in-depth risk assessments using more detailed evaluation items, increasing the frequency of reassessments, requiring the formulation and testing of exit strategies and plans, establishing cyber incident response plans, and monitoring concentration risk. These types of additional measures for critical third parties were also indicated in the "Cybersecurity Guidelines for the Financial Sector"[22] issued by the Japanese Financial Services Agency. As further examples of additional measures for critical third parties, it was noted that cyber threat intelligence monitoring was conducted. Specific examples included ongoing monitoring of third-party vulnerabilities using risk scoring tools and ASM, dark web monitoring by intelligence teams, and, at some overseas financial institutions, negative news monitoring of third parties—including from a cybersecurity perspective—using AI.

[22] Financial Service Agency, "Guidelines on Cybersecurity for the Financial Sector" (October 4, 2024), p.34 and related sections

It was observed that, among the overseas financial institutions interviewed, the number of third parties defined as critical accounted for approximately 1 to 10% of the total third-party population at each institution, corresponding to a range of several dozen to several hundred third parties. This reflects the fact that the actual number of critical third parties is limited even when the overall number of third parties is large, and that effectiveness can be maintained by keeping the number of third parties requiring intensive management at a manageable level. It is considered necessary for Japanese financial institutions to be aware of this approach when selecting critical third parties.

(2) **Concentration Risk**

➢ **Concentration Risk of Third Parties**

① **Challenges**

✧ Japanese financial institutions may not have clearly defined concentration risk for third parties, and there is a need to confirm reference cases for measurement methods used to determine what constitutes concentration, as well as for efficient management and monitoring methods.

② **Considerations for Japanese Financial Institutions**

It was confirmed that, in international standards and guidelines from the EU and the UK, concentration risk was defined both at the systemic level, which covers risks that can impact the entire financial sector, and at the individual financial institution level, which covers risks that should be managed within the scope of each financial institution (see the table below for an overview). It was observed that all overseas financial institutions interviewed managed concentration risk in accordance with the guidelines. It was also confirmed that authorities collected information on third parties used by financial institutions, and that the information gathered was used by authorities for the identification of systemically important third parties.

Table V-3. Types of Concentration Risk and Their Overview

Type of Concentration Risk	Overview

Systemic Level Concentration Risk	➢ Refers to a risk that impacts the entire financial sector which arises from a dependence on one or a limited number of third parties providing one or more services. ➢ Systemic concentration risk is managed by the authorities in each country (while financial institutions are expected to be aware of systemic concentrations as part of their reporting obligations to authorities).
Financial Institution Level Concentration Risk	➢ Refers to a risk arising when a financial institution depends on one or a limited number of third parties for one or more services. ➢ Financial institution-level concentration risk is managed by individual financial institutions. ➢ Typical types of institution-level concentration risk include: ① Concentration where multiple services are provided by a single third party ② Geographic concentration resulting from dependence on a single region ③ Dependence of multiple third parties on a single critical Nth party

Based on the case studies of overseas financial institutions and the descriptions in various national guidelines, it was noted that good practice is to consider the following approaches for measuring each type of concentration risk (see below):

Table V-4. Types of Concentration and Example Measurement Methods

Type of Concentration	Description	Example of Measurement Method
Service Concentration	・ Concentration risk arising from dependence on a single third party ・ If the third party suspends services, a large portion of the financial institution's operations are affected.	✧ Total expenditure for specific categories ✧ Proportion of expenditure or number of transactions with a specific third party relative to the total number of transactions

Geographic Concentration	• Concentration risk arising from dependence on a single country or region • If there are multiple arrangements with third parties in the same country or region, events such as natural disasters, political instability, sanctions, or regulatory changes in that region can affect many of the financial institution's operations.	✧ Number of third parties contracted in specific countries or regions classified as high-risk
Concentration on Critical Nth Parties	• Concentration risk arising when critical third parties, even if the critical third parties themselves are diversified, rely on the same subcontractor (4th party) • Has similar impacts as service or geographic concentrations • If the subcontractor (4th party) also has direct transactions with the financial institution as a third party, that information can also be used for risk management.	✧ Total expenditure for specific categories or the proportion of expenditure or number of transactions with a specific subcontractor (4th party) relative to the total expenditure / transaction number

It was observed that, as a management method, many of the financial institutions interviewed used TPRM tools to record and visualize the degree of concentration of third parties through ledgers and dashboards, allowing the concentration status to be monitored at any time. Using such functionality, the concentration status of third parties was checked, and it was determined whether alternative third parties were available. In the TPRM process, for service providers where alternative options exist, candidate providers are listed. In cases where no alternatives are available, the direction is clarified, such as shifting to in-house solutions, and an exit plan for transitioning is developed. It was also noted that, among overseas financial institutions, there was recognition that concentrating third parties increases concentration risk but can also provide benefits, such as enhanced operational resilience, efficiency, strengthened relationships, improved quality and flexible resource allocation due to third parties' deeper understanding of the financial institution, and increased proficiency of users at the financial institution. Thus, concentration itself was not necessarily regarded as a risk on its own. Among the financial institutions interviewed, some included concentration risk assessment in the third-party selection process, with the need for risk mitigation considered on a case-by-case basis and the final decision on whether to accept the concentration made by the contracting

department, while others developed business continuity plans (BCP) together with the third party even when concentration was present.

It was also noted that, in this research, there were no cases where data concentration itself was recognized as a concentration risk. Overseas financial institutions tended to view data concentration as a resilience risk, in the sense that, if a third party holding confidential data ceases service, the financial institution's operations would also be interrupted. From the perspective of information leakage risk, the focus tends to be on the specific risks associated with the confidentiality and volume of the data handled in each business activity, rather than on whether the data is concentrated with a particular third party.

In considering the management of third-party concentration risk for Japanese financial institutions, it is first necessary to establish and maintain a centralized ledger or database to analyze dependency or concentration on specific third parties or regions. Once such a database is established and a comprehensive view of all third parties is achieved, the next step is to consider categories for measuring the degree of concentration. For example, it is advisable to define and determine the scope of categories for monitoring third party concentration risk from perspectives such as the impact on business continuity and vulnerability to cyberattacks. After organizing a comprehensive database and defining the management scope, it is practical to proceed with consideration of efficiency improvements through systematization.

(3) On-going Monitoring

➢ **Cyber Threat Intelligence Monitoring**

① Challenges

- ✧ In the TPRM of Japanese financial institutions, on-going monitoring of third-party risks is often conducted by reassessing all third parties simultaneously once a year to confirm that there have been no changes to controls. However, it is recognized that this approach causes a concentration of work during a specific period, resulting in increased burdens on both the frontline and second-line staff.
- ✧ In addition, periodic assessments provide only an evaluation at that point in time, and efforts to appropriately grasp ongoing changes in third-party risks after contract execution are also being considered. In many cases, incident responses are taken only after receiving post-incident reports from third parties, following the occurrence of incidents or other events. Therefore, there is a need to understand reference cases

regarding continuous monitoring activities for third-party cybersecurity risks at overseas financial institutions.

② **Considerations for Japanese Financial Institutions**

It was observed that many overseas financial institutions conducted cyber threat intelligence monitoring during ongoing monitoring of third parties in addition to periodic reassessments.

However, even when utilizing such services, it was noted that information detected may include false positives. Therefore, after detecting risk signs, it is necessary to confirm findings with the third party, adjust the information acquisition conditions of the risk scoring tool, and ensure that personnel with specialized knowledge are available to handle the output information.

It is considered that Japanese financial institutions can benefit from implementing continuous cybersecurity risk monitoring measures after contract execution, referencing the practices of overseas financial institutions. For example, by utilizing risk scoring services and OSINT, the process of continuous monitoring for vulnerabilities in the cybersecurity domain of third parties can be automated and risk indicators can be managed, thereby reducing operational burdens during periods of concentrated activity.

In this research, examples were observed where multiple threat intelligence sources were used to detect signs of cyberattacks on third parties and to monitor the occurrence of such attacks, enabling assessment of potential impacts on the institution and its customers. It was also noted that risk-based monitoring of critical third parties is an effective option.

On the other hand, it is assumed that small and medium-sized financial institutions may find it difficult to establish their own cyber threat intelligence teams. Therefore, it is considered appropriate to focus on selecting third parties for prioritized monitoring, ensuring thorough and periodic re-execution of due diligence, confirming the status of cyber-related audits for third parties, and considering the standardization of third-party assessment items within the industry.

- **Utilization of AI in TPRM**

① **Challenges**

- ✧ In recent years, technologies such as generative AI and AI agents have begun to be utilized in business, and there is significant potential for efficiency and advancement through AI utilization in TPRM as well. Japanese financial institutions need to understand examples of how AI can be used in TPRM and how it is being utilized overseas.

② Considerations for Japanese Financial Institutions

It was observed that, among the overseas financial institutions interviewed as of the time of this research, initiatives to promote the use of rapidly advancing generative AI in business operations had begun. And the research was underway into potential areas and methods for future utilization.

Although current AI usage is still at this level, it was noted from interviews with the financial institutions as well as from publicly available research information that the recent advancements in AI were expected to enable the following types of utilization.

- ✧ Automation of workflows such as risk assessment by AI agents
- ✧ Automatic evaluation of inherent risk by having AI read proposals and SOWs
- ✧ Automatic evaluation by having AI read questionnaire responses and evidence from third parties, etc.

The conventional/traditional AI, which was used to automate predefined activities and perform analysis or judgment on input data, was not recognized as a particularly advanced initiative, as it was already widely used among the financial institutions interviewed. In particular, conventional/traditional AI was widely used for negative news monitoring during ongoing monitoring processes, and many financial institutions had automated the extraction of negative news about third parties from multiple information sources.

At Japanese financial institutions, AI utilization has already advanced in areas other than TPRM. With respect to TPRM, commercial TPRM tools have begun to implement such AI functions, and there is a possibility that these AI-based functions will be adopted without users being aware of them. General AI use cases in operations and AI solutions specialized for TPRM are expected to continue to advance and be provided by IT vendors and industry organizations.

➢ Framework for Sharing Questionnaires within the Industry

① Challenges

- ✧ Japanese financial institutions conduct risk assessments based on questionnaires that are independently designed by each institution. However, challenges remain regarding how to ensure that assessment items appropriately reflect changes in the external environment, as well as how to secure the resources required to implement such updates.
- ✧ In addition, it is considered that there is a need to understand examples of initiatives in which assessment questionnaires are shared among institutions to achieve greater efficiency and enhanced risk management across the industry.

② Considerations for Japanese Financial Institutions

At Japanese financial institutions, it is common to use third-party questionnaires that are prepared by each institution based on supervisory guidelines and the FISC Security Guidelines. By contrast, among overseas financial institutions, initiatives such as the standardization of questionnaires and the sharing of assessment results among financial institutions and corporations have been implemented, and efforts aimed at improving efficiency on both the financial-institution side and the third-party side can also be observed.

There were frameworks, such as industry-wide questionnaire templates, developed and shared by industry associations, as well as industry-wide platforms and communities for sharing the assessment results of third parties. Among the financial institutions interviewed, there were cases where such frameworks were utilized. It was noted that some institutions looked to the question items in the common questionnaire template only as a reference, while others used the templates as-is or customized them by adding their own question items based on their business processes. Regarding industry-wide platforms or communities, it was confirmed that some institutions also used the recent third-party risk assessment results conducted by other organizations as a reference only if questions were based on perspectives similar to those of their own questionnaires. Through the interview, it was confirmed that benefits of utilizing such frameworks included the option to use industry-standard questionnaire templates without taking time to prepare individual questionnaires, as well as the opportunity to understand perspectives of how other participating organizations conduct risk assessments. On the other hand, some financial institutions that did not use such frameworks stated that although they were aware of such frameworks, they had not yet identified sufficient benefits for using them due to gaps with the control items required at their financial institutions or the costs associated with implementation.

With the recent rise in third-party cybersecurity risks, it is considered important for financial

institutions to share information and work together as an industry to advance TPCRM. From the perspective of operational efficiency as well, utilizing frameworks for sharing industry-wide common questionnaires is considered beneficial. However, the ultimate responsibility for managing third-party risks lies with each financial institution, and the purpose of evaluating third parties is to determine whether risk management at the third party is assured to the same standard as the institution itself. Therefore, even when an industry-wide framework is used, each financial institution needs to make its own independent judgment on this matter and it is essential that each financial institution sets its own risk appetite and applies such frameworks within those parameters.

(4) Securing Audit Rights and Methods for Third Parties

➢ **Contractual Clauses Related to Cybersecurity**

① Challenges

- ✧ At Japanese financial institutions, while requirements regarding information management are stipulated in memorandums or similar agreements with third parties, in some cases, minimum cyber-security requirements that should be ensured are not clearly defined as contractual provisions. As a result, necessary security measures may not be implemented, or institutions may be limited to a practice in which remediation items identified through individual third-party risk assessments are reflected in contracts on a case-by-case basis, leading to challenges in ensuring that the overall security level required under the contract is adequately maintained.
- ✧ As a countermeasure to such concerns, it is considered effective to include detailed minimum security requirements that are applicable to all subjected third parties as standard contractual clauses. There is also a need among Japanese institutions to understand reference cases from overseas, such as what types of clauses are included in contracts to ensure and mandate third-party compliance with security requirements.

② Considerations for Japanese Financial Institutions

It was observed that all overseas financial institutions interviewed included, in their standard contract templates used for all third-party transactions, clauses that specified not only relevant legal requirements but also audit rights and the minimum cybersecurity controls set by the financial institution. In some cases, instead of including the minimum control requirements directly in the contract clauses, overseas institutions published an annex listing these requirements on their websites.

Table V-5. Examples of Clauses for Security Control Requirements to Be Established by Third Parties

Service Provided by Third Party (Examples)	Minimum Security Controls Required of Third Parties (Examples)
➢ High-risk operations, such as cases where the financial institution's confidential data is processed or stored in the third party's environment, etc.	➢ Data encryption (algorithms, key requirements, etc.) ➢ Prevention of data leakage (restrictions on data transfer, storage, etc.) ➢ Network security (firewall requirements, etc.) ➢ Access control (access control, password management, etc.) ➢ Vulnerability management (malware countermeasures, log management, etc.) ➢ IT asset management (version and patch management, etc.) ➢ Physical security management (access to storage locations, monitoring)etc.

In actual operations, standard contract template clauses were not always applied as-is, and adjustments to the clauses were sometimes made through negotiations with third parties. In such cases, the legal department was also involved in adjusting the contract clauses, and it was confirmed that personnel in charge of the cybersecurity domain were assigned to the legal department, enabling the organization to negotiate to third parties during the contract process.

With regard to the situation at Japanese financial institutions, contracts with outsourcing partners now expected to include clauses related to cybersecurity. However, it is assumed that there are still cases where these clauses are insufficient, the existence of contracts from previous years. Due to the large number of third-party contracts adjustments with third parties are required when reviewing contract clauses, it is not easy to uniformly add new clauses to all contracts. Given these circumstances, it is considered effective to prioritize the review and negotiation of contract clauses with critical or high-risk third parties and to update contract clauses based on third-party risk assessments when entering into new contracts or renewing contracts with third parties. For this purpose, it is ideal to establish a setup that enables collaboration not only with the cybersecurity department but also with the risk management department, which oversees company-wide risk, and the legal department, which consists of contract and legal experts.

- **Audit Rights and On-site Assessments**

① Challenges

- ✧ At Japanese financial institutions, the development of such standards is still underway, and there is a need to understand case studies regarding the criteria for determining which third parties should be targeted and which audit methods (including on site assessment) should be used.
- ✧ In Japan, there are cases where major cloud service providers refuse to access to facilities, resulting in difficult negotiations. There is, therefore, a need to understand reference cases from overseas regarding whether audit rights are ensured for such cloud service providers.

② Considerations for Japanese Financial Institutions

Based on interviews with overseas financial institutions, it was confirmed that all institutions included audit rights, including onsite assessments, as contractual clauses with third parties. It was also confirmed that third parties refusing to grant audit rights were escalated to senior management within the financial institution, as well as to the supervisors and senior management of the relevant third-party personnel as non-compliant with the financial institution's requirements. It was also noted that the assessment methods were based on questionnaires established according to the principle of requiring third parties to maintain controls at the same level as the financial institution itself and that evidence-based assessments were conducted inclusive of topics such as the third party's organizational structure, processes, controls, and technologies. Regarding the cybersecurity point of view, which required specialized expertise, it was confirmed that personnel from specialized cybersecurity departments and external experts participated in the assessment process.

On the other hand, it was observed that overseas financial institutions had shifted their emphasis on onsite assessments following the COVID-19 pandemic. Specifically, there was a trend to transition from onsite assessments to remote assessment, using methods such as virtual walkthroughs by screen sharing to observe facilities and verify policy documents, device configuration, and control implementation. In fact, it was observed that some financial institutions had already removed onsite assessments from the regular TPRM risk assessment process and replaced them entirely with remote assessments. There were comments indicating that, during the pandemic, the necessity to substitute onsite assessments with remote methods led to the realization that a certain level of assessment and clarification was possible remotely. As a result, it was observed that the scope of onsite assessments was now focused primarily on the physical security controls of third parties where direct examination was more important.

These points are also considered to provide useful insights for Japanese financial institutions, from the perspective of selecting appropriate audit methods based on the criticality of third parties and the risks and objectives to be assessed. In addition, particularly in the area of cyber security, an expertise is required, and it may be considered an option to involve personnel with knowledge and experience in ICT and server security, as necessary.

Regarding cases where major cloud service providers do not cooperate with audits, resulting in difficult negotiations and challenges in conducting assessments, it is considered that utilizing disclosure materials such as SOC2 reports may serve as an alternative. Based on the results of risk assessments conducted using such information, it is also considered that processes to suspend use of the service provider for critical operations if sufficient assurance cannot be obtained, or to accept the risk and continue using the service provider depending on the operation for which they are used, could also be established. Furthermore, when individual financial institutions face difficulties in negotiating, multiple institutions collaborating as an industry and jointly negotiating with service providers to increase negotiating power is also considered effective.

(5) Exit Strategies and Exit Plans

➢ **Exit Strategies and Exit Plans for Third Parties**

① Challenges

✧ Japanese financial institutions, partly in response to the "Cybersecurity Guidelines for the Financial Sector" issued by the Japanese Financial Services Agency, have begun formulating exit strategies and exit plans. However, it is assumed that financial institutions need consider how to distinguish between these two concepts and what content should be included in each. As a result, there is a need to understand reference cases from overseas, such as the following.

・ Methods for distinguishing between exit strategies and exit plans, and examples of their content

② Considerations for Japanese Financial Institutions

Based on the interviews with overseas financial institutions, it was confirmed that each institution had established documents equivalent to exit strategies and exit plans; however, there was no standardized naming convention or distinction between exit "strategies" and exit

"plans." Although the terminology and specific structure of exit strategies or exit plans vary among financial institutions interviewed, many institutions commonly prepare documents equivalent to exit strategies or exit plans for critical third parties. This reflects the increasing risk of operational disruptions at critical third parties due to the growing number of cyberattacks in recent years. As a result, the development of exit strategies and exit plans is considered to be emphasized as a means of addressing risks that cannot be sufficiently mitigated by traditional BCPs, which have primarily focused on natural disasters

Although no unified standards or terminology were identified in this research, considering the trends in national guidelines and the results of overseas financial institution interviewed, it may be generally considered documents equivalent to exit strategies summarize the basic policy for how a financial institution responds in the event of termination or interruption of services provided by a third party (such as internalization or switching to another third party), while documents equivalent to exit plans detail the specific procedures for such transitions. In some cases, it was noted that the specific procedures described in the exit plan were separately detailed in the institution's BCP. In any case, it is considered important for financial institutions to maintain internal documentation equivalent to exit strategies and exit plans and manage such documentation in an integrated manner, ensuring consistency across documents and continuous updates—such as timely reflection of changes—to prevent any omissions.

Table V-6. Overview of Exit Strategies and Exit Plans

Category	Overview
Exit Strategy	A document summarizing the basic policy and general response of the financial institution in the event of termination or interruption of services provided by a third party ➢ Conditions for activation (e.g., bankruptcy of the third party, cyber incidents, etc.) ➢ Contact information ➢ Policy for determining the continuation or termination of services that are dependent on the third party ➢ Policy for switching to alternatives (internalization, switching to alternative providers) ➢ List of alternative providers, etc.

Exit Plan	A document detailing the transition plan to enable the financial institution to maintain its operations or services ➢ Schedule for switching to alternatives ➢ Roles, responsibilities, and resources for switching to alternatives ➢ Costs associated with the transition ➢ Internal and external communication strategies ➢ Interoperability with alternative providers ➢ Transition procedures ➢ Procedures for return / disposal of data, etc.

It was also observed that ensuring the effectiveness of exit strategies and exit plans was required by guidelines in each region, and in response, overseas financial institutions conducted actual testing and updates of these plans. In many cases, tabletop testing was used to review scenarios. While involving third parties and simulating actual tasks in addition to tabletop exercises may be useful for risk reduction, it was noted that even major overseas financial institutions currently consider tabletop testing to be realistic for regular verification. There were also cases where industry-wide exercises were conducted with third parties on specific themes, such as incident response; for details, refer to "V-(6) Incident Response."

For Japanese financial institutions, as indicated in the "Cybersecurity Guidelines for the Financial Sector" issued by the Japanese Financial Services Agency, it is desirable to first establish exit strategies and exit plans for critical third parties. Although the distinction between exit strategies and exit plans may be a subject of discussion, based on overseas trends, it is considered more important to flexibly position these documents in accordance with the current situation of each institution and in relation to existing documents such as BCPs rather than to focus on strictly defining the differences between strategies and plans. In practice, it is desirable for financial institutions to develop and manage basic policies and procedures for responding to the termination or interruption of services provided by third parties, ensuring alignment with other internal documents. These documents should not be considered complete upon initial formulation; rather, it is important to verify and update them to ensure they function as intended when needed, considering changes in external and internal environments. To facilitate regular verification and updates, such as through tabletop testing, it is essential to define regular update processes and assign roles and responsibilities, thereby establishing an effective maintenance framework.

(6) **Incident Response**

➢ **Development of Provisions, Frameworks, and Conditions for System Reconnection in Anticipation of Cyber Incidents**

① **Challenge**

✧ At Japanese financial institutions, the lack of pre-established cyber incident response plans or contingency plans that anticipate cyber incidents occurring at third parties has resulted in the lack of clarity concerning which department is responsible for responding when such incidents occur. This may lead to delays in incident response or require the cybersecurity department to manage the entire response with limited resources and is thus deemed as a challenge.

✧ Therefore, there is a need among Japanese financial institutions to understand whether they are prepared to address cyber incidents occurring at third parties.

② **Considerations for Japanese Financial Institutions**

It was confirmed that, as shown in the table below, to prepare for incidents at third parties, overseas financial institutions had established cyber incident response plans that described the roles of organizations responsible for responding to cyber incidents, the policy for response from detection to recovery as well as post-incident actions, and communication plans or detailed procedures (playbooks) for each scenario, such as by type of cyberattack. It was also observed that, in some cases, procedures were specifically developed to address incidents at third parties, including reporting processes, procedures for submitting event logs, and steps to be taken when disconnecting network connections. In other cases, even where procedures specifically designed for third parties had not developed, existing cyber incident response procedures that anticipated incidents occurring at third parties were applied as the basic policy for responding to cyber incidents occurring at third parties.

In addition to the development of procedures, it was observed that the first-line departments that contracted with third parties were also defined to be responsible for acting as the point of contact during cyber incidents occurring at third parties. These departments collaborated with the incident response team, who are experts in the field, when a cyber incident occurred. The basic approach did not distinguish between internal and external (third party) incidents in terms of how to respond. It was also observed that the incident response teams through activities such as dark web monitoring, detected indications that third parties were under

cyberattack or that information may have leaked from a third party and coordinated with the first-line department acting as the contact point to advance the incident response.

- ✧ In order to improve the effectiveness of responding to cyber incidents at third parties, it was observed that some institutions required third parties to participate in incident response training as necessary and that joint trainings were conducted with third parties such as cloud service providers. The participation of third parties is expected to enable the financial institution to gain useful information for developing scenarios and expert input during discussions on the day of the training. It was also observed that financial institutions tended to participate in industry-wide trainings organized by industry associations for FMIs and similar service providers.
- ✧ In cases where overseas financial institutions and third parties were connected by a network, it was observed that, when a cyber incident occurred at a third party, disconnecting the network from the third party was also considered. In such cases, recovery decisions were made based on established procedures, and, if necessary, assessments by external parties were utilized to inform decisions regarding reconnection.

Table V-5. Examples of Initiatives for Third-Party Cyber Incidents at Overseas Financial Institutions

Initiatives and Examples for Third-Party Cyber Incidents	
➢ Normal Operations	➢ Establishment of response plans or procedures for cyber incidents ・ Reporting process in the event of a cyber incident at a third party ・ Escalation flow to authorities ・ Reporting procedures, including confirmation of the cause of the incident and information leaked ・ Contingency plans, including alternative solutions, switching procedures, and approval processes ・ Network reconnection conditions and procedures
	➢ Implementation of joint exercises with third parties ・ At least annual tabletop trainings based on the cyber incident response plan ・ Joint trainings with critical third parties ・ For FMIs, etc., participation in trainings organized by industry associations rather than conducting trainings by themselves
➢ Emergency Operations	➢ In the event of an incident, the department in charge of the contract

	serves as the point of contact with the third party ・ Include contractual obligation for third parties to give notice in the event of a cyber incident ➢ The cyber incident response team provides early detection through threat intelligence activities and expert input ➢ The contracting department and the cyber incident response team collaborate in response

For Japanese financial institutions, it is desirable to establish incident response plans and procedures that anticipate cyber incidents at third parties. By developing reporting processes and conducting regular in-house trainings, institutions can prepare for prompt incident response during emergencies. Furthermore, it is considered effective to enhance the effectiveness of procedures by conducting joint trainings with critical third parties. At overseas financial institutions, it was observed that not only the cybersecurity department but also the first-line contracting departments are responsible for taking on roles during cyber incidents, and a framework for collaboration between the first-line and the incident response team is in place. Therefore, it is considered important not only for the cybersecurity department to develop incident response plans and procedures, but also to advance the sophistication of the TPRM framework by involving the main contracting departments for third parties in the development of cyber incident response.

(7) **Management Policy for Insurance Agents, etc.**

➢ **Management Policies for Third Parties Related to Intermediaries (Insurance Agents, Brokers) and Third Parties Associated with Insurance Products**

① **Challenge**

✧ Japanese insurance companies have historically established management programs for intermediaries (insurance agents, brokers) and have conducted periodic reviews. However, the recent increase in risks, such as customer information leakage at insurance companies caused by cyberattacks targeting third parties, is similarly affecting counterparties, including agents, brokers and service providers associated with insurance products that may hold sensitive information of insurance companies. As a result, insurance companies are required to develop measures and approaches to manage those risks, but are struggling to come up with methods for doing so.

✧ Therefore, Japanese insurance companies need to understand the methods used by overseas insurance companies to identify risks associated with intermediaries

(insurance agents, brokers), as well as their management policy for those counterparties.

② Considerations for Japanese Insurance Companies

It was observed that, among the overseas insurance companies interviewed, intermediaries (insurance agents, brokers) had previously been managed outside the TPRM framework. However, since some intermediaries (insurance agents, brokers) had access to policyholder information, measures were taken to expand the scope of TPRM management and Cyber Threat Intelligence monitoring to include them for the purpose of risk visualization and enhanced management. It was also noted that, with respect to service providers offering services associated with insurance products such as second opinion services, there were cases where these providers handled policyholder information in order to act as intermediates, and as a result, they were also managed within the TPRM framework on a risk-based approach.

For Japanese insurance companies , it is expected to be difficult to immediately include all third parties, such as insurance agents, within the scope of TPRM due to the wide variety of parties involved. Therefore, as seen in examples (assesses inherent risks and prioritizes third parties on a risk-based approach, thereby allocating resources to those that require more in-depths management) from overseas insurance companies, it may be appropriate to consider establishing a hybrid mechanism that partially expands the scope of TPRM to include intermediaries. In addition, regarding service providers associated with insurance products, it is considered appropriate to review management policies, taking into account the nature of the information handled and the relationships among the financial institution, third parties, and policyholders.

Furthermore, given the large number of entities that would be involved, it is expected to be difficult to rely solely on traditional third-party risk assessments using questionnaires to monitor risks such as cyber threats in real time. Therefore, as observed in examples from overseas insurance companies, utilizing Cyber Threat Intelligence may be considered as one option.

VII. Conclusion

In this research, advanced cases of TPCRM and regulatory trends among major financial institutions in the US, EU, and UK were examined, and considerations for Japanese financial institutions were analyzed. It was observed that the initiatives of overseas countries, which have gone ahead of Japan in expanding the scope of management from outsourcing partners to a broader range of third parties, can be utilized for the enhancement of TPCRM in Japanese financial institutions. In recent years, the threat of cyberattacks has increased, with more cases of risk materialization and growing impacts not only on financial institutions but also on society as a whole. It is expected that Japanese financial institutions will appropriately assess their own third-party cyber risks and, with reference to the findings of this research, further advance their TPCRM initiatives.

VIII. Appendix

Guidance for Reference by Japanese Financial Institutions

Appendix 1: List and Overview of Relevant Laws, Regulations, and Guidelines

(1) Basel Committee on Banking Supervision（BCBS）

Premise:

"Principles for the sound management of third-party risk" is a consultative document issued by the Basel Committee on Banking Supervision, which sets forth principles for the sound management of third-party risk in the banking industry. The principles in this document are mainly intended for large, internationally active banks and their prudential supervisory authorities; however, the content is also beneficial for smaller banks and authorities in all other countries.

This document presents twelve principles; Principles 1 to 9 provide guidance on effective risk management of third-party service providers for banks, and Principles 10 to 12 provide guidance for supervisory authorities.

Research Items	Principles for the sound management of third-party risk
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】** In this guideline, entities or individuals providing services to banks are classified and defined as follows: (p.3 "III. Definitions") ➢ Third-party service provider (TPSP)： Refers to an entity or individual that directly provides services, activities, business processes, or functions to a bank. ➢ Critical TPSP： Refers to a TPSP that provides critical services to a bank. Critical services are those whose failure or interruption could have a significant impact on the bank's viability, important operations, or ability to fulfill legal and regulatory obligations. ➢ Intragroup TPSP： Refers to a TPSP that mainly provides services within a banking group. This includes entities under common ownership or control, such as parent companies, sister companies, subsidiaries, or service companies. **【Third Parties and Nth Parties Subject to Management】** The concept of TPSPs subject to management by banks covers, in principle, all

Research Items	Principles for the sound management of third-party risk
	entities with which the bank has a formal contractual relationship for the provision of services or business, and this contractual relationship is referred to as a "TPSP arrangement." Such arrangements also include contracts for services provided to banks by intragroup TPSPs, and banks are required to manage risks for intragroup transactions in the same manner as for other contracts. (p.3-4 "III. Definitions") ➢ TPSP Arrangement： Refers to a formal contractual relationship between a bank and a TPSP for the provision of services or business (including outsourcing). The definition of TPSP arrangement does not include financial service transactions between the bank and its customers, employees, or counterparties (for example, acceptance of deposits from consumers, lending to consumers, provision of insurance to policyholders, clearing or settlement services to other banks, or provision/receipt of services related to financial market infrastructure (FMI)). However, business operations supporting these transactions (e.g., compliance or back-office outsourcing necessary for conducting transactions) are included. Additionally, the definition of TPSP arrangement does not include direct relationships with subcontractors to which a third-party service provider outsources services. However, this does not mean that subcontractors do not need to be managed; from the perspective of supply chain risk in TPSP arrangements, management of subcontractors is required. In this guideline, "subcontractors" are classified and defined as follows: ➢ Nth party： Refers to an entity that is part of the TPSP's supply chain and supports the TPSP's provision of services to the bank. This definition includes, but is not limited to, subcontractors of TPSPs. ➢ Key Nth party： Refers to an entity among the Nth parties that supports the TPSP's provision of critical services to the bank. It also refers to entities among the Nth parties that have access to highly confidential bank information (e.g., customer data). **【Criteria for Determining Criticality】** As described above in [Method of Third Party Classification], the criteria for determining criticality require consideration of the impact of the services provided by the TPSP on the bank's important operations. The guideline

Research Items	Principles for the sound management of third-party risk
	presents the following as examples of criteria for such determination: (p.8 "Risk Assessment") ➢ "Monetary scale" ➢ "Operational or strategic importance" ➢ "Tolerance for service interruption" ➢ "Nature of data and information shared with TPSP" ➢ "Substitutability of the service," etc. **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third-Party Concentration Risk】** In this guideline, the concentration risk of TPSPs is defined from two main perspectives as follows: (p.4 "III. Definitions", p.16 "Role of supervisors Principle 11") ➢ Bank level： This refers to the risk arising from a bank's dependence on services provided by a single or a limited number of TPSPs, where the interruption or failure of such services poses a potential impact on the bank's critical operations. This includes, for example, "concentration of multiple services with the same TPSP" or "concentration in a specific region," where the bank has direct TPSP arrangements. It also covers cases in which multiple TPSPs are concentrated with the same key Nth party. ➢ Systemic level： This refers to the risk that dependence on services provided by a single or a certain number of TPSPs (directly or through Nth parties) may have systemic effects on the entire banking sector, or in some cases, the broader financial sector, through service interruptions or failures. Supervisory authorities are required to analyze available information to identify and monitor potential systemic risks caused by concentration of one or multiple TPSPs in the banking sector. As a policy for managing concentration risk at the bank level, this guideline requires banks to implement the following management measures: (p.5 "IV. Third-party risk management principles", p.7-8 "Risk Management") ➢ Banks are required to understand information related to concentration risk

Research Items	Principles for the sound management of third-party risk
	at the systemic level, which is monitored by supervisory authorities. ➢ Banks are required to understand information related to concentration risk at the systemic level, which is monitored by supervisory authorities. ➢ For effective identification of concentration risk in such lifecycle management, banks are required to maintain an up-to-date TP register, as well as mapping of dependencies and interconnections. If it is difficult to avoid concentration risk, banks are required to strengthen countermeasures such as continuous monitoring and more frequent testing. As additional measures, the following examples are given, and in all cases, banks are required to manage risks within their risk tolerance and preparedness for service interruptions: ➢ Ensuring the availability of critical services provided by a single TPSP (by zone or geographic region) ➢ Confirming that TPSPs are appropriately managing supply chain resilience ➢ Confirming that TPSPs are appropriately managing supply chain resilience ➢ Confirming that TPSPs are appropriately managing supply chain resilience ➢ Confirming that TPSPs are appropriately managing supply chain resilience
(3) Ongoing Monitoring of Third Parties	In this guideline, as ongoing monitoring in the TPSP risk management lifecycle, banks are required to continuously assess and monitor the performance, risk, and criticality of TPSPs after the establishment of arrangements with TPSPs. In addition, banks are required to regularly report the results to the Board of Directors and senior management. (p.12 “Onboarding and ongoing monitoring”, p.13-14 “Reporting”, p.14 “Response”) The following measures are listed as actions that banks should implement in ongoing monitoring: 1. Confirmation of the quality and sustainability of the TPSP's management system, as well as its ability to fulfill contractual obligations. 2. Confirmation of the TPSP's performance status and the occurrence of significant issues or concerns (e.g. significant or recurring findings, deterioration of financial condition, data loss or leakage, service interruptions and other incidents, compliance violations, concentration, and indicators of the materialization of other risks). If, based on the above confirmations, a problem is identified, the following

Research Items	Principles for the sound management of third-party risk
	actions are required: 1. Confirmation of the quality and sustainability of the TPSP's management system, as well as its ability to fulfill contractual obligations. 2. Confirmation of the quality and sustainability of the TPSP's management system, as well as its ability to fulfill contractual obligations. 3. Confirmation of the quality and sustainability of the TPSP's management system, as well as its ability to fulfill contractual obligations. 4. Confirmation of the quality and sustainability of the TPSP's management system, as well as its ability to fulfill contractual obligations. If, as a result of the above monitoring, it is determined that the TPSP is no longer a viable option, the bank must initiate measures to terminate the contractual relationship in a manner that minimizes impact on operations as much as possible. Separately, all TPSP arrangements should be reviewed and evaluated regularly, or when there are significant changes in the bank's internal environment (e.g., organizational structure, conflicts of interest), significant changes in the TPSP (e.g., organizational structure, service delivery location, introduction of new or advanced technology), or significant changes in the external environment (e.g., political, economic, social, legal, and financial conditions, or potential obstacles to service delivery). In particular, arrangements with critical TPSPs should be re-evaluated more frequently. When a bank renews an arrangement with a TPSP, it is necessary to conduct due diligence again before renewal. At that time, it is suggested that information obtained during TPSP onboarding and ongoing monitoring may be utilized. (p.14 "Response")
(4) Securing Audit Rights and Methods for Third Parties	Transactions with TPSPs should be governed by clearly defined, legally binding contracts, and as a method for securing audit rights over TPSPs, the guideline indicates that the bank's audit rights (access to TPSPs, assessment, and acquisition of relevant information) should be considered at the time of contracting. (p.11-12 "Contracting") In addition, it is suggested that contract provisions should include rights for supervisory authorities to access, audit, and obtain information from TPSPs.

Research Items	Principles for the sound management of third-party risk
	Furthermore, in arrangements with critical TPSPs, in addition to the audit rights of the bank and supervisory authorities mentioned above, if important Nth parties are involved in such arrangements, the guideline states that provisions regarding relationships with these important Nth parties should also be included, such as advance notification of use or changes, incident reporting, and rights of supervision, audit, and information acquisition by the bank and supervisory authorities.

(2) Financial Stability Board（FSB）

Premise:

"Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities" is a toolkit issued by the Financial Stability Board for financial authorities, financial institutions, and service providers regarding third-party risk management and oversight.

The purpose of this toolkit is to mitigate fragmentation in regulatory and supervisory approaches across jurisdictions and sectors, as well as to reduce compliance costs for both financial institutions and third-party service providers. It is intended to complement and further develop existing relevant standards and guidance established by international standard setting bodies and financial authorities. Therefore, it does not replace these standards and guidance.

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】** In this guideline, entities or individuals providing services to financial institutions are referred to as service providers, and are defined as entities or individuals that provide services directly or indirectly (e.g., as part of the supply chain of another service provider) to financial institutions. Service providers are classified and defined as follows. (p.5 "1. Common terms and definitions") ➢ Third-party service provider (TPSP)： Refers to a service provider that provides services to one or more financial institutions under a third-party service relationship. ➢ Intra-group service provider： Refers to a member of a financial institution group that mainly provides services to institutions within the same group. This includes entities under common ownership or control, such as parent companies, sister companies,

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
	subsidiaries, and service companies. ➢ Critical service provider： Refers to a service provider that provides critical services to a financial institution. Critical services are services whose failure or interruption could have a significant impact on the financial institution's viability, critical operations, or ability to fulfill key legal and regulatory obligations. Critical operations refer to activities, processes, services, and related assets that, if disrupted, would have a significant impact on the financial institution's ongoing operations or its role in the financial system. **【Third Parties and Nth Parties Subject to Management】** In this guideline, TPSPs subject to management are, as described in [Method of Third-Party Classification], service providers that provide services directly to financial institutions. This includes intra-group service providers. (p.4-5 "1. Common terms and definitions") The relationship between financial institutions and service providers is defined as follows: ➢ Third-party service relationship： Refers to a formal arrangement in which a financial institution receives one or more services or parts thereof from a service provider. The scope of services includes, but is not limited to, activities, functions, processes, and tasks performed by the financial institution. Service provision by intra-group service providers is also included in this definition. The definition of a third-party service relationship does not include financial service transactions between a financial institution and its customers, employees, or counterparties (for example, acceptance of deposits from consumers, lending to consumers, provision of insurance to policyholders, clearing or settlement for other banks, or provision/receipt of services related to financial market infrastructure (FMI)). However, business operations that support these transactions (e.g., compliance or back-office outsourcing necessary for conducting transactions) are included. In addition, outsourcing arrangements in which a financial institution repeatedly or continuously entrusts a TPSP to perform services or parts thereof that the institution would normally conduct itself or could reasonably do so, are also subject to management. Furthermore, the scope of TPSP service relationships subject to management

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
	includes Nth-party service providers that constitute components of the supply chain of services provided by the TPSP, which are defined as follows: ➢ Nth-party service provider： Refers to an entity that is part of the TPSP's supply chain and supports the TPSP's provision of services to the financial institution. **【Criteria for Determining Criticality】** As described above in [Method of Third Party Classification], the criteria for determining criticality should be established based on whether the failure or interruption of services provided to the financial institution would have a significant impact on the institution's viability, critical operations, or ability to fulfill legal and regulatory obligations. Examples of such criteria include: ➢ Financial, operational, or strategic importance of the service ➢ The financial institution's level of tolerance in case of service failure ➢ Nature of data shared with the service provider ➢ Substitutability of the service, etc. This guideline requires that criticality be defined and established by each financial institution, as it differs among institutions. The above criteria may be used as reference information when doing so. Each financial institution is also required to periodically review its criteria for determining the importance of services. (p.13 "3.1 Identification of critical services and assessment of criticality") **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third-Party Concentration Risk】** In this guideline, concentration risk and concentration-related risks of TPSPs in financial institutions are defined as arising from a combination of multiple factors, including the following: (p.28 "3.8.1. Identification of concentration-related risks within individual institutions") ➢ The total number of services supported by a single or closely connected service provider ➢ The number of critical services supported by a single or closely connected service provider ➢ Exposure to certain jurisdictions or regions

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
	The combination of these factors not only creates concentration risk and related risks for individual financial institutions, but may also lead to systemic third-party dependencies across the financial sector, resulting in potential systemic risk. However, it is also indicated that dependence on a single TPSP can bring benefits, such as internal expertise, synergy in business model development, and efficiency in risk management, which can enhance the resilience of financial institutions and improve operational efficiency and flexibility. (p.28 "3.8 Management of concentration-related risks by individual financial institutions", p.36 "Assessment of market concentration") Therefore, in managing the risks of critical services, it is important for financial institutions to consider the overall concentration status of services, identify and assess concentration (as needed, on a group basis), and establish appropriate measures to mitigate such risks. Specific examples of such initiatives include: (p.29 "3.8.1 Identification of concentration-related risks within individual institutions", "3.8.2 Mitigation of potential concentration-related risks") ➢ Enhanced due diligence and audits for TPSPs identified as posing risks during onboarding and ongoing monitoring ➢ Mapping of concentration risk, including risks arising from the TPSP's supply chain ➢ Adding information on the degree of concentration and substitutability of services to the register of third-party service relationships ➢ Measures to ensure that services provided by TPSPs meet standards during normal times and stress events (e.g., business interruptions, abnormal market activities), such as including TPSPs in business continuity plan (BCP) tests ➢ Securing appropriate and feasible contractual rights regarding key Nth-party service providers that may increase risks for critical services ➢ For critical services provided by a single TPSP, requiring provision from multiple availability zones or multiple regions, where possible, to avoid operational or geographic concentration risk Other measures, where appropriate and feasible, include maintaining the capability to insource critical services, selecting different TPSPs for different critical services, designating primary and backup TPSPs for critical services, and maintaining a list of viable alternatives. In such cases, financial institutions are also required to weigh the potential advantages of a multi-vendor approach

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
	against its potential disadvantages, unintended consequences, and risks.
(3) Ongoing Monitoring of Third Parties	In this guideline, ongoing monitoring refers to continuous or periodic activities conducted by financial institutions to assess and manage risks in third-party service relationships, in order to confirm the service delivery capability of third parties in accordance with contractual obligations. Examples of procedures that financial institutions should implement include the following: (p.16-17 "3.2.3 Ongoing monitoring and internal reporting") ➢ Monitoring of key performance indicators (KPIs) related to services provided by TPSPs ➢ Monitoring the TPSP's ability to provide services in accordance with contractual terms, the financial institution's regulatory obligations, and the institution's risk tolerance and risk appetite ➢ Monitoring the financial condition of TPSPs and risks to their financial soundness ➢ Monitoring emerging risks, including political and legal factors, that could affect the continued delivery of services by critical service providers, etc. Financial institutions are required to establish processes for ongoing monitoring of TPSPs, including the above elements, and to establish regular escalation and reporting processes to senior management.
(4) Securing Audit Rights and Methods for Third Parties	Although contracts can take various forms, it is indicated that the rights and obligations of both the financial institution and the TPSP must be clearly specified in any contract. In addition, as matters to be considered at the time of contracting, it is stated that financial institutions should establish rights to access relevant information from TPSPs as necessary (including information on supply chain risk management), audit rights, and rights to obtain information, and that these rights may extend to authorities when necessary. (p.15-16 "Contracting") As specific examples of matters to be considered at the time of contracting, the following are listed: ➢ The legal and regulatory obligations of both the financial institution and the TPSP (including, where necessary, clauses or annexes specifically addressing financial regulations and audit requirements) ➢ Clarification of service performance benchmarks, KPIs, and their metrics ➢ Conditions regulating subcontracting to Nth party service providers

Research Items	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities
	➢ The right of the financial institution to receive accurate and timely information regarding critical services (including, but not limited to, incidents, service details, and significant changes to the TPSP) ➢ The right of the financial institution to appropriately access, audit, and obtain relevant information from the TPSP (including information on supply chain risk management); including, where necessary, the extension of such rights to financial authorities ➢ Commitments regarding operational resilience (business continuity, emergency response plans, disaster recovery, etc.), including minimum operating times, maximum downtime, recovery time objectives (RTO), and recovery point objectives (RPO), etc.

(3) Financial Conduct Authority（FCA）

Premise:

"SYSC" (Senior Management Arrangements, Systems and Controls) is a part of the FCA Handbook, which is issued by the Financial Conduct Authority (FCA) and established under the Financial Services and Markets Act 2000, as amended (FSMA). The FCA Handbook consolidates FCA laws and other regulations.

One of the sections constituting "SYSC" is "SYSC 8.1 General outsourcing requirement," which stipulates how financial institutions (such as banks, securities firms, and investment companies) should design and operate their outsourcing arrangements and related systems. This section includes rules that impose obligations, as well as guidance providing examples and recommendations, with the legal force differing for each item. In addition, the applicability of each item depends on the type of firm and the nature of its business; while these details are specified within SYSC, this report summarizes them simply as "financial institutions" without providing detailed descriptions.

Research Items	SYSC 8 Outsourcing
Classification and Management Policy of Third Parties	**【Method of Third Party Classification】&【Criteria for Determining Criticality】** In this guideline, third parties are described as outsourcing providers that perform regulated activities, listed activities, or ancillary services, and the criteria for determining their criticality are defined as follows (outsourcing providers are also referred to as service providers): (p.2 "8.1.1 R", p.3 "8.1.4 R") ➢ If a defect or failure in performing a business function would significantly impede the ongoing compliance with the financial institution's

Research Items	SYSC 8 Outsourcing
	authorization conditions, obligations, or other regulatory requirements, financial condition, or the soundness and continuity of related services and operations, then the function is designated as critical or important. **【Third Parties and Nth Parties Subject to Management】** As described above in [Method of Third Party Classification] and [Criteria for Determining Criticality], this guideline targets as third parties subject to management those outsourcing providers involved in the financial institution's critical business functions. There is no description in this guideline regarding Nth-party subcontractors that should be managed. **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	N/A
(3) Ongoing Monitoring of Third Parties	In this guideline, there is no direct definition of ongoing monitoring for outsourcing providers of critical business functions. However, it stipulates that financial institutions must take necessary measures to ensure the following conditions are met: (p.4-5 "8.1.8 R") ➢ Service providers must have sufficient capability, systems, and necessary authorizations to perform the outsourced functions in a stable and professional manner. ➢ Methods for assessing the standards of performance by service providers must be established. ➢ The execution of business functions by service providers must be properly audited, and risks associated with outsourcing must be properly managed. ➢ Financial institutions must maintain expertise for auditing and risk management of the outsourced functions and continue to audit and manage these functions and risks. ➢ Service providers must promptly disclose any events that may affect their ability to perform the outsourced functions. ➢ A system must be established that enables the contract to be terminated when necessary without compromising service continuity or quality. ➢ Service providers must cooperate with the FCA and relevant authorities.

Research Items	SYSC 8 Outsourcing
	➢ Financial institutions, auditors, the FCA, and relevant authorities must be able to access data related to the outsourced functions and relevant facilities of the service providers. ➢ Service providers must ensure the protection of confidential information. ➢ Financial institutions and service providers must establish and regularly test business continuity plans, disaster recovery plans, and backup arrangements.
(4) Securing Audit Rights and Methods for Third Parties	Financial institutions are required to secure audit rights by clearly specifying the rights and obligations of both the institution and the service provider in a written contract with the service provider. In addition, financial institutions are required to take necessary measures to ensure that, in the event of an occurrence that could significantly affect the provider's ability to effectively and compliantly perform the outsourced functions, the service provider will reliably disclose such events to the financial institution. (p.5 "8.1.8 R", "8.1.9 R")

(4) Bank of England (BoE), Prudential Regulation Authority (PRA)

Premise:

"SS2/21 Outsourcing and third-party risk management" is a supervisory statement (SS) issued by the Bank of England and the Prudential Regulation Authority, which sets out the PRA's expectations for how PRA-regulated financial institutions should comply with regulatory requirements and expectations related to outsourcing and third-party risk management.

This guideline applies to the following financial institutions. In addition, requirements applicable to certain credit unions and non-directive firms (NDFs) are also specified.

- UK banks, building societies, and PRA-designated investment firms
- Insurance and reinsurance companies subject to Solvency II (including Lloyd's syndicates and managing agents)
- UK branches of overseas banks and insurance companies

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
(1) Classification of Third Parties and Management	**【Method of Third Party Classification】** In this guideline, entities that provide services to financial institutions are referred to as service providers, and are classified and defined as follows: (p.5 "2. Definitions and scope", p.16-17 "Pre-outsourcing phase") ➢ Outsourcing：

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
Policies	Any form of arrangement between a financial institution and a service provider under which the service provider directly (or through subcontracting) performs operations, services, or activities that the financial institution would otherwise itself conduct. ➢ Non-outsourcing： Service providers that do not fall under the definition of outsourcing but have a business relationship or contract with the financial institution and provide products or services. Examples of arrangements that fall under non-outsourcing third-party arrangements include, but are not limited to: (p.6 "2. Definitions and scope" > "Expectations for non-outsourcing third party arrangement" 2.4) ➢ Purchase of hardware, software, or other ICT products -(a) Design and construction of on-premises IT platforms -(b) Purchase of data collected by service providers (data brokers), such as geospatial data, in-app device activity, social media data, etc. -(c) Purchase of "off-the-shelf" machine learning models developed by service providers (including sample data used for training and testing, open-source software, machine learning libraries), etc. ➢ For insurance companies, examples include: -Use of aggregators such as price comparison platforms -Use of delegated underwriting services, etc. Although the forms of non-outsourcing third-party arrangements differ from outsourcing arrangements, risk management is important for banks and insurance companies. The guideline stipulates that appropriate governance and monitoring, similar to those required for outsourcing arrangements, are necessary. Conditions for material outsourcing or third-party arrangements are defined as those in which a failure by the service provider could have a significant impact on the financial stability of the UK, or could hinder the financial institution's ability to comply with threshold conditions (legal status, location of offices, prudent business operations, suitability, effective auditing, as set out by the PRA and FCA in "The PRA's and FCA's Threshold Condition"), fundamental rules (the eight principles for business management set out by the PRA in "Fundamental Rules and Principles for Businesses": 1. Integrity, 2. Skill, care, and diligence, 3. Prudent management, 4. Financial soundness, 5. Effective risk management, 6.

Research Items	Supervisory Statement	SS2/21 Outsourcing and third party risk management
	Internal controls, 7. Cooperation and disclosure to authorities, 8. Planning and minimizing impact in case of failure), related laws, PRA Rulebook, and other requirements. For details, refer to [Criteria for Determining Materiality]. **【Concept of Third Parties and Nth Parties Subject to Management】** This guideline mainly provides explanations regarding outsourcing, but non-outsourcing third parties are also required to be managed from perspectives such as PRA's fundamental rules, business continuity, governance, operational resilience, and risk management (including, but not limited to, cyber risk). (p.5-6 "Definitions and scope" > "Outsourcing" and "Expectations for non-outsourcing third party arrangements") Certain arrangements between regulated financial institutions (e.g., with other financial institutions or financial market infrastructures) are not considered outsourcing. These include clearing, settlement, and custody services, all of which are subject to separate regulatory requirements. Although not defined as outsourcing, such arrangements may pose significant risks and are subject to appropriate monitoring and risk-based management. (p.7 "Third party arrangements subject to regulatory requirements") Management of subcontractors is also required. For material outsourcing or third-party arrangements, in addition to the above management, financial institutions are required to visualize the service provider's supply chain and always maintain an up-to-date list of subcontractors. (p.30 "9. Sub-outsourcing") The PRA expects that, in written contracts for material outsourcing, whether sub-outsourcing is permitted should be clearly stated, and if permitted, financial institutions should secure rights to terminate the contract under certain circumstances, such as when sub-outsourcing significantly increases the institution's risk or is carried out without notification to the institution. (p.31-32 "9. Sub-outsourcing") **【Criteria for Determining Criticality】** The criteria for determining materiality are defined as follows: regardless of whether the arrangement is outsourcing, a service is considered material if poor performance or failure of the service meets any of the following: (p.16-18 "Materiality Assessment") ➢ May have a significant impact on the stability of the UK financial system

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
	➢ Raises serious doubts about compliance with regulatory threshold conditions or fundamental rules ➢ May significantly affect the achievement of requirements of related laws, PRA Rulebook, financial soundness (assets, capital, liquidity, funding), operational resilience (the ability to continuously provide critical business services), etc. ➢ For insurance companies, may impact policyholder protection or the provision of continuous and adequate services In principle, outsourcing of specific functions by financial institutions (such as all regulated activities or key functions) is considered material. Examples include: ➢ Outsourcing of operations subject to OCIR (Operational continuity in resolution: systems to ensure the continued provision of critical services even in the event of institution failure) ➢ Even outside OCIR, outsourcing of operations that may affect PRA's objectives, such as those involving personal information or critical data ➢ Outsourcing of portfolio management, internal controls, or other key functions, etc. Additionally, there are multiple materiality criteria such as business continuity, information security, data protection, difficulty of substitution, scale, and complexity, which must be comprehensively assessed by each financial institution. **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	**【Policy and Examples of Third-Party Concentration Risk Management】** In this guideline, concentration risk is defined as the situation where a financial institution or an entire group is excessively dependent on a particular service provider or its supply chain, such that a risk event at a particular service provider or in a specific region could potentially impact the institution's entire operations, critical business functions, or even the financial system as a whole. This definition includes the following situations: (p.21 "Firm or group-wide concentration risk") ➢ Multiple outsourcing contracts are concentrated with a single or closely connected service provider ➢ Contracts are concluded with service providers for whom replacement or

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
	switching is difficult or impossible ➢ Dependence on service providers is concentrated in a specific region ➢ The situation where multiple independent service providers depend on the same subcontractor or supply chain is also included in the definition To manage such concentration risks, financial institutions are required to take the following measures: ➢ Identify and manage the overall dependency on all service providers ➢ Manage concentration risk arising from multiple contracts with a single or closely connected service provider ➢ Even if not through direct contracts, identify and manage risks where multiple service providers in the supply chain depend on a single subcontractor ➢ Confirm and manage whether there is dependency on service providers that are difficult or impossible to replace ➢ Confirm and manage whether dependency on service providers is geographically concentrated in a specific location (such as a single jurisdiction, country, or region), even if multiple service providers are used (e.g., concentration in offshore or BPO hubs)
(3) Ongoing Monitoring of Third Parties	This guideline requires the board of directors of financial institutions to be responsible for the effective management of risks faced by the institution. This includes establishing an appropriate and effective risk management framework and strategy for dealing with outsourcing service providers. The board should approve, regularly review, and implement the outsourcing policy. One of the minimum contents to be included in the outsourcing policy is the ongoing evaluation and audit of service provider performance, and financial institutions are required to implement the following measures: (p.13-15 "Governance and record-keeping" 4.4, 4.10, 4.14, "Table 4. Contents of the outsourcing policy" > "Oversight") ➢ Daily monitoring of service providers (incident monitoring, regular performance evaluation against service level agreements (SLAs), and strategic periodic evaluations) ➢ Communication, response, and audit when contracts or service providers are changed ➢ Independent audits for compliance with legal/regulatory requirements and policies ➢ Contract renewal processes

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
	For arrangements with service providers deemed material, the following actions should also be taken: (p.22 "Material outsourcing agreement" 6.4) ➢ Determination of materiality and ongoing reassessment (p.17 "Timing and frequency of materiality assessments" 5.8) ➢ Appropriate and proportionate due diligence on service providers (p.20 "Due diligence" 5.18, 5.19) ➢ Documentation of terms in writing (services, duration, relevant regions, conditions for subcontractors [audit, access, etc.], monitoring, SLAs, reporting, business continuity/plans, etc.). If there is no alternative provider, contingency plans and disaster recovery plans should be considered to ensure the continued provision of critical operations in the event of a major failure at the service provider. (p.20 "Due diligence" 5.18) ➢ Notification to the PRA and other authorities regarding material outsourcing arrangements ➢ Securing access, audit, and information rights (including the authority of the PRA and supervisory authorities) ➢ Establishment, testing, and regular review of business continuity plans (BCP) involving the service provider ➢ Assessment and management of concentration and supply chain risks ➢ Ongoing evaluation of service provider performance and corrective management in case of underperformance ➢ Information security goals and measures (minimum ICT security requirements, specifications for the financial institution's data lifecycle, data security [data classification, location, configuration, encryption, access control, segregation, etc. (p.23-26 "7. Data security" 7.1)], network security, and clarification of information regarding security monitoring processes) ➢ Establishment of response procedures for operational and security incidents, including escalation and reporting processes
(4) Securing Audit Rights and Methods for Third Parties	Financial institutions are required to clearly specify, in contracts, cooperation with regulatory authorities and the rights of audit, information access, and site visits to secure audit and information access rights over service providers. In particular, for arrangements with service providers deemed material, contracts must grant the financial institution and supervisory authorities, or their designated representatives, sufficient and unrestricted rights to audit, obtain information, and terminate the contract. It is also required that these rights extend, as appropriate, to subcontractors in the supply chain. (p.21-22 "6.

Research Items	Supervisory Statement | SS2/21 Outsourcing and third party risk management
	Outsourcing arrangement" 6.1, 6.2, 6.3, and p.26-34 "8. Access, Audit, and information rights") When data transfer is involved in arrangements with material service providers, the PRA expects financial institutions to implement the following: (p.20 "Due diligence" 5.18) ➢ Classify relevant data based on its confidentiality and criticality ➢ Identify potential risks and their impacts regarding the relevant data ➢ Agree on appropriate levels of data availability, confidentiality, and integrity ➢ Where necessary, obtain appropriate assurances and documentation from third parties regarding the origin and history of the data, and ensure that data is collected and processed in accordance with applicable legal and regulatory requirements

(5) Bank of England (BoE), Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA)

Premise:

"SS6/24 Operational resilience: Critical third parties to the UK financial sector" is a supervisory statement (SS) jointly issued by the Bank of England, Prudential Regulation Authority, and Financial Conduct Authority (collectively referred to as "regulators").

This supervisory statement sets out the regulators' expectations for how Critical Third Parties (CTPs) should comply with duties and responsibilities imposed by the Financial Services and Markets Act 2000 (FSMA, as amended) and the regulators' rules (collectively, "CTP duties").

Within the statement, the CTP supervisory regime is also referenced. The overall objective of the regime is to ensure that risks to the stability and trustworthiness of the UK financial system—arising from failures or disruptions in services provided by CTPs to financial institutions—are properly managed ("Overall Objective"). CTPs are expected to interpret their duties and the expectations described in the statement in light of this overall objective.

At the time of this research, designation of CTPs in the UK was still under consideration and had not yet been implemented. Although the conditions described below are to be considered, the final designation of CTPs in the UK will be determined by HM Treasury (HMT). The timing of designation remains undecided.

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
(1) Classification and	**【Method of Third Party Classification】** This guideline defines the relationship between financial institutions ("Firms") and entities providing services to them as a "third-party arrangement" from the

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
Management Policy of Third Parties	perspective of maintaining the stability and reliability of the UK financial system. The definition is as follows (p.8 "2. Key terms"): ➢ Third party arrangement： Any arrangement with an external entity that provides products or services, directly or indirectly, to financial institutions as defined by this guideline. This includes cases where: (i) The product or service is something the financial institution would otherwise perform itself; (ii) The service is provided directly by the contractor or by subcontractors; (iii) The service is provided by an entity within the same group (e.g., intra-group services from a parent company to a subsidiary). The guideline defines financial institutions as including: ➢ (i) Entities authorized by the PRA and/or FCA (including dual-regulated and FCA solo-regulated entities), as well as UK branches of non-UK financial institutions (see FSMA section 31) ➢ (ii) Financial market infrastructure entities (as defined in FSMA section 312L(8)), including: - Recognized clearing houses (including central counterparties) - Recognized central securities depositories - UK recognized investment exchanges - Recognized payment systems - specified service providers to recognized payment systems ➢ (iii) Relevant service providers (as defined in FSMA section 312L(8)), including: - Authorized payment institutions, small payment institutions, or account information service providers (as defined in the Payment Services Regulations 2017, regulation 2(1)) - Electronic money institutions (as defined in the Electronic Money Regulations 2011, regulation 2(1)) Based on the above, service providers in such arrangements are classified and defined as follows: ➢ Critical third party： An entity designated by HM Treasury under section 312L(1) of FSMA. HM Treasury will designate an entity as a CTP only if it is satisfied that a failure or disruption in the services it provides could threaten the stability or reliability of the UK financial system.

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	➢ Key Nth Party Provider： A service provider that forms part of a CTP's supply chain and plays an essential role in delivering systemic services to one or more financial institutions. A CTP's supply chain refers to the network of individuals or entities that directly or indirectly provide infrastructure, products, services, or other inputs necessary for the provision, support, or maintenance of systemic services. **【Scope of Third Parties and Nth Parties Subject to Management】** The guideline states that the scope of management covers service providers offering systemic third-party services. A systemic third-party service is one where a failure or disruption (individually or collectively, in the case of multiple services) provided by a CTP to one or more financial institutions (regardless of location) could threaten the stability or reliability of the UK financial system (p.9 "Key Concepts"). **【Criteria for Determining Materiality】&【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** As described above, HM Treasury designates as CTPs those service providers whose systemic third-party services could, in its judgment, threaten the stability or reliability of the UK financial system. The criteria for designation are defined in the regulators' joint "Approach to CTP Oversight" (section 3), based on the following perspectives (p.18 "Focus on CTP's services to firms" and "Approach to CTP Oversight" p.9-12 "Assessing whether to recommend a third party to HM Treasury for designation as a CTP"): 1. Concentration of services provided by the third party to financial institutions: HM Treasury will consider the number and types of financial institutions served by the third party (including whether any are systemically important). Analysis will be conducted on usage across the UK financial system and in specific sectors. Concentration is assessed both in absolute terms (total number of firms relying on the provider) and relative systemic significance. 2. Materiality of services provided by the third party: Authorities assess whether the third party's services could create, amplify, or transmit risks to the UK financial system, based on the concept of "materiality" as defined in UK and international regulatory documents and

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	guidelines on systemic risk. Note that the authorities' assessment of materiality may differ from assessments made by individual financial institutions; not all services deemed material at the firm level are necessarily considered "systemically material" from the regulatory perspective. Assessment axes include "interconnectedness" (the higher the interconnectedness, the greater the potential for failures to propagate across the UK system) and "speed of transmission" (how quickly disruptions could affect the system, with FPC's impact tolerance as a reference). Authorities may treat multiple related services provided by a single provider as a single "systemic third-party service" if, in aggregate, they threaten UK financial stability or reliability. Each individual component of such a systemically important service is also subject to regulation. 3. Other factors relating to potential systemic impact: Authorities also consider other factors, such as availability of substitutes or backups (whether realistic alternatives exist or have sufficient capacity), whether the third party or parties in its supply chain have direct access to financial institutions' assets (which could increase systemic risk, e.g., through cyber-attacks affecting confidentiality, integrity, or availability of assets). HM Treasury designates CTPs at the entity level, but the CTP supervisory regime applies only to services provided by the CTP to financial institutions. The term "service" is defined broadly, encompassing any facility, activity, function, process, task, ICT service, etc., provided by the CTP, thus ensuring that all aspects with a potentially significant impact on the stability and reliability of the UK financial system are covered.
(2) Concentration Risk of Third Parties	**【Policy and Examples of Managing Third-Party Concentration Risk】** In this guideline, the concentration of services provided by CTPs (Critical Third Parties) is highlighted as a macro-vulnerability; it is noted that incidents occurring when services to financial institutions are highly concentrated can have a significant impact on the UK financial system. However, as pointed out in the Financial Stability Board (FSB) toolkit, it is also recognized that concentration of services provided by third parties does not necessarily constitute a systemic risk for the entire market. (p.12-13 "Macro vulnerabilities" 3.8, 3.9) To manage CTP concentration risk, the authorities require any third party

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	designated as a CTP to identify, document, and submit the following within 12 months of designation: (p.36 "Requirement 6: Mapping") ➢ The resources (including key Nth party providers), related assets, support services, and technologies used to provide, support, and maintain systemic services ➢ Internal and external interconnections and interdependencies among the above resources (mapping of these relationships) By conducting this mapping, authorities are able to manage the degree of concentration across the entire supply chain for services provided by the CTP, and to identify single points of failure (e.g., specific subcontractors, services, or regions). Furthermore, this information is used by authorities to identify essential resources and their interconnections for the provision of systemic services within the supply chain, and to design tests (such as incident management test plans for CTPs) to periodically assess whether these resources align with the authorities' objectives.
(3) Ongoing Monitoring of Third Parties	Within the framework for designating CTPs, the authorities require CTPs to effectively manage risks that may affect their ability to provide systemic services. Specifically, CTPs are required to take the following measures: (p.30 "Requirement 2: Risk Management") ➢ <u>(1) Identification and monitoring of relevant risks:</u> CTPs must identify and continuously monitor both external and internal risks that could affect the provision of systemic services. These risks may arise from technological, operational, economic, regulatory, or environmental factors. The guideline highlights "dependency and supply chain risk" and "cyber and technology risk" as particularly important from the supervisory perspective. ➢ <u>(2) Establishment and operation of risk management processes:</u> CTPs are required to establish risk management processes to effectively manage identified risks and to ensure these processes function appropriately. The process must cover all stages: identification, assessment, mitigation, and monitoring of risks. ➢ <u>(3) Regular updates of risk management processes:</u> CTPs must regularly update their risk management processes to reflect lessons learned and findings from: (a) Incidents in CTP operations: Utilizing insights from past incidents to strengthen future risk mitigation.

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	(b) Engagement with regulatory authorities: Integrating feedback from interactions and supervision by regulators. (c) New and emerging risks: Responding to newly arising risks and changes in the external environment. (d) Results of tests and trainings: Reflecting lessons learned from tests and trainings, including those conducted under Requirement 5 (Change Management). *Tests under Requirement 5 (Change Management) refer to pre-implementation tests for changes to the provision, maintenance, or supporting processes and technologies of systemic services. These tests must follow steps including risk assessment (inherent and residual risk), documentation, testing, validation, and approval before the change is made. Additionally, as part of their obligations, CTPs providing systemic third-party services are required to submit the results of self-assessments of these controls (including the above requirements) to the authorities at least annually. (p.47 "Self-Assessment" 7.3, 7.4)
(4) Securing Audit Rights and Methods for Third Parties	This guideline establishes a legal framework by which HM Treasury designates Critical Third Parties (CTPs), which then become subject to supervision by the authorities. The overall objective of the CTP supervisory regime is to manage risks to the stability and reliability of the UK financial system that may arise from failures or disruptions in services provided by CTPs to financial institutions. The criteria for designation are based on whether the service constitutes a systemic third-party service, as described in [(1) Classification of Third Parties and Management Policy]. For CTPs headquartered outside the UK, the supervisory regime does not require them to establish a UK subsidiary or branch, as the regime applies to all services provided by the CTP to financial institutions, regardless of the provider's location. (p.20 "No requirement to establish a UK subsidiary or branch" 4.12) The guideline sets out the fundamental rules for CTPs ("Critical third parties Part of the PRA Rulebook", "Bank of England FMI Rulebook", "Critical third parties sourcebook in the FCA Handbook"), which express the overall objective and represent the core obligations under supervision (p.24 "CTP Fundamental Rules" 5.1, 5.2):

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	➢ CTP Fundamental Rule 1: CTPs must conduct their business with integrity. ➢ CTP Fundamental Rule 2: CTPs must conduct their business with due skill, care, and diligence. ➢ CTP Fundamental Rule 3: CTPs must act prudently. ➢ CTP Fundamental Rule 4: CTPs must have an effective risk strategy and risk management framework. ➢ CTP Fundamental Rule 5: CTPs must organize and manage their affairs responsibly and effectively. ➢ CTP Fundamental Rule 6: CTPs must deal with each authority in an open and cooperative way, and promptly disclose any matter relating to the CTP about which the authority would reasonably expect notice. Rules 1-5 apply only to systemic third-party services provided to firms, whereas Rule 6 applies to all services provided by the CTP to firms. The broader scope of Rule 6 ensures that authorities can receive all relevant information for supervisory purposes. (p.24-25 "CTP Fundamental Rules" 5.3, 5.4) Supplementary explanations are provided for Rules 3 and 6. For Rule 3, prudent conduct includes (p.25-26 "CTP Fundamental Rules" 5.6, 5.8): ➢ Ensuring the company's culture and processes support the overall objective ➢ Maintaining adequate financial, human, and technical resources to provide systemic third-party services to financial institutions during normal and stressed conditions, including operational incidents ➢ Taking reasonable steps to maintain resilience of its own and key subcontractors' infrastructure For Rule 6, a non-exhaustive list of matters that should be notified to authorities includes: ➢ Significant changes to the CTP's business related to the overall objective or CTP duties, including: ・ Changes to corporate/group structure (e.g., acquisitions essential for services to firms) ・ Changes to board, management, or decision-makers responsible for services to firms ➢ Changes to systemic third party services provided to firms, including: ・ Changes to risk profile ・ Changes to maximum tolerable disruption level ・ Planned major change management programs

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	・ Planned or sudden termination/discontinuation of service ・ Changes to essential resources for service provision, including key Nth parties ・ Transfer of service delivery responsibility to CTP affiliates or key Nth parties ・ Changes to geographic locations (jurisdictions) from which services are provided or could be provided, including backup sites ➢ Advance warning of incidents likely to meet the definition of operational incident in the near future ➢ Advance warning of changes to relevant laws or regulations in the UK or other jurisdictions ➢ Matters potentially seriously affecting: ・ the CTP's reputation or its ability to provide systemic services, or ・ fulfill its duties The guideline also sets out operational risk and resilience requirements for CTPs, which apply only to systemic third-party services provided to firms ("Critical third parties Part of the PRA Rulebook", "Bank of England FMI Rulebook", "Critical third parties sourcebook in the FCA Handbook") (p.27 "Operational Risk and Resilience Requirements" 6.1, 6.3): ➢ Requirement 1: Governance CTPs must ensure that their governance arrangements promote the resilience of any systemic third-party service they provide. This includes: (1) Appointing at least one individual who: (a) Is an employee of the CTP or a member of its governing body; and (b) Has the appropriate authority, knowledge, skills, and experience to act as the central contact point with the authorities for supervisory purposes. (2) Defining clear roles and responsibilities for all staff essential to the provision of systemic third-party services at all levels, and establishing clear and well-understood channels for communicating and escalating issues and risks. (3) Developing, overseeing, and implementing an approach that covers prevention, response, adaptation, and recovery capabilities in relation to operational incidents affecting the CTP. (4) Implementing lessons learned from operational incidents and from tests and trainings conducted under Requirement 5, among others. (5) Ensuring appropriate review and approval of information provided to

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	the authorities. (6) Notifying the authorities in writing of the following details: (a) The name(s) of the appointed individual(s) under point (1) (b) The business address(es) of those individual(s) (c) The email addresses, telephone numbers, and out-of-hours contact details for each individual (7) If any of the information notified under (6) changes, promptly informing the relevant authorities. ➢ Requirement 2: Risk Management CTPs must effectively manage risks to their ability to provide systemic third-party services. This includes the following: (1) Identifying and monitoring relevant external and internal risks (2) Ensuring that effective risk management processes are established to manage those risks (3) Regularly updating the risk management processes to reflect challenges and lessons learned arising from: (a) Operational incidents at the CTP (b) Engagement with the authorities (c) New risks and emerging risks (d) Relevant tests and trainings, including but not limited to those conducted in accordance with Requirement 5 ➢ Requirement 3: Dependency and Supply Chain Risk Management As part of the obligations under Requirement 2, CTPs must identify and manage any risks within the supply chain that could affect their ability to provide systemic third-party services. CTPs must take reasonable steps to ensure that key subcontractors and other parties in the supply chain related to the CTP carry out the following: (1) Notification of the obligations applicable to the CTP (2) Cooperate with the CTP to fulfill these CTP obligations (3) Provide the authorities with access to relevant information for the exercise of supervisory functions ➢ Requirement 4: Technology and Cyber Resilience As part of the obligations under Requirement 2, CTPs must take reasonable steps to ensure the resilience of all technologies used to provide, maintain, and support systemic third-party services. This includes the following: (1) Having sound, effective, and comprehensive strategies, processes, and systems in place to appropriately manage risks related to technology and cyber resilience, as part of the obligations under Requirement 2

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	(2) Regularly conducting tests and trainings on these strategies, processes, and systems—including obligations under the authorities' rules—and implementing processes and measures that reflect lessons learned from such tests and trainings ➢ Requirement 5: Change Management CTPs must establish arrangements to systematically and effectively respond to changes affecting systemic third-party services, including changes to the processes or technologies used for the provision, maintenance, or support of such services. This includes the following: (1) Introducing appropriate policies, procedures, and controls to effectively manage the resilience of changes to systemic third-party services (2) Implementing changes to systemic third-party services in a manner that appropriately minimizes the risk of operational incidents occurring at the CTP (3) Ensuring that all changes are subject to appropriate risk assessment, documentation, testing, validation, and approval prior to implementation ➢ Requirement 6: Mapping CTPs must carry out the following: (1) Within twelve months of designation by HM Treasury, identify and document: (a) The resources used for the provision, support, and maintenance of each systemic third-party service provided by the CTP, including personnel (including key subcontractors), assets, support services, and technology (b) The internal and external interconnections and interdependencies among the resources identified in (a) in relation to the relevant service (2) Thereafter, regularly update the processes implemented under (1) ➢ Requirement 7: Incident Management CTPs must effectively manage operational incidents. This includes the following: (1) Implementing appropriate measures to respond to and recover from operational incidents in a manner that minimizes the actual or potential impact on the stability or reliability of the UK financial system (2) Appropriately setting the maximum tolerable level of disruption for each systemic third-party service (3) Maintaining and operating an incident management playbook. The initial version must be prepared within twelve months of designation by HM Treasury and must set out the plans and procedures to be followed by

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	the CTP in the event of an operational incident, including: (a) Response to and recovery from operational incidents at the CTP (b) Facilitation of effective communication and support to authorities and affected financial institutions, both individually and collectively (4) Cooperating and coordinating with authorities and affected entities, including through Collective Incident Response Frameworks, to respond to operational incidents at the CTP ➢ Requirement 8: Service Termination CTPs must take appropriate measures to respond to the termination of any systemic third-party service they provide, regardless of the reason. This includes: (1) Establishing arrangements to facilitate the effective, orderly, and timely termination of the service, and, where applicable, the transfer of the service to other entities, including service recipients (2) Establishing provisions to ensure that service recipients have access to, can retrieve, and can return relevant assets, including, where applicable, the return of such assets in a readily usable format In addition, this guideline sets out how CTPs should comply with the incident reporting requirements for CTP operational incidents ("Critical third parties Part of the PRA Rulebook", "Bank of England FMI Rulebook", "Critical third parties sourcebook in the FCA Handbook"). The incident reporting requirements for CTPs are intended to supplement those imposed on each financial institution, and in particular, to ensure that affected financial institutions receive appropriate, consistent, and timely information about CTP operational incidents, thereby enabling the following (p.60 "Incident Reporting and Notifications" 8.1, 8.3): ➢ Assess the impact on their ability to comply with applicable requirements ➢ Fulfill incident reporting and notification obligations to the authorities ➢ Withstand, respond to, recover from, and learn from such incidents, either individually or collectively These incident reporting requirements for CTPs also enable the authorities to gain an overall understanding of the impact of incidents that occur at CTPs on their objectives, and to respond accordingly (for example, by deciding whether to activate the ARF or by coordinating with other authorities or regulatory bodies in the UK and abroad).

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	These incident reporting requirements apply to operational incidents at CTPs, which are defined as a single event or a series of related events that meet any of the following criteria (p.61 "Incident Reporting and Notifications" 8.6, 8.7): ➢ Cause serious disruption to the provision of systemic third-party services ➢ Affect the operations of the CTP, resulting in the availability, authenticity, integrity, or confidentiality of the assets of financial institutions accessed via those systemic third-party services being, or potentially being, seriously and adversely affected CTPs are only required to comply with these requirements for incidents that actually have an impact as described above; they do not apply to incidents with only potential or unmanifested impact. There is no obligation to report incidents that do not cause such impact ("near misses"). However, CTPs should: ➢ In accordance with CTP Fundamental Rule 6, notify the authorities of incidents that, while not currently having such impact, are highly likely to do so imminently or in the short term ➢ Include aggregate data on near misses and incidents that do not meet the reporting threshold in their self-assessments (as the authorities are particularly interested in improvements, other lessons learned, and commonalities or trends among such near misses) As a staged approach to incident reporting, CTPs must provide the following to both the affected financial institutions receiving the impacted services and to the authorities. CTPs may use various formats for reporting operational incidents to authorities and firms, as long as all information required by the authorities' regulations is included. Optional templates will be provided in due course. Once such templates become available, CTPs may use them to report operational incidents to the authorities. (p.62-63 "Incident Reporting and Notifications" 8.12, 8.16, 8.17) ➢ Initial reporting ➢ One or more interim reporting, as necessary ➢ Final incident reporting For the initial report, after the occurrence of an operational incident at the CTP, the CTP must, as soon as possible and to the extent known at the time of submission, provide an individual initial incident report containing the information specified in the table below to each affected financial institution and the authorities. If there is a conflict between the level of detail in the initial report and the timeliness of reporting to the affected firms and regulatory authorities,

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	the CTP should prioritize timeliness and provide additional detailed information as necessary. When reporting the time of incident detection, both the relevant time in the UK (GMT or BST) and, if different, the local time at the location where the incident was detected must be included. (p.64-65 "Incident Reporting and Notifications" 8.19, 8.20) Information to be provided to authorities and affected financial institutions: (1) Description of the operational incident at the CTP, including: (i) The nature and scope of the following: - Disruption to systemic third-party services (e.g., complete or partial service outage, service not functioning as intended, etc.) - Impact on CTP operations (2) The time the incident was detected, and, if different, the local time at the location where the CTP operational incident was detected (3) The names and number of the affected systemic third-party services (4) The geographical areas (including jurisdictions) impacted by the CTP operational incident (5) The cause of the CTP operational incident, if known (6) The contact details of the person responsible for communicating with the affected financial institutions regarding the CTP operational incident (7) Details of the initial response already taken or planned in response to the CTP operational incident (8) The estimated time required to resolve the CTP operational incident, including the expected recovery time for each affected systemic third-party service (9) Any other relevant information that the CTP reasonably considers pertinent to the initial assessment of the potential impact of the operational incident by the affected financial institutions and authorities Additional information to be provided to authorities only: (10) Names of the affected financial institutions (11) Names of other authorities or organizations that have been notified of the CTP operational incident (12) Any other relevant information that the CTP reasonably considers will assist the authorities in their initial assessment of the potential impact of the CTP operational incident on the stability or reliability of the UK financial system For interim reports, if there is a significant change in the situation described in the initial incident report or any previous interim incident reports (including if

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	the CTP operational incident has been resolved), the CTP must, as soon as possible and to the extent known at that time, provide the authorities and affected financial institutions with an interim incident report containing the information specified in the table below. (p.65 "Incident Reporting and Notifications" 8.21) Information to be provided to authorities and affected financial institutions: (1) Information that the CTP reasonably considers will assist the authorities and affected financial institutions in understanding the nature and scope of the CTP operational incident (2) Measures taken towards the resolution of the CTP operational incident (3) When an operational incident of the CTP has been resolved, the date and time of its resolution (4) Any other information that the CTP reasonably considers relevant to the authorities and affected financial institutions For the final incident report, after the operational incident has been resolved, the CTP must, within a reasonable period, provide the authorities and affected financial institutions with the information specified in the table below. (p.65 "Incident Reporting and Notifications" 8.29) Information to be provided to authorities and affected financial institutions: (1) The date and time when the CTP operational incident was resolved (2) Description of the root cause (to the extent known at the time of submission) (3) Description of corrective measures already implemented or planned by the CTP, including the expected completion date (4) The explanation of CTP's assessments regarding: - The likelihood of recurrence of the CTP operational incident - The long-term impact of the CTP operational incident (5) Description of areas for improvement for the CTP and, where applicable, the affected financial institutions (6) Any other information that the CTP reasonably considers relevant to the affected financial institutions (7) For the authorities only, any other information that the CTP reasonably considers relevant to the regulatory authorities It is also stipulated that CTPs must create and maintain orderly records regarding their business operations and internal organization, to the extent relevant to the provision of services to financial institutions. These records must be sufficient to

Research Items	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector
	enable each authority to: (p.71 "Record keeping" 11.1) ➢ Perform its supervisory functions ➢ Perform its supervisory functions

(6) European Banking Authority (EBA)

Premise:

The "EBA Guidelines on Outsourcing Arrangements" is a set of guidelines issued by the European Banking Authority (EBA). Through these guidelines, the EBA sets out the criteria for determining which arrangements between financial institutions (specifically, banks (credit institutions), investment firms (institutions), payment institutions, and electronic money institutions) and third parties qualify as outsourcing arrangements. The guidelines also provide the criteria for identifying critical or important functions—those that have a significant impact on a financial institution's risk profile or internal control framework. Furthermore, the guidelines stipulate that financial institutions must also manage outsourcing arrangements with third parties located in third countries.

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
(1) Classification and Management Policy for Third Parties	**【Method of Classification of Third Parties】** In this guideline, outsourcing is defined as follows (p.19 "Definitions" 12): ➢ Outsourcing refers to an arrangement of any form concluded between a bank (credit institution), investment firm (institution), payment institution, or electronic money institution and a service provider, under which a process, service, or activity that would ordinarily be performed by the institution itself is instead performed by the service provider. In addition, when determining whether a relationship with a third party falls under the definition of outsourcing, it is stated that the following aspects should be considered in addition to the above definition (p.25 "4. Guidelines on outsourcing, Title II – Assessment of outsourcing arrangements"): ➢ Whether the function (or part thereof) entrusted to the service provider is performed by the service provider on a regular or ongoing basis ➢ Whether the function (or part thereof), even if it has not been performed by the institution in the past, would normally be performed by the institution or is within the range of functions that could realistically be performed by the institution

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	【Third Parties and Nth Parties Subject to Management】 This guideline mainly focuses on the risk management of third parties with whom outsourcing arrangements for critical or important functions are concluded. On the other hand, it is indicated that, even when a financial institution entrusts the provision of services to a third party and the relationship does not fall under an outsourcing arrangement or the delegation of critical or important functions, risks may arise and all risks must be appropriately managed (the risk management initiatives set forth in this guideline are not necessarily limited only to outsourcing arrangements). Specifically, it is stated that third parties with whom contracts other than outsourcing arrangements are concluded should also, in accordance with the principle of proportionality, implement the risk management prescribed in this guideline (identification, assessment, monitoring, and management of all risks). Therefore, financial institutions are required to manage risks for relationships with third parties other than outsourcing arrangements based on the principle of proportionality (p.30 "5. Sound governance arrangements and third-party risk" 33). The background to this is that financial institutions are required to ensure that their outsourcing arrangements comply with EU law and regulatory requirements (e.g., business confidentiality, access to data, protection of personal data), and in particular, when delegating critical or important functions, supervision of the financial institution by the competent authority is also required. However, in the case of service providers located in third countries, it is noted that the competent authority of the third country where the service provider is located may not have sufficient powers or means to effectively supervise the service provider. Specifically, it is stated that a financial institution may only outsource banking or payment service functions to a service provider authorized by the competent authority of a third country if the following conditions are met (p.40 "Title IV – Outsourcing process, 12.1 Supervisory conditions for outsourcing" 63): ➢ The service provider has obtained authorization or registration to provide the relevant banking or payment services in the third country and is supervised by the relevant competent authority of the third country ➢ There is a formal cooperation agreement, such as a memorandum of understanding, between the competent authority responsible for supervising the financial institution and the competent authority

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	responsible for supervising the service provider ➢ The aforementioned cooperation agreement must at least ensure the following: i. Information necessary to carry out supervisory tasks under Directive (EU) 2013/36, Regulation (EU) No. 575/2013, Directive (EU) 2015/2366, and Directive (EC) 2009/110/EC can be obtained upon request ii. Appropriate access to data, documents, facilities, or personnel stored in the third country related to the exercise of supervisory powers iii. Timely receipt of information from the competent authority of the third country for investigating suspected breaches of the requirements of Directive (EU) 2013/36, Regulation (EU) No. 575/2013, Directive (EU) 2015/2366, and Directive (EC) 2009/110 iv. Cooperation with the relevant competent authority of the third country regarding enforcement in the event of a breach of applicable regulatory requirements or the national law of a Member State. Such cooperation includes, but is not limited to, the timely receipt of information from the competent authority of the third country about possible breaches of applicable regulatory requirements In addition, this guideline stipulates that subcontractors related to outsourcing arrangements are also subject to management, and defines subcontractors as follows (p.20 "2. Subject matter, scope and definitions, Definitions"): ➢ Refers to the situation where a service provider further outsources a function entrusted to it under an outsourcing arrangement to another service provider In cases where, under an outsourcing arrangement, a service provider may further outsource critical or important functions to another service provider, the financial institution is required to additionally consider the following points (p.42 "12.2 Risk assessment of outsourcing arrangement"): ➢ Additional risks arising when the subcontractor is located in a third country or in a country different from the service provider ➢ The risk that long and complex chains of sub-outsourcing may reduce the ability of the financial institution to manage the outsourced critical or important functions, as well as the ability of the competent authority to effectively supervise them

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	【Criteria for Determining Criticality】 In this guideline, when assessing whether an outsourcing arrangement concluded between a financial institution and a service provider relates to a critical or important function, it is stated that the financial institution must additionally consider at least the following elements (p.27-29 "4. Guidelines on outsourcing, Title II – Assessment of outsourcing arrangements" > "4. Critical or important functions" 31): ➢ Whether the outsourcing arrangement is directly related to the provision of regulated banking or payment services by the delegating institution ➢ The potential impact, in the event of interruption of the outsourced function or the service provider's inability to continue providing services at the agreed service level, on the following: i. Short-term and long-term financial resilience and viability (including assets, capital, costs, funding, liquidity, profit and loss, as applicable) ii. Business continuity and operational resilience iii. Operational risks (including conduct risk, ICT risk, legal risk) iv. Reputational risk v. Where applicable, recovery and resolution planning, resolvability, and continuity of operations during early intervention, recovery, or resolution ➢ The potential impact of the outsourcing arrangement on the following capabilities of the delegating institution: i. The ability to identify, monitor, and manage all risks ii. The ability to comply with all legal and regulatory requirements iii. The ability to conduct appropriate audits of the outsourced function ➢ The potential impact on services provided to customers ➢ The aggregate dependence on a single service provider in all outsourcing arrangements of the delegating institution, and the potential cumulative impact of concluding multiple outsourcing contracts in the same business area ➢ The scale and complexity of the affected business area in the delegating institution ➢ The possibility of expanding the outsourcing arrangement without amending or revising the underlying contract ➢ The ability, where necessary or desirable, to transfer the proposed outsourcing arrangement contractually and practically to another service provider (substitutability), and the estimated risks, obstacles to business

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	continuity, costs, and time required ➢ The ability, where necessary or desirable, to reintegrate the outsourced function into the institution ➢ The protection of data, and the potential impact on the financial institution and its customers if confidentiality is breached or data availability/integrity is not ensured **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** NA
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** In this guideline, it is stated that competent authorities should assess financial institutions based on a risk-based approach, and that, in doing so, concentration risk should be particularly considered as follows. When concentration risks are identified, competent authorities must monitor the trends of the identified concentration risks and assess their potential impact on other financial institutions and the stability of the financial market. Furthermore, if necessary, it is stipulated that competent authorities must notify the resolution authority of any newly identified potentially critical functions during this evaluation process. The guideline defines the concentration risks to be confirmed by competent authorities from the following two main perspectives (p.54 "4. Guidelines on outsourcing, Title V – Guidelines on outsourcing addressed to competent authorities" 116 d, e): ➢ Concentration risk within a financial institution (including on a consolidated basis): Concentration risk arising from multiple outsourcing arrangements with a single or closely connected service provider, or from outsourcing multiple business functions within the same business area. ➢ Sector-level concentration risk: Risk arising when multiple financial institutions use a single or a small number of service providers. In addition, the guideline also requires that, when conducting risk assessments at the time of outsourcing arrangements, financial institutions must at a minimum consider the following concentration risk perspectives (p.41 "4. Guidelines on outsourcing, Title IV – Outsourcing process" 66 a): (i) Concentration of outsourcing arrangements with key service providers to whom it is not easy to switch alternatives. (ii) Concentration of multiple outsourcing arrangements with a single or

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	closely connected service provider.
(3) Ongoing Monitoring of Third Partie	Financial institutions are required to continuously monitor the performance of service providers for all outsourcing arrangements using a risk-based approach in accordance with the principle of proportionality. In particular, emphasis is placed on outsourcing of critical or important functions, and it is required to ensure the availability, integrity, and security of data. In order to continuously confirm that outsourcing arrangements meet appropriate performance and quality standards in line with the institution's policies, the following must be implemented (p.51 "4. Guidelines on outsourcing, Title IV – Outsourcing process" 104): ➢ Ensure that appropriate reports are reliably received from the service provider ➢ Evaluate the performance of the service provider using tools such as key performance indicators, key control indicators, service delivery reports, self-certifications, and independent reviews ➢ Review all other relevant information received from the service provider, including reports on business continuity measures and testing Furthermore, if a financial institution identifies deficiencies in the provision of outsourced functions, it must take appropriate action, and in particular, if there are signs that the service provider is not effectively performing critical or important functions or is not complying with legal and regulatory requirements, thorough follow-up is required (p.51 "4. Guidelines on outsourcing, Title IV – Outsourcing process" 105). In addition, when entering into outsourcing arrangements for critical or important functions, financial institutions are also required to establish and document exit strategies that are consistent with their outsourcing policies and business continuity plans. In formulating exit strategies, at a minimum, the following scenarios must be considered (p.51-52 "5. Exit Strategies" 106): ➢ Termination of the outsourcing contract ➢ Failure of the service provider ➢ Potential business disruption due to deterioration of the quality of services provided, or inappropriate or failed service delivery ➢ Material risks that arise in the course of proper and ongoing execution of business activities

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	Taking the above possibilities into account, the exit strategy must include the following elements to enable the financial institution to terminate the outsourcing arrangement without causing excessive disruption to business activities, compromising regulatory compliance, or negatively affecting the continuity or quality of services to customers (p.51-52 "5. Exit Strategies" 107, 108): ➢ Develop a comprehensive and documented exit plan, and, where necessary, conduct sufficient testing (e.g., analysis of costs, impacts, resources, and time required for transferring outsourced services to an alternative provider) ➢ Identify alternatives and formulate transition plans, clarifying procedures for transferring outsourced operations and related data from the service provider to an alternative provider or back to the institution itself The guideline specifies the following minimum items to be included: ➢ The purpose of the exit strategy ➢ The human and financial resources and time required to execute the exit plan, based on a business impact analysis (BIA) that corresponds to the risks associated with the outsourced processes, services, or activities ➢ Ensuring roles and resources for managing the exit plan and business transition ➢ Success criteria for the migration of outsourced operations and data ➢ Definition of indicators used to monitor the outsourcing contract (indicators for triggering the exit plan when service levels are unacceptable) Financial institutions are also required to monitor and document the trigger conditions for the exit strategy (such as service provider performance) as part of ongoing management (p.39 "11. Documentation requirements" 60).
(4) Securing Audit Rights and Methods for Third Parties	Competent authorities must confirm that, within outsourcing arrangements, financial institutions secure audit rights and access rights to third parties for both the competent authorities and the financial institution itself. Furthermore, competent authorities are required to assess financial institutions using a risk-based approach regarding the following points: ➢ Whether the financial institution is appropriately monitoring and managing, in particular, outsourcing arrangements for critical or important functions ➢ Whether the financial institution has sufficient resources to monitor and

Research Items	Final Report on EBA Guidelines on outsourcing arrangements
	manage outsourcing arrangements ➢ Whether the financial institution identifies and manages all relevant risks ➢ Whether the financial institution identifies, assesses, and appropriately manages conflicts of interest related to outsourcing arrangements If concerns arise that a financial institution does not have a robust governance framework or is not complying with regulatory requirements, competent authorities should take appropriate measures, which may include restricting or reducing the scope of outsourced functions or requiring the termination of outsourcing arrangements (p.55 "4. Guidelines on outsourcing, Title V – Guidelines on outsourcing addressed to competent authorities"). Additionally, when a financial institution enters into outsourcing arrangements for critical or important functions, it is required to include in the contract clauses that demand and agree upon audit rights for itself, the competent authorities, or designated third-party bodies to audit the service provider. The scope of audit rights to be included is as follows (p.47 "13.3 Access, information and audit rights" 87 a, b): ➢ Full access rights to business premises related to outsourcing (such as the service provider's headquarters and operation centers), as well as access to all relevant equipment, systems, networks, and data used to provide outsourced operations (including relevant financial information, responsible personnel, and the service provider's external auditor) ➢ Unrestricted rights of inspection and audit regarding the outsourcing arrangement (so that monitoring of the outsourcing arrangement and assurance of compliance with all applicable regulatory and contractual requirements are possible)

(7) European Banking Authority（EBA）

Premise:

This guideline has been developed as an updated version of the previous EBA "Guidelines on outsourcing arrangement." Unlike the previous version, which mainly focused on outsourcing arrangements, the updated guideline covers a broader scope of "third-party arrangements," including outsourcing, and sets out the risk management methods, standards, and roles that financial entities and competent authorities should implement regarding such arrangements. Furthermore, the update reflects the enforcement of Regulation (EU) 2022/2554 (DORA) from

January 2023. Specifically, since information and communication technology (ICT) services provided by third parties to financial entities fall under the scope of DORA, this guideline applies to third parties that provide services other than ICT-related services to financial entities. Against this background, after the official implementation of this guideline, financial entities will be required to ensure close consistency in third-party risk management across both regulatory frameworks. In addition, the previous version of the EBA "Guidelines on outsourcing arrangement" will be repealed upon the official release of this guideline.

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】** In this guideline, entities or individuals that provide services to financial institutions are classified and defined as follows (p.20-21 "Definitions"): ➢ Third-party service provider (TPSP): Refers to an entity that provides or supports functions for a financial institution based on an arrangement with the financial institution. ➢ Intra-group third-party service provider： Refers to an entity that provides or supports functions for another financial institution within the same financial group or within the same institutional protection scheme. Furthermore, arrangements with third parties are defined as follows: (p.21 "Definitions") ➢ Third-party arrangement： Refers to any type of contract between a financial institution and a TPSP (including intra-group TPSPs) for the provision of one or more functions to the financial institution. This includes outsourcing arrangements as a part thereof. Outsourcing arrangements included in the above definition of third-party arrangement are defined as follows (p.21 "Definitions"): ➢ Outsourcing arrangement： Refers to any type of arrangement between a financial institution and a TPSP (including intra-group TPSPs), under which the TPSP is required to perform functions that the financial institution would ordinarily perform itself, on a repetitive or ongoing basis. Additionally, this guideline specifies that when a service is used to provide

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	critical or important functions, the TPSP providing those functions is categorized as a "critical TPSP." For the criteria, refer to [Criteria for Determining Importance] (p.27 “4. Critical or important functions”). **【Third Parties and Nth Parties Subject to Management】** This guideline defines TPSPs to be managed as those that directly provide services to financial institutions, considering third-party risks that may arise from the functions or support provided by TPSPs or their subcontractors to financial institutions. This definition includes TPSPs located in third countries as well as intra-group TPSPs (p.20-21 “Definitions”). When utilizing a TPSP located in a third country, the guideline stipulates that a financial institution may enter into arrangements regarding banking or payment service functions with a TPSP authorized by the competent authority of the third country only if the following conditions are met: ➢ The TPSP is authorized or registered to provide the relevant services in the third country and is supervised by the relevant competent authority of that third country. ➢ A cooperation agreement (such as a memorandum of understanding) is appropriately concluded between the competent authority supervising the financial institution and the competent authority supervising the TPSP. ➢ The above cooperation agreement must ensure at least the following: i. Information necessary to perform supervisory duties under Directive (EU) 2013/36, Directive (EU) 2015/2366, Directive (EC) 2009/110/EC, Directive (EU) 2014/65/EU, Directive (EU) 2019/2034/EU, and Regulation (EU) 2023/1114 can be obtained upon request. ii. Appropriate access to data, documents, facilities, or personnel stored in the third country related to the exercise of supervisory powers. iii. Timely provision of information from the competent authority of the third country when a breach of the requirements of Directive (EU) 2013/36, Regulation (EU) No 575/2013, Directive (EU) 2015/2366, Directive (EC) 2009/110, Directive (EU) 2014/65, Directive (EU) 2019/2034, or Regulation (EU) 2023/1114 is suspected. iv. Cooperation with the relevant competent authority of the third country regarding enforcement in the event of a breach of applicable regulatory requirements or national law of a Member State. Such cooperation includes, but is not limited to, the timely receipt of information from the competent authority of the third country regarding possible breaches of applicable

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	regulatory requirements. Additionally, this guideline also covers subcontractors, and defines subcontracting in arrangements with third parties as follows: (p.21 "Definitions") ➢ Refers to a situation where a TPSP transfers functions to another service provider under any form of contract. Subcontracting may also be referred to in other documents as a "chain of subcontracting" or "use of nth party service providers." When, under a third-party arrangement, a TPSP may subcontract critical or important functions to another service provider, the financial institution is required to additionally consider the following points: (p.43 "11.2 Risk assessment of third-party arrangements") ➢ Risks associated with subcontracting contracts, including additional risks if the subcontractor is located in a third country or a country different from the TPSP. ➢ The risks that a long or complex operational chain may reduce the institution's or payment institution's ability to manage externally outsourced critical or important functions, as well as the ability of the competent authority to effectively manage those functions. 【Criteria for Determining Criticality】 In this guideline, the definition of "critical or important function" is in line with Article 3(22) of DORA ("Definitions"), and refers to a function whose interruption could significantly impair the financial performance of the institution or the soundness or continuity of its services or activities, or a function whose interruption, defect, or non-performance could make it significantly difficult for the institution to continuously comply with authorization conditions and obligations, or other obligations under applicable financial services law. This guideline defines critical or important functions as follows: (p.21 "Definitions") ➢ Functions whose failure could have a significant adverse effect on the financial performance, services, or the soundness or continuity of activities of the institution; or ➢ Functions whose interruption or inadequate provision could significantly impede the institution's continuous compliance with authorization

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	conditions or other regulatory obligations. Based on the above definition, this guideline specifies that critical or important functions are those whose failure or interruption would have a significant adverse impact on the following aspects for the institution: (p.27 "4. Critical or important functions" 33 a, b, c) ➢ The institution's ability to continuously fulfill authorization conditions and obligations, or other obligations under applicable laws ➢ The financial performance of the institution ➢ The soundness or continuity of the institution's services and activities Additionally, specific examples of critical or important functions include the following: (p.28-29 "4. Critical or important functions" 34, 35) ➢ When the institution relies on TPSPs for internal control functions ➢ When the institution relies on TPSPs for key business areas or important functional activities ➢ When the institution utilizes TPSPs, within the scope requiring authorization, for banking business activities, payment services, or the issuance of Asset Referenced Tokens (ART) as defined in Article 3(1)(6) of Regulation (EU) 2023/1114 (ART is defined as a type of crypto asset intended to maintain stable value by referencing other values or rights, or a combination thereof, including multiple official currencies, but excluding electronic money tokens) Furthermore, when evaluating whether an institutional function qualifies as a critical or important function, at a minimum, the following elements should be considered: (p.28-29 "4. Critical or important functions", 36, 37) ➢ Whether the third party arrangement is directly related to the provision of banking, investment, payment services, etc., subject to authorization ➢ The potential impact of interruption of functions provided by the TPSP, or failure to continuously provide services at the agreed service level, on the following: - Short-term and long-term financial resilience and viability (including assets, capital, costs, funding, liquidity, profit and loss) - Business continuity and operational resilience - Operational risk and legal risk - Reputational risk

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	- Other related risks (including credit risk, market risk, ESG risk, AML/CFT risk, etc.) - Where applicable, recovery and resolution planning, resolvability, and continuity of operations during early intervention, recovery, or resolution **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** In this guideline, concentration risk of TPSPs in financial institutions is defined as follows: (p.22 "Definitions") ➢ The risk that, due to dependence on one or more related TPSPs, the financial institution may be unable to provide critical functions, suffer other significant disadvantages, or threaten the stability of the financial system in the event that such provider(s) become unavailable, experience failures, or other deficiencies occur. The guideline stipulates that, when there is concentration in a financial institution's arrangements with third parties—especially those concerning critical or important functions—the competent authority shall monitor such concentration, as failure of those services could hinder the provision of financial services by multiple institutions. If multiple financial institutions are dependent on a small number of TPSPs and sector-level concentration risk is identified, the competent authority is required to take the following actions: (p.58 "Title V – Guidelines on third-party risks arrangements addressed to competent authorities" 128, 129) ➢ The competent authority must monitor the trend of such concentration risk and assess its potential impact on other financial institutions and the stability of the financial system. Furthermore, if, during the course of this evaluation, new potentially critical functions are identified, the competent authority must notify the resolution authority as necessary. ➢ If it is determined that a financial institution no longer maintains a robust governance framework or is not complying with regulatory requirements, the competent authority should take appropriate measures, which may include restricting or limiting the scope of functions performed by TPSPs, or requiring the termination of third-party arrangements, as necessary.

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	➢ In particular, taking into account the need for financial institutions to continue their operations, if regulatory supervision or enforcement cannot be ensured by other means, the competent authority may also require the termination or temporary suspension of contracts. In addition to the above concentration risk management by competent authorities, the guideline also requires financial institutions to consider the following perspectives on concentration risk as a minimum in their risk assessment when entering into arrangements with third parties: (p.42 "11.2 Risk assessment of third-party arrangement" 76) ➢ Entity-level concentration risk: (i) Concentration of operations with key TPSPs for which alternative providers are not readily available (ii) Multiple third-party arrangements with a single or closely connected TPSP
(3) Ongoing Monitoring of Third Parties	This guideline requires financial institutions, when conducting pre-contract risk assessments and ongoing monitoring of the performance of TPSPs for third-party arrangements, to consider at least the following common requirements: (p.43 "11.2 Risk assessment of third-party arrangements") ➢ A thorough risk-based analysis of the functions for which a contract with a TPSP is being considered or which are already being provided to the financial institution by a TPSP: - Assessment of whether the function qualifies as a critical or important function - In particular, addressing potential risks such as operational risk, reputational risk, and management constraints arising from the country in which the function is provided ➢ The impact from the TPSP's location (inside or outside the EU) ➢ Consideration of the political stability and security environment of the relevant jurisdiction. This includes: i. Current laws, including data protection laws compliant with the EU General Data Protection Regulation (GDPR) ii. Applicable law enforcement provisions iii. Insolvency regulations applicable if the TPSP fails, and, in particular, constraints that may arise in the urgent recovery of financial institution

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	functions ➢ Confirmation of whether the TPSP is a subsidiary or parent company of the financial institution, a consolidated entity for accounting purposes, or a member of an institutional protection scheme - If applicable, consideration of the financial institution's control or influence over the TPSP (As a principle, this guideline indicates that, even when a financial institution concludes arrangements with intra-group TPSPs, the same regulatory framework as for other third-party arrangements applies, and the risk is not necessarily lower. Furthermore, if important or critical functions are provided or supported by intra-group TPSPs, the financial institution must objectively select the contractor, ensure that the terms of the arrangement are set according to the arm's length rule, and clearly address any potential conflicts of interest. Accordingly, all relevant risks must be clearly identified, and the arrangement must detail risk mitigation measures and controls to ensure compliance with applicable regulations (p.24 "Governance of third-party arrangements" 23, 24)). Based on the above, for ongoing monitoring of TPSPs, financial institutions must continuously monitor TPSP performance for all third-party arrangements on a risk-based basis, with particular focus on ensuring the availability, integrity, and confidentiality of data for delegations of critical functions. It is also required that, if there are significant changes in risk or the terms of delegation, the assessment should be reviewed. The following measures are required: (p.53-54 "13. Monitoring" 111, 112, 113, 114, 115) ➢ Obtain appropriate reports from the TPSP ➢ Evaluate TPSP performance using KPIs, KCIs (Key Control Indicators), service delivery reports, self-certification, and independent reviews ➢ Review other relevant information received from the TPSP, such as reports on business continuity measures and testing Furthermore, the results of TPSP risk assessments must be updated regularly, and any risks identified in third-party arrangements for critical or important functions must be reported to management on a regular basis (p.53 "13. Monitoring" 116). When conducting TPSP risk assessments, financial

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	institutions are required to include consideration of the following aspects: (p.41 "11.2 Risk assessment and third-party arrangements" 73, 74) ➢ The potential impact of the third-party arrangement on the institution's ability to: (i) Identify, monitor, and manage all risks (ii) Comply with all legal and regulatory requirements (iii) Conduct appropriate audits of the functions provided by the TPSP ➢ The potential impact on services provided to customers ➢ The scale and complexity of the affected business area ➢ The possibility that the proposed third-party arrangement may be expanded without amending or revising the underlying contract (from a legal risk perspective) ➢ Where necessary or desirable, the ability to transfer the third-party arrangement to another TPSP (both contractually and operationally), as well as the associated risks, obstacles to business continuity, costs, and required time (substitutability) ➢ Where necessary or desirable, the ability to insource the functions provided by the TPSP into the financial institution ➢ The protection of data, and the potential impact on the financial institution of breaches of confidentiality or failure to ensure data availability and integrity (including compliance with GDPR)
(4) Securing Audit Rights and Methods for Third Parties	This guideline stipulates that audit rights, inspection rights, and access rights to information, accounts, and premises for financial institutions and competent authorities (including resolution authorities) over TPSPs must be secured in all written third-party arrangements. When concluding such arrangements, financial institutions should ensure that at a minimum, the following elements are included in the contract: (p.45 "Contractual phase" 85, 86 and p.49 "12.2 Access, information and audit rights" 99) ➢ A clear and complete description of all functions provided by the TPSP ➢ Whether the outsourcing of critical or important functions, or significant parts thereof, is permitted ➢ The location (region or country) where the TPSP provides the functions and the conditions to be fulfilled (including an obligation to notify if the TPSP plans to change the service provision location)

Research Items	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk
	➢ The location where data related to the arrangement is processed or stored ➢ The contract start date and, where applicable, the end date ➢ The applicable laws and regulations for the contract ➢ The financial obligations of the parties ➢ Availability, authenticity, integrity, and confidentiality of data protection (including personal data) ➢ Provisions for access to, retrieval, and return of data owned by the financial institution in the event of TPSP insolvency, failure, suspension of service, or contract termination ➢ Details of service levels, and the methods for their update and revision ➢ The financial institution's right to continuously monitor the performance of the TPSP ➢ The obligation for the TPSP to fully cooperate with the competent authorities of the financial institution (including the resolution authority) and any third parties designated by the competent authority ➢ The termination of the third-party arrangement, and the notification period thereof ➢ For arrangements involving the provision of critical or important functions by the TPSP, full access to all relevant premises (such as headquarters and operation centers), as well as to relevant equipment, systems, networks, data, and information used in the provision of functions (including relevant financial information, personnel, and the TPSP's external auditors), and the right to obtain copies of relevant information and documents ➢ For arrangements involving the provision of critical or important functions by the TPSP, unrestricted rights to relevant inspections and audits (including on-site inspections) Even if the functions entrusted to the TPSP are not critical at the time, financial institutions should consider, based on a risk-based approach in accordance with the principle of proportionality, including the above access and audit rights in contracts, taking into account the nature of the function, associated operational and reputational risks, scalability, potential impact on business continuity, and contract duration, in light of the possibility that such functions may become critical or important over time. Furthermore, financial institutions are required to ensure that their arrangements and other contracts do not prevent or restrict the effective exercise of access or audit rights by the financial institution, competent authorities, or any third party appointed by the financial institution or competent authorities.

(8) FRB, FDIC, OCC

Premise:

The "Interagency Guidance on Third-Party Relationships: Risk Management" is a joint guidance on risk management for third-party relationships, issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (collectively, the "agencies") to all banking organizations supervised by the agencies.

The agencies have issued this guidance to promote consistency in supervisory approaches, and it replaces each agency's previous general guidance on risk management for third-party relationships. The purpose of this guideline is to support banking organizations in identifying and managing risks in their relationships with third parties and to help ensure compliance with applicable laws and regulations; it does not impose new requirements on banking organizations.

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】** This guideline applies to all business arrangements between banking organizations and other entities, regardless of whether a contract exists, and states that a third-party relationship may be established even if there is no contract or compensation. Specific examples of third-party relationships include the following. It is also noted that some banking organizations may form third-party relationships in new or innovative structures or forms, such as relationships with fintech companies. (p.1-2 "A. OVERVIEW") ➢ Outsourcing services ➢ Use of independent consultants ➢ Referral agreements ➢ Merchant payment processing services ➢ Services provided by affiliates or subsidiaries ➢ Joint ventures **【Third Parties and Nth Parties Subject to Management】** Not all third-party relationships present the same level of risk, and the same level or method of audit or risk management is not required for all relationships. Banking organizations should analyze the risks associated with each third-party relationship and adjust risk management practices according to their own size, operational complexity, risk profile, and the nature of the relationship. More

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	comprehensive and rigorous management is required for higher-risk activities, particularly relationships with third parties supporting critical activities. (p.2-3 "B. RISK MANAGEMENT") As considerations during the contract negotiation phase, it is stipulated that, in contracts with overseas third parties, it is important to consider governing law and jurisdiction clauses for dispute resolution. When using overseas third parties or when the contract includes governing law clauses from jurisdictions outside the United States, it is important to understand that such contracts may be subject to the laws of those jurisdictions and interpretation by foreign courts. (p.16 "3. Contract Negotiation") Additionally, in each stage of the risk management lifecycle, the use of subcontractors is explicitly included as a subject for evaluation and management. (p.4, 10, 16 "C. THIRD-PARTY RELATIONSHIP LIFE CYCLE") ➢ In the planning stage before initiating a third-party relationship, one of the considerations is to examine the nature of the business arrangement (transaction volume, use of subcontractors, required technology, customer interactions, use of overseas third parties, etc.). For critical activities, such plans may be submitted to and approved by the board of directors of the banking organization. (p.4 "1. Planning") ➢ In the due diligence stage, among 14 considerations, "dependency on subcontractors" is included. This involves evaluating the degree of dependency, the ability to identify, manage, and mitigate risks related to the third party's subcontractors, and assessing how the third party selects and audits subcontractors, and how it ensures that subcontractors have effective controls. (p.10 "2. Due Diligence and Third-Party Selection") ➢ In the contract negotiation stage, among 17 considerations, "subcontracting" is included. It is important to stipulate in the contract when and how the third party should notify the banking organization if it uses or plans to use subcontractors, and whether the banking organization prohibits the use of specific subcontractors. It is also important to consider whether to prohibit the third party from assigning, transferring, or subcontracting its obligations to other organizations without the banking organization's consent. If subcontracting is essential for services to the banking organization, it is also important to consider more detailed

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	contractual obligations, such as requiring reports on subcontractor performance indicators, regular audit results, and compliance status. (p.16 "3. Contract Negotiation") **【Criteria for Determining Criticality】** Banking organizations are required to conduct more comprehensive and rigorous audits and management for relationships with third parties supporting higher-risk activities, particularly critical activities. Characteristics of critical activities include: ➢ Activities that could expose the banking organization to significant risk if the third party does not perform as expected ➢ Activities that have a significant impact on customers ➢ Activities that have a significant impact on the financial condition or business operations of the banking organization It is also state that the responsibility of each banking organization to identify which activities are critical and which third-party relationships support those activities. What is critical for one banking organization may not be critical for another. Some banking organizations may assign an importance or risk level to each third-party relationship, while others may identify critical activities and the third parties that support them. (p.2-3 "B. RISK MANAGEMENT") **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** This guideline does not contain a direct description of the definition or management methods for "concentration risk." However, as part of the considerations in the due diligence stage of risk management, it stipulates the need to assess the degree of operational dependence on third parties and on subcontractors when evaluating third-party operational resilience initiatives (p.9-10 "2. Due Diligence and Third-Party Selection"): ➢ "i. Operational Resilience": Banking organizations are required to assess the operational resilience capabilities of third parties, including the results of their business continuity testing, performance during actual disruptions, redundancy in communications with third parties, and preparedness for

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	known and emerging threats and vulnerabilities such as widespread natural disasters, pandemics, DDoS attacks, and other intentional or unintentional events. Among other considerations in this context, the guideline specifies checking the level of dependence on a single third party. ➢ "I. Dependence on Subcontractors": This includes evaluating the extent to which services depend on subcontractors, the ability to identify, manage, and mitigate risks related to third-party subcontractors, and assessing how third parties select and audit subcontractors and ensure that subcontractors implement effective controls. Additionally, in the context of governance documentation and reporting, the guideline requests that the level of dependence on a single third party be reported to the board of directors. As an example of documentation and reporting within the banking organization, it lists "regular reports to the board of directors (including, as necessary, the level of dependence on a single provider across multiple business lines)." (p.22 "3. Documentation and Reporting")
(3) Ongoing Monitoring of Third Parties	For effective third-party risk management, ongoing monitoring of third-party relationships and the activities performed by third parties is required, adapted to the risk level and complexity of those activities. Ongoing monitoring should be conducted regularly or continuously, and, in particular, for relationships with third parties supporting critical activities of the banking organization, more comprehensive and frequent monitoring is considered appropriate. Since the level and nature of risk may change, banking organizations need to adjust their monitoring practices as necessary, including the frequency of monitoring and the types of information used. General monitoring activities include the following: (1) Review of reports on the performance and effectiveness of controls of third parties (2) Discussion of performance and operational issues through regular visits and meetings with third-party personnel (3) Periodic testing of the banking organization's controls to manage risks arising from third-party relationships (especially when supporting high-risk activities, including critical activities) Depending on the risk, banking organizations may also directly test the controls

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	of third parties. Furthermore, for efficiency and to utilize specialized expertise, banking organizations may use external resources, refer to conformity assessments or certifications, or collaborate in conducting ongoing monitoring. (p.17-19 "C. THIRD-PARTY RELATIONSHIP LIFE CYCLE, 4. Ongoing Monitoring") As a prerequisite for ongoing monitoring of third parties, the contract phase also addresses the need for banking organizations to secure audit rights over third parties. It is common for contracts to stipulate the banking organization's audit rights and corrective actions in the event of issues, and, generally, contracts specify that periodic and independent audits of the third party and relevant subcontractors should be conducted according to the risk and complexity involved. (p.13 "3. Contract Negotiation")
(4) Securing Audit Rights and Methods for Third Parties	Agencies review the risk management of third-party relationships at supervised banking organizations, assess the risks and effectiveness of risk management and determine whether operations are conducted in a safe and sound manner and in compliance with relevant laws and regulations. The scope of supervision and review varies depending on the degree and complexity of the risks related to the activities of the banking organization and its third-party relationships. When reviewing third-party risk management processes, the following activities are typically conducted: ➢ Assessing the ability of the banking organization's management to oversee third party relationships ➢ Evaluating the impact of third party relationships on the banking organization's risk profile and on important financial and operational matters, including compliance with relevant laws and regulations ➢ Conducting transaction testing or reviewing the results of such testing regarding the activities performed by third parties, and assessing compliance with relevant laws and regulations ➢ As necessary, discussing and pointing out significant risks or deficiencies in the banking organization's risk management processes with management or the board of directors ➢ Reviewing whether the banking organization has developed appropriate and sustainable corrective actions for deficiencies identified in audits of third parties, especially those involved in critical activities ➢ Considering audit findings when determining evaluations for various items in the evaluation system, and clearly stating significant risks and deficiencies in audit reports

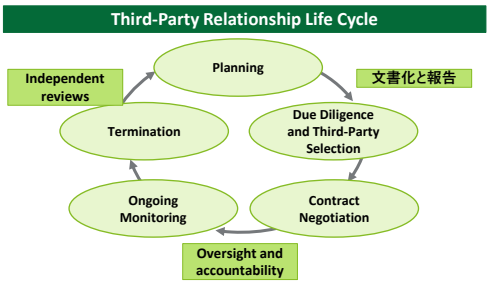
Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	Depending on the situation, supervisory agencies may, under legal authority and on behalf of the banking organization, investigate the functions or activities performed by third parties. Such investigations confirm whether third parties conduct operations in a safe and sound manner and comply with relevant laws and regulations aimed at customer protection and the fair provision of financial services. Additionally, supervisory agencies may take corrective or enforcement actions if the banking organization or third party violates laws or regulations, or if operations compromise confidentiality or soundness. (p.23 "E. SUPERVISORY REVIEWS OF THIRD-PARTY RELATIONSHIPS") For banking organizations, it is important to clearly stipulate in contract provisions the obligation of third parties to maintain and provide timely, accurate, and comprehensive information for the purpose of risk and performance monitoring and compliance with relevant laws and regulations. Examples of such provisions that banking organizations are required to include are as follows: (p.12 "c. Responsibilities for Providing, Receiving, and Retaining Information") ➢ Ensuring the banking organization has appropriate and timely access to its own data ➢ Allowing the bank to access and use third-party data and related materials ➢ Allowing these data and evidentiary documents to be shared with regulators in a timely manner as part of the audit process ➢ Whether the third party may resell, transfer, or grant access to customer data, the banking organization's data, metadata, or systems to other companies ➢ Obligation to notify the banking organization in the event of compliance violations, law enforcement actions, regulatory proceedings, or other events that pose significant risks to the banking organization or its customers ➢ Obligation to notify the banking organization of major strategic or operational changes that may affect involved activities, such as mergers, acquisitions, business sales, use of subcontractors, or changes in key personnel ➢ Clarification of the types and frequency of reports to be received from the third party (e.g., operational reports, financial reports, security reports, control evaluation results)

Research Items	Interagency Guidance on Third-Party Relationships: Risk Management
	It is also important to specify in contracts that the activities performed by the third party for the banking organization are subject to regulatory supervision, and that appropriate retention and access to relevant documents and materials are required. (p.17 “q. Regulatory Supervision”) The board of directors of the banking organization has ultimate responsibility for third-party risk management and for holding management accountable. The board provides clear guidance on acceptable third-party risk, approves policies, and ensures that necessary procedures and practices are established. Banking organization management is responsible for formulating and implementing third-party risk management policies, procedures, and practices according to the risk appetite and the risks and complexities of third-party relationships. (p.20 “1. Oversight and Accountability”)

(9) FRB, FDIC, OCC

Premise:

This guidance is developed for community banks based on the "Interagency Guidance on Third-Party Relationships: Risk Management" (hereafter, TPRM Guidance).

Research Items	Third-Party Risk Management A Guide for Community Banks
Overview	This guideline provides community banks with considerations, sources of information, and examples for each stage of the third party risk management lifecycle (see Figure 1) when implementing third party risk management practices. It also cites and explains the management practices described in the TPRM Guidance for each stage of the risk management lifecycle. Figure 1:  The guideline emphasizes the following key points for managing third parties: ✓ Utilizing third parties does not diminish or exempt the bank’s

Research Items	Third-Party Risk Management A Guide for Community Banks
	responsibility to conduct its operations in a safe and sound manner and to comply with legal and regulatory requirements, just as if the bank were performing the services or activities itself. ✓ Banks must manage third party relationships according to the associated level of risk. ✓ Regular risk assessments allow for appropriate management tailored to the size, complexity, and risk profile of each third party. ✓ It is important to involve bank staff with the necessary knowledge and skills at each stage of the risk management lifecycle. ✓ An essential first step is to identify third parties that support high risk activities, including critical activities. When determining whether an activity is high risk, banks should assess whether the third party has access to sensitive information, including customer data, processes transactions, or provides critical technology or operational services. 【TPRM Guidance】 As part of sound risk management, banks should conduct rigorous audits and risk management for relationships with third parties that support high risk activities, including critical activities. High risk or critical activities may include: ・ Situations where a third party fails to meet the bank's requirements and exposes the bank to significant risk ・ Activities that have a significant impact on customers ・ Activities that have a significant impact on the bank's financial condition or business operations
Planning	Community banks need to develop plans, conduct risk assessments, identify potential risks in third party relationships, and evaluate the risk management resources and scope of practices necessary for effective management. 【TPRM Guidance】 As part of sound risk management, banks should develop effective plans and assess how risks will be managed before entering into relationships with third parties. 【Considerations】 ✓ What risk management and governance practices are necessary to

Research Items	Third-Party Risk Management A Guide for Community Banks
	manage and mitigate potential risks? ✓ Does the third party have physical or system access to the bank's facilities, systems, and records, and are they involved in record management processes? ✓ How does the third party access, process, and protect customer information from an information security perspective? ✓ How will the third party's technology be integrated with the bank's existing systems and infrastructure? What changes are required on the bank's side to ensure compatibility, and what are the associated risks and costs? Do staff have the necessary skills to manage risks associated with technology integration (and if not, how will the bank address integration)? ✓ Has consideration been given to the termination of the activity or the transition to another third party or in-house operations? etc. 【Sources of Information】 ✓ The bank's policies, processes, and controls for assessing the impact of initiating and operating new relationships. ✓ The existing third party inventory to evaluate whether current relationships can support new activities. ✓ Insights from subject matter experts within the bank, including specialists in information technology, legal, and compliance risks. ✓ Assessment of how easily the bank's technology infrastructure and staff can integrate with the third party to support new activities. etc.
Due Diligence and Third Party Selection	Due diligence is the process of evaluating whether a third party can perform expected activities in a safe and sound manner, has the capability and reliability to help the bank achieve its strategic and financial objectives, and complies with legal and regulatory requirements. If the bank cannot obtain the information it desires from the third party, it must consider obtaining alternative information or implementing additional controls and monitoring. 【TPRM Guidance】

Research Items	Third-Party Risk Management A Guide for Community Banks
	✓ Due diligence serves as an indicator of whether the third party will contribute to achieving the bank's strategic and financial objectives. It is also a necessary process for the bank to evaluate whether it can appropriately identify, monitor, and manage risks associated with a particular third party. 【Considerations】 ✓ What resources and expertise do the third party have to support its activities? ✓ Do the third party's policies, processes, and internal controls support the provision of services that meet the bank's expectations and standards? ✓ Is the third party's information security program aligned with the bank's requirements and expectations for the confidentiality, integrity, and availability of information? ✓ Does the third party demonstrate the ability to effectively respond to and recover from both internal and external operational incidents or disruptions? ✓ Does the third party rely on subcontractors, and could that reliance pose risks to the bank? ✓ Does the third party use technologies that could introduce additional risks? etc. 【Sources of Information】 ✓ Licenses and other legal authorities required by the third party to perform its activities ✓ Review of the third party's strategic plans and disclosures to evaluate whether business strategies or contracts with other entities could introduce or increase risks ✓ Assessment of the third party's staffing and qualifications to determine whether they can fulfill obligations to the bank ✓ SOC reports, independent assessments, and industry certifications to evaluate the third party's operational risk management and internal controls ✓ Audit reports to assess the third party's risk management and internal controls ✓ Recommendations and feedback from other banks or customers currently using the third-party services

Research Items	Third-Party Risk Management A Guide for Community Banks
	etc.
Contract Negotiation	Before entering into a contract with a third party, the bank should clarify the expectations and obligations of both parties, consider contract provisions that align with its business objectives and risk management policies and procedures, and negotiate with the third party to ensure effective risk management. If the bank has limited bargaining power, it is important to understand the resulting constraints and associated risks, including determining whether the contract increases risk and whether any residual risk is acceptable. 【TPRM Guidance】 ✓ Banks should negotiate contract provisions that promote effective risk management and clearly state the expectations and obligations of both the bank and the third party. In difficult contract negotiations, including situations where the bank's bargaining power is limited, it is important to fully understand the constraints and associated risks. 【Considerations】 ✓ To what extent does the contract clearly define responsibilities and all aspects of the relationship between the parties (costs, reimbursement, other liabilities, etc.)? ✓ What provisions should the bank include regarding grounds for contract termination (e.g., default or force majeure), business continuity planning, and related costs or fees? ✓ Does the contract ensure the bank can obtain, in a timely manner, the information needed for ongoing monitoring, to demonstrate compliance with laws and regulations, and to respond to supervisory requests (e.g., application and loan data, account opening/customer information, audit reports, suspicious activity monitoring information, reports for identifying safety, soundness, and compliance issues)? ✓ What are the governance and escalation arrangements regarding the third party's performance, security measures, and benchmarks? ✓ Does the contract set appropriate restrictions and regulations on the access, use, and storage of information, technology, and intellectual property, including customer data, by the third party in connection with

Research Items	Third-Party Risk Management A Guide for Community Banks
	its services? ✓ How and when does the third party notify the bank in the event of service degradation or interruptions, and how does it support the bank's business continuity? etc. 【Sources of Information】 ✓ Results of the bank's risk assessment and due diligence to determine which provisions should be included in the contract ✓ Service level agreements (SLAs) provided by the third party for setting performance and security standards ✓ Self-assessments of business needs and customer service objectives by each department (to determine business and security standards to be included in the contract) ✓ Contract provisions granting the bank access to third-party audit reports, test results, and self-assessment reports for ongoing monitoring ✓ Opinions from legal, compliance, and other stakeholders to advise management on contract provisions that appropriately protect the bank's interests. etc.
Ongoing Monitoring	Confirm the quality and continuity of the third party's management structure and ability to fulfill contractual obligations and escalate any significant issues or concerns. 【TPRM Guidance】 ✓ When conducting ongoing monitoring, banks may enhance efficiency by utilizing external resources and referencing conformity assessments or certifications. (1) Confirm the quality and sustainability of the third party's controls and its ability to fulfill contractual obligations. (2) Escalate significant issues or concerns (such as serious or repeated audit findings, deterioration of financial condition, security breaches, data loss, service interruptions, compliance violations, or other indicators of increased risk).

Research Items	Third-Party Risk Management A Guide for Community Banks
	(3) Respond appropriately when significant issues or concerns are identified. 【Considerations】 ✓ Is the third party fulfilling its contractual obligations? ✓ Are there changes in the third party's financial condition, such as a decrease in sales or increase in debt? ✓ Is the third party complying with applicable laws, regulations, and service level agreements (SLAs)? ✓ Do audit or test results indicate that the third party is managing risks appropriately and effectively meeting contractual and regulatory requirements? ✓ Do the third party's business continuity and disaster recovery plans and practices demonstrate the ability to respond to and recover from service interruptions or disruptions? ✓ Does the third party maintain systems within the bank's availability requirements, such as latency, bandwidth, and uptime? ✓ Is the third party properly maintaining the confidentiality, availability, and integrity of customer data and the bank's systems, information, and data? ✓ For third parties that interact with customers or access customer data, are they responding appropriately to the bank's requests for records or information? 【Sources of Information】 ✓ Service level agreements (SLAs) and standards for assessing whether the third party's performance and current provisions continue to address risks and meet the bank's expectations ✓ Audit reports and other financial information to assess whether the third party's financial condition is sound and contractual requirements are met ✓ Audit reports to confirm the third party's overall compliance with laws and regulations ✓ Results of contingency tests by the bank and the third party to assess response and recovery capability during service disruptions ✓ Reviews and tests of the effectiveness of controls, including SOC reports and self-assessments based on industry standards, to evaluate the health

Research Items	Third-Party Risk Management A Guide for Community Banks
	of the third party's control environment ✓ Information security test results to assess the ability to maintain confidentiality, availability, and integrity of customer data and systems/information/data ✓ Customer complaints to evaluate the number, nature, and the third party's promptness and appropriateness of responses ✓ Staffing plans, succession plans, and organizational charts of the third party to identify changes in key personnel or dual roles with other organizations that may affect contract fulfillment ✓ Ongoing educational and training materials for third-party and bank staff ✓ Internal reports for reviewing changes to the bank's risk assessment or risk management processes. etc.
Contract Termination	It is common for banks to consider the potential impact of contract termination during the "planning" stage of the lifecycle. This advance consideration helps mitigate costs and operational disruptions associated with termination and is especially effective for high-risk activities such as critical operations. 【TPRM Guidance】 ✓ Banks may terminate relationships with third parties for various reasons, such as contract expiration or breach, non-compliance with applicable laws or regulations, or transition to alternative providers or in-house operations. In such cases, it is important to end the relationship efficiently. 【Considerations】 ✓ How will contract termination affect the bank's operations and compliance with applicable laws and regulations? Could it impact high-risk activities? ✓ Are there alternative third parties to which the bank can transition, or can the bank perform the activities internally? ✓ If outsourced activities are brought in-house, how prepared are the bank's staff, systems, and control environment? ✓ How will intellectual property be handled between the bank and the third party?

Research Items	Third-Party Risk Management A Guide for Community Banks
	✓ To what extent has the third party been granted access to the bank's systems and information, and how and when will that access be revoked? ✓ If the third party has accessed bank or customer data, how and when will the bank confirm that data has been returned or deleted? ✓ Can the bank access data necessary to meet AML/CFT requirements and other record-keeping obligations? ✓ How will the bank manage risks associated with termination or transition, including impacts on customers? ✓ What additional controls or processes will the bank implement during the transition period? etc. 【Sources of Information】 ✓ Inventories of bank and customer data held by third parties to support risk management of data retention/deletion, system connections, access controls, and other management concerns ✓ Evaluations of the bank's systems, processes, and personnel resources to determine the ability, resources, and time required for transition to another third party or to in-house operations ✓ Third party inventories to assess whether existing relationships can be transitioned to other third parties. etc.
Governance	Community banks need to consider the following items throughout the third party risk management lifecycle. 【TPRM Guidance: Oversight and Accountability】 ✓ The bank's board of directors has ultimate responsibility for overseeing third-party risk management, approving appropriate policies, and ensuring that proper practices are established. Bank management is responsible for developing and implementing third-party risk management policies, procedures, and practices according to the bank's risk appetite and the risks and complexities of third-party relationships. 【TPRM Guidance: Independent Review】 ✓ Banks should regularly conduct independent reviews to evaluate the

Research Items	Third-Party Risk Management A Guide for Community Banks
	adequacy of their third-party risk management processes. Banks can use the results of these reviews to determine how to revise and adjust their policies, reporting, resources, expertise, and management structure for third-party risk management. 【TPRM Guidance: Documentation and Reporting】 ✓ Documentation and reporting are important elements that support those conducting management both inside and outside the bank, but the content and methods will differ among banks depending on the risk and complexity of each third-party relationship. 【Considerations】 ✓ How do the bank's policies and procedures promote governance over third-party risk management? ✓ How do documentation and reporting support the board of directors in consistently managing third-party risk? ✓ Does the bank's governance structure and internal control environment effectively promote compliance with its policies, procedures, and applicable laws and regulations? ✓ Are the resources (including staff levels and expertise) needed to manage third-party risk accurately assessed? ✓ Are all third-party relationships documented, with an up-to-date management register maintained that clearly identifies relationships involving high-risk activities, including critical activities? etc. 【Sources of Information】 ✓ Applicable policies and procedures for evaluating whether risks arising from third-party relationships are being appropriately addressed ✓ The bank's contingency test plans to understand how business continuity is maintained during disruptions ✓ Audit reports to assess the bank's risk management and internal controls. etc.

(10) European Parliament, European Council

Premise:

This regulation, established by the European Parliament and the European Council, provides prudential requirements for insurance and reinsurance companies within the EU. The primary objective of the regulation is to ensure that policyholders and beneficiaries are adequately protected. It sets out various requirements applicable to insurance and reinsurance companies operating within the EU.

The regulation adopts a risk-based approach, enabling the overall solvency of insurance and reinsurance companies to be assessed through both quantitative and qualitative methods.

Research Items	Solvency II Directive（Article 38, 49）
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】&【Third Parties and Nth Parties Subject to Management】&【Criteria for Determining Criticality】** Entities that provide services to insurance companies or reinsurance companies are referred to as "service providers." Outsourcing is defined as follows: (Article 13) ➢ Outsourcing means any form of arrangement between an insurance company or a reinsurance company and a service provider (regardless of whether the service provider is a supervised entity), whereby the service provider, either directly or through subcontracting, performs a process, service, or activity that would otherwise be undertaken by the insurance company or reinsurance company itself. Although there is no direct description of the method of classification of service providers, the service providers to be managed, the concept of Nth providers, or the criteria for determining criticality, it is stipulated that insurance companies and reinsurance companies remain fully responsible for fulfilling all obligations under this directive, even when outsourcing their functions or activities, indicating the necessity to manage service providers. ("Article number: 49, 1") Furthermore, the outsourcing of important or critical operational functions or activities must not be conducted in a manner that leads to any of the following: ("Article number: 49, 2") (a) Materially impairing the quality of the company's governance structure (b) Unjustifiably increasing operational risk (c) Impairing the ability of supervisory authorities to monitor the company's compliance with its obligations

Research Items	Solvency II Directive（Article 38, 49）
	(d) Disrupting the continuous and satisfactory service to policyholders **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A
(2) Concentration Risk of Third Parties	N/A
(3) Ongoing Monitoring of Third Parties	N/A
(4) Securing Audit Rights and Methods for Third Parties	When insurance companies and reinsurance companies outsource functions or activities, it is stipulated that measures must be taken to satisfy the following: conditions (“Article number: 38, 1”) (a) The service provider must cooperate with the supervisory authorities of the insurance company and reinsurance company in relation to the outsourced functions or activities. (b) The insurance company and reinsurance company, their auditors, and supervisory authorities must be able to effectively access data related to the outsourced functions or activities. (c) The supervisory authorities must be able to effectively enter the premises of the service provider and exercise their right of entry. Additionally, it is stipulated that the Member State where the service provider is located must permit the supervisory authorities of the insurance company and reinsurance company to conduct on-site investigations at the service provider’s premises, either directly or through persons appointed by them. (“Article number: 38, 2”)

(11) IAIS

Premise:

This guideline is an application paper related to the Insurance Core Principles (ICPs) established by the IAIS. Application papers are documents created by the IAIS to provide examples and case studies in cases where uniform interpretation or application of principles and standards on specific supervisory topics is difficult. This paper serves as supplementary material for

supervisory authorities and insurance companies, presenting practical methods for applying operational resilience based on the principle of proportionality, as well as recommendations, examples, and tools. It indicates that TPRM (Third Party Risk Management) is included as an element of operational resilience for insurance companies, and is based on the premise that the failure of critical services can have a significant impact on the continuity of insurance companies and their fulfillment of regulatory obligations. The paper refers to the FSB's TPRM toolkit for its approach to identifying critical services.

Research Items	Draft Application Paper on Operational resilience objectives and toolkit
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】&【Third Parties and Nth Parties Subject to Management】&【Criteria for Determining Criticality】** This guideline stipulates that, from the perspective of operational resilience of insurance companies, relationships with third-party service providers, group companies, and Nth parties should be managed effectively. The respective definitions and concepts refer to the FSB toolkit and DORA. (p.30 "Objective 2.8", p.31 "Box 15: Outsourcing and third-party risk management") **【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A (Refers to the FSB toolkit and DORA)
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** This guideline, from the perspective of operational resilience for insurance companies, addresses systemic concentration risk arising from increased dependence by insurance companies on a small number of large, critical third-party service providers. For the management of such systemic concentration risk related to third-party service providers, the guideline highlights the necessity of cooperation by authorities and, specifically, the need for direct supervision by authorities (referring to DORA). (p.31 "Objective 2.8, 58", "Box 15: Outsourcing and third-party risk management", p.33 "Objective 3.2")
(3) Ongoing Monitoring of Third Parties	This guideline, with reference to the FSB toolkit and other sources, identifies the implementation of the following processes as part of third-party risk management initiatives: ・ Planning ・ Due diligence and selection ・ Contracting

Research Items	Draft Application Paper on Operational resilience objectives and toolkit
	・ Ongoing management and audit ・ Contract termination Additionally, from the perspective of operational resilience, the guideline outlines expectations from authorities to insurance companies. These include organizing the conditions for identifying critical third-party service providers based on the principle of proportionality, and cooperation between authorities and insurance companies (such as regular and ad hoc information sharing, and incorporating reviews of information received by insurance companies from service providers—e.g., audit results, certification information, training results—into the process for each specific theme like TPRM). Specific details are referenced in DORA and other sources. (p.31 "Objective 2.8" 56, 57, "Box 15: Outsourcing and third-party risk management")
(4) Securing Audit Rights and Methods for Third Parties	This guideline, with reference to the FSB toolkit and other sources, states that audit rights for third-party service providers should be secured by including contractual clauses. Although the specific contractual requirements are referenced in DORA, elements to be included are audit rights over third-party service providers and access to information related to the services provided. (p.31 "Objective 2.8, 53", "Box 15: Outsourcing and third-party risk management")

(12) NAIC

Premise:

The "Insurance Data Security Model Law" is a model law adopted in 2017 by the National Association of Insurance Commissioners (NAIC). The U.S. Department of the Treasury requested that each state promptly implement this model law within five years of its adoption. The purpose of this law is to establish data security standards for regulatory authorities and insurance companies in order to mitigate the potential harm caused by data breaches. It applies to insurance companies, insurance agencies, and other entities licensed by state insurance departments. The law requires insurance companies, insurance agencies, and other entities licensed by insurance departments to develop, implement, and maintain an information security program, investigate cybersecurity events, and notify the state insurance commissioner if such an event occurs.

Research Items	The NAIC Insurance Data Security Model Law
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】&【Third Parties and Nth Parties Subject to Management】** In this law, a third party service provider is defined as a person other than the licensee who, under a contract with the licensee, is permitted to manage, process, store, or otherwise have access to nonpublic information in the course of providing services to the licensee. (p.3 "Section 3. Definitions, 'P'") *"Licensee" means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State. There is no direct description of the method for classifying third parties, the third parties to be managed, or the concept of Nth parties. However, the law sets out requirements regarding the management of third party service providers, such as considering the use of third party service providers in the licensee's information security program and conducting due diligence at the time of selection to ensure appropriate measures are in place, as follows: ➢ The licensee must develop, implement, and maintain an information security program appropriate to the size and complexity of the licensee, the nature and scope of its activities including the use of third party service providers, and the sensitivity of nonpublic information used, held, managed, or controlled by the licensee. The program must be a comprehensive written document that, based on the licensee's risk assessment, includes administrative, technical, and physical safeguards to protect nonpublic information and information systems. (p.4 "Section 4. Information Security Program, A. Implementation of an Information Security Program") ➢ The licensee must identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information. This includes the security of information systems and nonpublic information that third party service providers can access or hold. (p.4 "Section 4. Information Security Program, C. Risk Assessment") ➢ (1) The licensee must conduct due diligence when selecting third-party service providers. (2) The licensee must require third party service providers to implement appropriate administrative, technical, and physical measures to protect and securely manage information systems and nonpublic information that

Research Items	The NAIC Insurance Data Security Model Law
	third party service providers can access or hold. (p.7 "Section 4. Information Security Program, F. Oversight of Third Party Service Provider Arrangements") **【Criteria for Determining Criticality】&【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** **N/A**
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** **N/A**
(3) Ongoing Monitoring of Third Parties	Although there is no direct provision regarding ongoing monitoring of third parties, the law stipulates that the licensee must monitor, evaluate, and adjust its information security program as appropriate in response to changes in its business operations, including outsourcing contracts. This suggests the need for continuous management and monitoring of third party service providers and for reflecting such management in the information security program. ➢ The licensee must, as appropriate, monitor, evaluate, and adjust the information security program in response to changes in technology, the sensitivity of nonpublic information, internal or external threats to information, and changes in its business operations, such as mergers and acquisitions, affiliations and joint ventures, outsourcing contracts, and changes to information systems. (p.7 "Section 4. Information Security Program, G. Program Adjustments")
(4) Securing Audit Rights and Methods for Third Parties	There is no direct provision regarding the securing of audit rights or specific audit methods. However, if a cybersecurity event occurs or is suspected to have occurred in a system managed by a third party service provider, the licensee is required either to conduct the following actions itself or confirm that the third party service provider has done so, and to retain records of these actions: (p.8, p.3 "Section 3. Definitions, P", "B, C") (1) Confirm whether a cybersecurity event has occurred (2) Assess the nature and scope of the cybersecurity event (3) Identify nonpublic information that may have been involved in the event (4) Implement or oversee reasonable measures to restore the security of the affected information systems in order to prevent further unauthorized acquisition, disclosure, or use of nonpublic information held, managed, or controlled by the licensee

Research Items	The NAIC Insurance Data Security Model Law
	Although the law describes the commissioner's authority to conduct investigations and examinations of licensees, it does not mention the securing of audit rights or specific audit methods for third-party service providers. (p.11 "Section 7. Power of Commissioner")

(13) NYDFS

Premise:

On October 21, 2025, the New York State Department of Financial Services (DFS) issued an Industry Letter to financial institutions under its supervision regarding risk management related to third-party service providers (TPSPs). This guidance does not impose new regulatory requirements; rather, it aims to promote compliance with Section 500.11 (Third-Party Service Provider Security Policy) of the DFS Cybersecurity Regulation (23 NYCRR Part 500), in light of the increasing use of services involving access to information systems and nonpublic information held by financial institutions. The guidance provides examples of best practices for lifecycle management of third-party service providers, including due diligence, ongoing management, contractual clauses, and contract termination. Detailed information on classification of third parties or concentration risk is not included.

Research Items	Industry Letter：Guidance on Managing Risks Related to Third Party Service Providers
(1) Classification of Third Parties and Management Policies	**【Method of Third Party Classification】&【Criteria for Determining Criticality】&【Framework for Designation of Critical Third Parties by Authorities, Including Criteria and Processes】** N/A **【Third Parties and Nth Parties Subject to Management】** The guidance indicates that financial institutions should determine which third-party service providers are subject to management based on risk, taking into consideration factors such as system access, data confidentiality, location, and the importance of the services provided to the institution's operations. (Industry Letter, "Identification, Due Diligence, and Selection")
(2) Concentration Risk of Third Parties	**【Policy and Examples of Initiatives for Managing Third Party Concentration Risk】** N/A

Research Items	Industry Letter：Guidance on Managing Risks Related to Third Party Service Providers
(3) Ongoing Monitoring of Third Parties	The guidance lists processes that insurance companies should implement for ongoing monitoring of third-party service providers, and emphasizes that these processes should be regularly reviewed, considering threat trends, security events, and regulatory changes. Insurance companies are expected to continuously manage the cybersecurity risks and countermeasures presented by third-party service providers. Examples of evaluation items include: ・ Confirmation of security attestations (such as SOC2, ISO 27001) ・ Overview and results of penetration tests ・ Policy updates and their outcomes ・ Results of security awareness training ・ Results of compliance audits In addition to these risk assessments, the guidance recommends checking the latest information on vulnerability management by third-party service providers (such as patch application status, remediation of past vulnerabilities, and escalation records for critical or unresolved risks), as well as incident response plans and business continuity plans. Insurance companies are also expected to develop and test migration plans to alternative systems/providers in the event of a failure at the service provider, and to manage the results of such tests. (Industry Letter, "Ongoing Monitoring and Oversight")
(4) Securing Audit Rights and Methods for Third Parties	The guidance states that, in addition to due diligence and audit rights over third-party service providers, minimum security standards based on risk should be stipulated in contractual clauses with service providers. Examples of items that should be included are: ・ Access Management: Establishment and implementation of policies and procedures for access management, including multi-factor authentication (MFA). ・ Data Encryption: Establishment and implementation of policies and procedures for encryption of data both in transit and at rest. ・ Cybersecurity Event Notification Obligation: Immediate notification obligation if a cybersecurity event directly affects the insurance company's information systems used by the third-party service provider or confidential information handled directly by the provider. ・ Compliance Attestation: Obligation for the third-party service provider to

Research Items	Industry Letter：Guidance on Managing Risks Related to Third Party Service Providers
	provide statements and assurances regarding compliance with relevant laws and regulations. ・ Data Storage Location and Transfer Restrictions: Disclosure of where data is stored, processed, or accessed by the third-party service provider. Where cross-border data transfer is involved, prior written approval may be required, or such transfers may be completely prohibited. Providers must also comply with local data storage regulations. ・ Subcontractors: Obligation for the third-party service provider to disclose use of subcontractors who may access or use the insurance company's information systems or confidential information, and the right for the insurance company to refuse use of such subcontractors based on the results of appropriate due diligence. ・ Data Use and Conditions upon Contract Termination: Restrictions on the use and sharing of data, and obligations to delete or transfer data upon termination of the contractual relationship with the third-party service provider, as well as the obligation to obtain proper certification that such measures have been completed. Additionally, where necessary, contract clauses regarding the use of AI and liability/compensation for security incidents should be incorporated. (Industry Letter, "Contracting")

Appendix 2: Glossary of Terms Used in This Report

Glossary Term	Definition
Ongoing Monitoring	The continuous process conducted during the contractual period with a third party to monitor and evaluate service delivery performance and any changes in the associated risk profile.
Inherent Risk Assessment	The process of evaluating the risks inherently associated with services or operations provided by a third party, such as the handling of confidential data or the nature of system connections, which serves as the starting point for risk-based management.
Financial Market Infrastructure(FMI)	Institutions that provide the foundational systems for the functioning of financial markets, such as securities exchanges and payment systems, which may, in certain cases, be excluded from the scope of TPRM.
Operational Resilience	The ability of a financial institution to maintain business continuity in the face of external or internal shocks, such as cyberattacks or natural disasters.
Due Diligence	An investigative and evaluative process conducted when selecting a third party, involving an assessment of its financial condition, service offerings, and risk management capabilities.
Business Continuity Planning(BCP)	A plan and framework designed to ensure the continuity of operations in the event of a third-party outage or other disruption, including measures and arrangements to maintain critical business functions.
Systemic Risk	A risk that has the potential to cause significant adverse effects on the entire financial sector or broader socio-economic environment. Examples include disruptions affecting a critical third party upon which multiple financial institutions depend, leading to widespread impact on the financial system.
Service Level Agreement(SLA)	The standards and commitments regarding service quality, availability, and other performance metrics agreed upon in a contract between an organization and third party.
Key Performance Indicator(KPI)	A quantifiable metric used by an organization to measure and evaluate progress toward achieving its objectives and assess performance outcomes.
Software Bill of Material(SBOM)	A machine-readable inventory that lists all software components, along with information about their dependencies.

Crypto Inventory	A document or management ledger for systematically listing and managing the cryptographic technologies (such as cryptographic algorithms, keys, certificates, and protocols) used by an organization.