Deloitte.
デロイト トーマツ

Research on Strengthening Third-Party Cybersecurity Risk Management in Financial Institutions (Provisional Translation)

Summary Report

Deloitte Tohmatsu Cyber LLC
February 27, 2026

Index

© 2026. For information, contact Deloitte Tohmatsu Group.

The research was conducted based on global guidance related to TPCRM

Research overview

Purpose of the Research	This research examines management practices (advanced cases) for third-party cybersecurity risk management (TPCRM), which is becoming increasingly important, at major banks and insurance companies (hereinafter, financial institutions (FIs) in the United States, the EU, and the United Kingdom, where such measures are considered relatively advanced. Particular attention is given to considerations for TPCRM in Japanese FIs.	
Research Approach	The primary topics of the research regarding TPCRM at FIs in the US, EU, and UK included: (1) classification of third parties and management policies, (2) risks arising from the concentration of provision of critical services and functions by specific third parties (hereafter, "concentration risk"), (3) ongoing monitoring after entering into contracts with third parties, (4) securing supervisory rights over third parties and methods, (5) exit strategies and exit plans, and (6) incident response. Initially, relevant elements were organized based on various laws, regulations, and guidelines related to TPCRM in the financial sector. Subsequently, several FIs in the US, EU, and UK were requested to respond to a questionnaire, and interviews were conducted. In addition, as a supplementary item, (7) research on the management of third parties unique to the insurance sector, such as insurance agents, brokers, and third parties associated with insurance products and services, was also conducted.	
Scope of the Research	(1) Classification of Third Parties and Management Policies	• Methods for classifying third parties and third parties subject to management • Approach to Nth parties subject to management and IT asset management for third parties and Nth parties • Criteria for determining criticality and management practices for Critical Third Parties
	(2) Concentration Risk	• Concentration risk of third parties • Methods for measuring concentration risk
	(3) Ongoing Monitoring After Contracting with Third Parties	• Monitoring through cyber threat intelligence • Sharing questionnaires within the industry
	(4) Securing Audit Rights Over Third Parties and Methods	• Contractual provisions related to cybersecurity • Audit rights and onsite assessment
	(5) Exit Strategies and Exit Plans	• Exit strategies and exit plans for third parties
	(6) Incident Response	• Development of regulations and frameworks assuming the occurrence of cyber incidents
	(7) Insurance Company's Management Policies for Intermediaries and Other Third Parties	• Management policies for intermediaries (insurance agents, brokers) and third parties providing services associated with insurance products
Research Period	From June 17, 2025, to February 28, 2026 (Interviews with banks in the US, EU, and UK were conducted from September to October 2025, and interviews with insurance companies were conducted from November 2025 to January 2026.)	

© 2026. For information, contact Deloitte Tohmatsu Group.

The research was conducted based on global guidance related to TPCRM

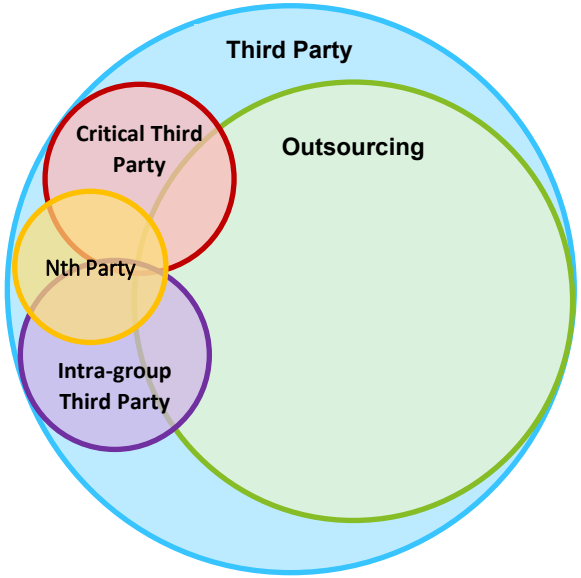
Research Findings overview

- As a prerequisite for the TPCRM framework, FIs in the US, EU, and UK have established a third-party risk management (TPRM) framework, and third-party cybersecurity risks are incorporated as one of the risk domains covered by TPRM.
- TPRM/TPCRM is implemented by building a system that will act as a platform to support the series of TPRM processes(Inherent Risk Assessments, Due Diligence, Contract, Ongoing Monitoring, Termination).

#	Scope of the Research	Research Findings
1	Classification of Third Parties and Management Policies	• FIs implement differentiated management based on inherent risk assessments. • The proportion of critical third parties is approximately 1%–10% of the total, and additional management measures are implemented for critical third parties, including the development of exit strategies and exit plans, concentration risk monitoring, and on-site inspections.
2	Concentration Risk	• FIs conduct concentration risk monitoring from the perspective of operational resilience. • Concentration in a single third party, concentration in specific Nth parties, and geographic concentration are categorized, transformed into data, and managed using the TPRM tool. The information is then utilized to determine the acceptability of the risk and feasibility of alternatives when the level of concentration is high.
3	Ongoing Monitoring After Contracting with Third Parties	• Regarding the utilization of cyber threat intelligence, objective risk assessment and timely risk detection were achieved by evaluating and monitoring the attack surface of third parties. The timely detection of vulnerable internet-connected devices is expected to reduce incident risk at small and midsize third-party vendors, where consistent enforcement of controls can be challenging. • If deficiencies were identified, cases were observed in which the FI required the third party to submit a remediation plan, and if these issues were not remediated, the FI terminated the contract.
4	Securing Audit Rights Over Third Parties and Methods	• Audit rights over third parties (including on-site inspections) and the minimum-security control requirements that must be complied with (encryption, access rights management, etc.) are explicitly stipulated and secured in contractual provisions. • In on-site inspections, in addition to verification of physical security, FIs carry out more in-depth evidence collection, confirmation of process maturity, and other such tasks than in remote investigations.
5	Exit Strategies and Exit Plans	• FIs establish response policies for the termination of third-party services and transition plans for switching to alternative solutions. To enhance effectiveness, institutions conduct regular testing. • With a focus on critical third parties, FIs establish processes for developing and approving strategies and plans at the time of contract execution and renewal.
6	Incident Response	• Each FI had established incident response procedures (such as reporting flows, procedures for network isolation, and risk assessments for reconnection) when a cyber incident occurs at a third party. Additionally, some cases were observed in which institutions conducted joint training with critical third parties to enhance the effectiveness of incident response. • In the event of an incident, the contract management department and cyber incident response team cooperate to respond.
7	Insurance Company's Management Policies for Intermediaries and Other Third Parties	• It was often observed that security assessment/management of intermediaries was managed outside the framework of TPRM. There were examples where the scope of TPRM was planned or extended to intermediaries by unifying the assessment of inherent risks, management standards, and the databases used for management between TPRM and intermediaries management.

Laws and guidelines require FIs not only to manage external contractors, but also to assess, identify, and appropriately manage the risks associated with third-party arrangements

supplementary information: requirements for third-party management under laws, regulations, and guidelines in various countries



■ Definition of a third party in "*Guidelines on Cybersecurity for the Financial Sector*"* ※1

Classification	Definition
Third Party	• 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."
Outsourcing	• An external contractor refers to "an organization to which operations are outsourced." This includes vendors of systems outsourced by FIs to provide financial services (including shared centers). Even in cases where no formal outsourcing contract exists, if the actual arrangement is equivalent to outsourcing, or if the outsourced operations are conducted overseas, such cases are also considered to fall under the definition of an external contractor.

※1： https://www.fsa.go.jp/common/law/cybersecurity_guideline_en.pdf

■ Classification and overview of third parties for which risks should be assessed and identified ※2

Classification	Overview
Critical Third Party	Refers not only to external contractors, but also to service providers that have direct business with FIs. This may include third parties with whom there are no business outsourcing contracts or remuneration arrangements, such as joint ventures. One proposal is to categorize third parties using current purchasing and service categories.
Nth Party	Refers to service providers that indirectly support the provision of services to FIs by third parties. Those that provide support third parties that deliver critical services are regarded as "critical Nth parties."
Intra-group Third Party	Refers to a member of an FI group that mainly provides services to institutions within the same group. This includes entities under common ownership or control of parent companies, sister companies, subsidiaries, and the like.

※2：Summarized based on documents listed in the appendix

© 2026. For information, contact Deloitte Tohmatsu Group.

FIs in the US, EU, and UK continue to focus on TPRM/TPCRM as a priority for risk management and are undertaking the following initiatives

Supplementary information : initiatives confirmed for the advancement of TPCRM

Implementation of TPCRM as a Component of TPRM	• As a prerequisite for the TPCRM framework, FIs in the US, EU, and UK have established a third-party risk management (TPRM) framework, and third-party cybersecurity risks are incorporated as one of the risk domains covered by TPRM. • The cybersecurity department is included as one of the subject matter expert departments for third-party risk and is promoting relevant measures. • 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.
Utilization of Technology and Data	• TPRM/TPCRM is implemented by building a system that will act as a platform to support the series of TPRM processes. • Relevant data (e.g., basic information on third parties, information on transactions with third parties, risk assessment results for each case, the status of improvements to identified issues, etc.) is managed on this system, which facilitates data analysis and visualization. Furthermore, since basic information and contract details of third parties are centralized, it is possible to manage and address concentration risk during the due diligence process for new contracts, such as by checking the concentration status of third parties or determining whether alternative third parties are available.
Utilization of Cyber Threat Intelligence	• From a cybersecurity perspective, the utilization of cyber threat intelligence has become widespread. • Methods such as risk scoring tools, open-source intelligence (OSINT), attack surface management (ASM), and dark web monitoring are being utilized to proactively conduct objective risk assessments that do not rely on responses from third parties, detect risk manifestations in a timely manner, and identify the impact of incidents such as information leakages. • Advanced practices have been observed, such as the establishment of dedicated cyber threat intelligence teams for third parties and the execution of in-depth investigations when signs of risk are detected in third parties. • It should be noted that, because the maturity of controls, such as policies and established processes, cannot be determined through cyber threat intelligence, risk assessments using questionnaires, etc., were conducted at all financial institutions.

© 2026. For information, contact Deloitte Tohmatsu Group.

Summary of Research Findings

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(1) Classification of third parties and management policies

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Methods of Third-Party Classification and Approach to Determining Which Third Parties Should Be Subject to Management	• While Japanese FIs are considering expanding their scope of management beyond traditional outsourcing, they are facing challenges in how to organize the classification of third parties to be managed under TPCRM.	• Each FI **classifies third parties** according to **factors such as the importance of the service, risk level, and type of service**. Each FI considered all third parties to be **within their scope of management**. Meanwhile, it was also observed that some FIs in the US included third parties supervised by the authorities (e.g., regulated third parties such as FMIs) within the scope of TPRM.	• Classifications should be reviewed and organized by reassessing the importance and categories, while utilizing the current purchasing category classifications and existing transaction data, including third-party services and transaction details • A mechanism should be considered to assign priorities based on risk and allocate resources to third parties that require enhanced management.
Nth Parties Subject to Management **Management of IT Assets Belonging to Third Parties and Nth Parties**	• How to manage subcontractors with whom the FI has no direct contractual relationship should be considered by referring to overseas best practices in this area. • There are difficulties in understanding the status of risk management related to IT asset management, such as cases where third parties reject requests to provide information on their rules and regulations.	• Each FI determines which **Nth parties should be subject to management** based on risk and **whether said party is a service provider**. • Many FIs sought to **visualize down to subcontractors** as part of their efforts to manage Nth parties. In addition, risks associated with Nth parties with whom these FIs have no direct contractual relationship were indirectly mitigated by **evaluating the third party's capability to manage its own contractors**. • Regarding **IT asset management for both third and Nth parties**, each FI checked the **development status of rules and regulations** by third parties. • Some FIs have begun pilot initiatives for the use of SBOMs. However, certain institutions requested regulatory intervention, as they were unable to obtain SBOMs due to a lack of cooperation from third parties.	• Processes should be designed to include evaluation procedures to verify control status, such as the development of policies and rules on third-party subcontractor management. • Regarding evaluation processes of a third party's rules such as IT asset management, where necessary, submission of concrete evidence such as system and network diagrams in addition to documentation should be requested and management policies and practices should be confirmed while having cybersecurity personnel participate.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(1) Classification of third parties and management policies

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Criteria for Determining Criticality and Management Practices for Critical Third Parties	• There is no clear guidance regarding the criteria for identifying critical third parties or management practices, which is why institutions are struggling to establish these.	• Regarding **the criteria for determining the criticality of third parties**, **in primarily the US, this determination is made mainly based on the results of inherent risk assessments of business operations, while in the EU and UK, this determination is made based on regulatory compliance requirements**. In all cases, third parties were classified as critical if the impact of suspending the services provided by said third parties was deemed critical to the business continuity of the FI. • From a cybersecurity perspective, it was observed that, for example, whether a third party is connected to their systems or networks was one of the inherent risk assessment items. • **Regarding the management practices for critical third parties**, all institutions conducted in-depth investigations through enhanced monitoring as an additional measure.	• Criteria for determining the importance of third parties should be established based on the content of the services provided by the third parties, the nature of the data handled, and the continuity of business operations in the event that the services provided by said third parties are suspended. • Continuous monitoring, such as enhanced monitoring of critical third parties, should be conducted to ensure that risks are being mitigated.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(2) Concentration risk

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Concentration Risk of Third Parties	• Classifications of concentration risk, which should be managed through TPCRM, have not been defined.	• Regarding **concentration risk of third parties**, each FI managed **third-party concentration, Nth party concentration, and geographic concentration** (such as the countries and regions where services are provided) from the perspective of operational resilience.	• As a method for managing concentration risk using existing systems and data, it may be necessary to review current vendor master files and databases and to develop and update ledgers or databases for analyzing which third parties or regions services are dependent on or concentrated in.
Methods for Measuring Concentration Risk	• There is uncertainty regarding measurement methods for determining what constitutes concentration. • There are challenges regarding how to efficiently manage and monitor third-party concentration risk with limited resources.	• **The total number of outsourcing contracts and total expenditure to a specific third party or their related subcontractors, as well as the region where the service is provided**, were used as **axes for measuring concentration risk**. Third party-related data used as measurement axes were taken from data registered in the TPRM tools utilized in the TPRM processes. This includes information on the third party or contract details (e.g., third party's address, contract amount, region where the service is provided, etc.), registered by the responsible personnel conducting the TPRM processes. • TPRM tools were utilized to centrally manage third-party data, and a dashboard and alert functions were implemented to efficiently identify and analyze concentration risk from third parties.	• After establishing a database and confirming the accuracy and completeness of the registered information, consideration should be given to the categories for measuring concentration. • From the perspective of centralizing the management of TPRM-related processes and data, gathering information on and considering the introduction of TPRM tools is also an option.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(2) Concentration risk (supplementary information)

Sector-Level Concentration

Types of Concentration Risk	Overview
Systemic-Level Concentration Risk	• This refers to a risk that impacts the entire financial sector which arises from a dependence on one or more services provided by a single or limited number of third parties. • Systemic concentration risk is managed by the authorities in each country. However, it was also indicated that, as part of providing information to the authorities, FIs should be aware of systemic concentrations within their own organizations.
FI-Level Concentration Risk	• This refers to a risk arising from situations where an FI depends on one or more services provided by a single or limited number of third parties. • FI-level concentration risk is managed by FIs.

Management Items (Examples)

Concentration on a Single Third Party	Concentration on Critical Nth Parties	Geographic Concentration
• This is a concentration risk arising from a dependence on a single third party in which many operations of the FI would be affected if said third party were to suspend their services. • Measurement methods: total expenditure for specific categories, ratio of the number of contracts, and other such information	• This is a concentration risk arising when a critical third party with whom an FI has a direct relationship depends on a single subcontractor (Nth party). Such a concentration risk can have similar impacts as a single third party or geographic concentration. • Measurement methods: total expenditure for specific categories, the ratio of the number of contracts held by this subcontractor versus total number of contracts, and other such information	• This is a concentration risk arising from dependence on a single country or region. If a natural disaster, political instability, sanctions, or regulatory changes were to occur in that country or region, many operations of the FI would be affected. • Measurement methods: the number of contracts in specific countries or regions classified as high-risk and other such information (e.g., using geographic data registered in the basic information of the contract with the third party)

Visualization and management using TPRM tools

*Summarized based on BCBS: “Principles for the sound management of third-party risk” and BoE/PRA: “SS2/21 Outsourcing and third-party risk management”

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(3) Ongoing monitoring after contracting with third parties (1/2)

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Monitoring through Cyber Threat Intelligence	• Contracts are regularly reassessed during ongoing monitoring, such as when the contract was concluded and through annual periodic inspections. However, there are concerns regarding methods for detecting risks in a timely manner. • Third-party incidents are detected via post-incident reporting from third parties.	• Regarding **the utilization of cyber threat intelligence**, **objective risk assessment and timely risk detection** were achieved by evaluating and monitoring the attack surface of third parties. Many FIs reduced **their operational burden by utilizing risk scoring tools, including ASM functions**. However, there were also comments indicating that it is necessary to carefully review and select the output information due to concerns such as excessive detection (false positives) when using such tools. • In addition to the approaches observed in which monitoring was focused on critical third parties, there were also advanced cases in which **monitoring was conducted for all third parties or a threat intelligence team dedicated to third-party risk was organized**. • Cyber threat intelligence monitoring was utilized as an additional input during third-party risk assessments prior to a contract's conclusion and for continuous monitoring after the contract's conclusion to confirm that there were no significant changes in the risk profile of the third party. • There are also cases where timely detection of risk indicators (such as vulnerable internet-connected devices) is expected to be effective in preventing incidents at small and medium-sized third parties, where it is difficult to thoroughly implement security controls. • If deficiencies were identified through this monitoring, cases were observed in which the FI required the third party to submit a remediation plan. There were also cases where contracts were terminated when no improvement was observed.	• Use of cyber threat intelligence in third-party risk assessments and ongoing monitoring should be considered. • In cases where there are constraints such as limited resources or budget (e.g., small and medium-sized FIs), alternative measures should be considered such as determining which third parties should be the focus of ongoing monitoring (e.g., contractors that process information in the FI's possession), re-conducting continuous due diligence, and confirming the status of cyber-related audits conducted by third parties on the FI.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(3) Ongoing monitoring after contracting with third parties (2/2)

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Sharing Questionnaires within the Industry	• Japanese FIs are facing challenges regarding efficient methods for developing and revising risk assessment items in response to the changing external cyber environment, as well as efficient methods and approaches for enhancing the management of numerous third parties.	• Conducting third-party risk assessments using individually designed proprietary questionnaires by each FI imposes a burden on both FIs and third parties. Therefore, overseas, there are frameworks such as **industry-standard questionnaire templates** designed among participating organizations in communities or **frameworks for sharing assessment (survey) results on industry-wide community-based platforms**. Among the FIs interviewed, there were also cases where such frameworks were utilized (**after confirming consistency with their own risk appetite**) for the purpose of operational efficiency. • The ways in which industry-standard questionnaire templates were used vary by FI. It has been confirmed that some institutions only refer to the question items as a reference, while others use these templates as they are, or customize them by adding their own questions or making other modifications. • Regarding the framework for sharing assessment results, cases were observed in which other organizations participating in industry-wide community-based platforms used the most recent third-party assessment results gained through a standard questionnaire based on risk. FIs that participate in such communities but do not use the standard questionnaire also mentioned that they sometimes refer to the results of recent assessments conducted by other firms only if the questions closely align with what their own risk assessment questionnaires are attempting to confirm.	• From the perspective of operational efficiency, it is considered useful to utilize frameworks for sharing industry-standard questionnaire templates and results. • However, the purpose of evaluating third parties is to assess whether “the third parties are able to ensure the same level of risk management as the institution itself.” Therefore, it is a prerequisite that each FI sets its own risk appetite and utilizes such frameworks within that scope.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(3) Ongoing monitoring after contracting with third parties (supplementary information)

Examples of technologies utilized, etc.
➢ **Risk scoring tools *Utilized by many of the institutions targeted by this research** Tools or services that regularly assess the cybersecurity posture of companies and organizations from an external perspective and visualize the results as scores or rankings. ➢ **Open-Source Intelligence (OSINT)** An investigative approach that involves investigating information that can be legally obtained, such as data available on the internet, to collect, combine, and analyze information that may indicate organizational vulnerabilities or potential avenues for attack. ➢ **Dark web monitoring** Monitoring and investigative activities conducted to understand the flow of information and trends in illicit transactions on websites and other resources that exist on specific networks not accessible via general search engines. ➢ **Attack Surface Management (ASM) *Utilized by many of the institutions targeted by this research** A mechanism for investigating information on IT assets that are accessible from external sources (such as the internet) and continuously assessing the vulnerabilities present in those assets.

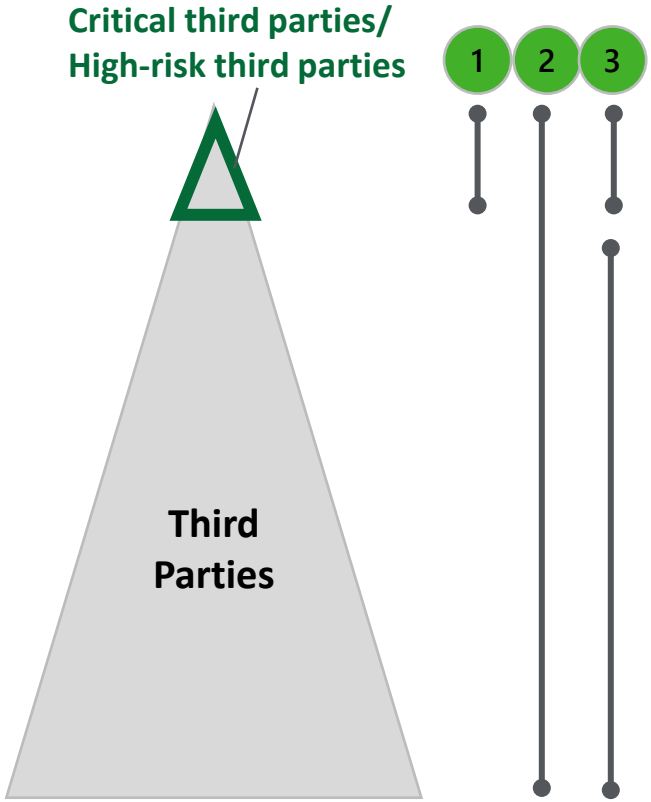
- Emphasis is placed on the effectiveness of achieving objective and timely monitoring that does not rely on responses to questionnaires administered to third parties during due diligence and other processes.
- Effects such as automation of the risk assessment process, reduction of operational burden, and expansion of the assessment scope are expected.
- Monitoring is conducted in a manner that does not affect the monitored entities.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(3) Ongoing monitoring after contracting with third parties (supplementary information)

Where and how threat intelligence is utilized



	Where threat intelligence is utilized	How threat intelligence is utilized
1	Limited to critical third parties/high-risk third parties	• Monitoring using risk scoring tools, ASM, and similar solutions is conducted. • Monitoring limited to critical third parties identified through inherent risk assessments and focused on the detection of incidents or significant changes.
2	Utilized equally for all third parties	• Achieving efficiency by utilizing risk scoring tools, ASM, and similar solutions. • In some cases, external vendors are commissioned to conduct in-depth investigations and dark web monitoring when third-party risks materialize, or incidents are identified. • There were also cases observed where dark web monitoring was conducted for all third parties.
3	Utilized for all third parties, with a particular focus on critical third parties	• Monitoring and in-depth investigations using OSINT, dark web monitoring, and similar solutions are conducted directly by the internal intelligence team of FIs • There are also cases where efficiency is achieved for non-critical third parties by utilizing risk scoring tools, ASM, and similar solutions.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(4) Securing audit rights over third parties and methods

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Contractual Provisions Related to Cybersecurity	• There is concern that, due to the absence of contractual provisions related to cybersecurity in contracts and other documents, the minimum necessary security measures may be insufficient.	• Each FI had **prepared standard contracts for agreements with third parties, and these contracts include clauses related to applicable laws and regulations as well as minimum required cybersecurity provisions that third parties must comply with (for example, requirements regarding data encryption, leakage prevention measures, network security, access control, etc.).** • It was also noted that, during contract negotiations, if a third party was **unable to meet** the minimum required cybersecurity clauses, some institutions **chose not to enter into contracts with those third parties.** • Additionally, it was confirmed that there were cases where the control clauses required of third parties as conditions for transactions were disclosed on the institution's website.	• The current contract templates should be reviewed to consider whether any additional clauses are necessary. • The contracts should be reviewed starting with those with existing critical third parties and the addition of clauses that enable appropriate management of third parties should be considered if no such clauses are in place. • Along with reviewing contract templates, the timing for updating existing contracts should also be considered, such as making changes during the contract period or at the time of the next contract renewal. • A framework should be established to allow for the consideration of contract provision changes and for communicating/explaining these changes both internally and externally (such as through collaboration among multiple departments).
Audit Rights and Onsite Assessments for Third Parties	• While risk assessments using questionnaires and onsite assessments are used in combination, overseas best practices should be referenced regarding methods for securing audit rights over third parties, especially when coordination becomes difficult with third parties who refuse to undergo onsite assessments.	• Regarding **audit rights over third parties** and the right to conduct **onsite assessments**, each FI **secured audit rights** over third parties by **including them as contractual provisions**. • On the other hand, with respect to onsite assessments, it was noted that while direct viewing or observation of evidence onsite was previously emphasized, after the COVID-19 pandemic, some FIs shifted to remote meetings and conducted assessments by confirming evidence via screen sharing. However, onsite assessments were still conducted for areas where direct confirmation was necessary, such as physical security. Additionally, some FIs believe that on-site reviews enable more in-depth evidence collection and more thorough verification of process maturity than remote reviews. • In the case of major CSPs, it was noted that joint audits were conducted together with industry groups in some cases, and the results were shared with FIs participating in those industry groups.	• The necessity of onsite assessments should be considered based on the risks and objectives to be assessed, as well as the level of importance of the third party to the FI. • In cases where it is difficult for the FI to obtain or exercise audit rights on their own (e.g., cloud services), alternative options, such as third-party certificates (e.g., SOC2 reports) and development of an industry-wide joint audit framework should be considered.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(5) Exit strategies and exit plans

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Exit Strategies and Exit Plans of Third Parties	• The contents to be included in third-party exit strategies and exit plans, as well as the methods for distinguishing between them, have not been clearly defined.	• **Exit strategies and exit plans for third parties were developed by each FI, with priority given to critical third parties.** In cases where FIs required the development of such plans even for non-critical third parties, the level of detail included in the items was adjusted according to their priority. • For third parties identified as critical, the TPRM processes incorporated procedures to ensure that exit strategies and exit plans were always formulated and approved. • Although there was no unified standard for the definition of each document, **an exit strategy was formulated as a basic policy for how to respond when third-party services are terminated or interrupted, and an exit plan was developed as a document detailing the procedures for transitioning to alternative measures (such as switching to an alternative provider).** • All financial institutions conducted regular reviews and tabletop testing of the exit plans they had developed, and incorporated maintenance and management activities to enhance their effectiveness into the TPRM processes.	• First, critical third parties to subject to the exit strategies and exit plans should be identified. • While it is not necessary to separate documents for “strategy” and “planning,” required items that will form a part of each document, such as the basic response policy and detailed migration plan, should be organized. While considering these items, one approach is to ensure they can be managed in alignment with existing internal documents, such as business continuity plans (BCPs). • Establishment of mechanisms to ensure effectiveness, such as regular reviews of exit plans and documentation of the results (for example, through ongoing management of the TPRM processes), should be considered.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(5) Exit strategies and exit plans (supplementary information)

Exit Strategy	
A document that summarizes the basic policy and overall approach regarding how an FI will respond in the event that services provided by a third party are terminated or interrupted.	• Activation conditions (e.g., bankruptcy of the third party, occurrence of a cyber incident, etc.) • Internal and external contact points • Termination or interruption of services dependent on the third party (including criteria for selecting alternative plans) • Policy for transitioning to alternative plans (insourcing or switching to alternative third parties) • List of alternative vendors, etc.

Exit Plan	
A document that details the migration plan to ensure that an FI can maintain its operations and services.	• Schedule for transitioning to alternative plans • Roles, responsibilities, and resources for the transition to alternative plans • Costs for the transition to alternative plans • Internal and external communication strategies • Interoperability with alternative third parties • Transition procedures • Procedures for data return and disposal, etc.

*Summarized based on the result of interviews as well as FSB's report, "Enhancing Third-Party Risk Management and Oversight – A toolkit for financial institutions and financial authorities"

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(6) Incident response

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Development of Regulations and Frameworks Assuming the Occurrence of Cyber Incidents	• When a cyber incident occurs at a third party, there is a concern that the responsible department may not be clearly identified, leading to delays in response. • Although contract management is the first line, responses tend to concentrate in the cybersecurity department, raising concerns about the impact on routine activities and resource allocation.	• Each FI had established **incident response plans and specific response procedures (such as procedures for network isolation and risk assessments for reconnection)** for reporting flows and other such actions when a cyber incident occurs at a third party. • In the event of an incident, **the contract management department and cyber incident response team cooperate** to respond. In addition, regardless of the type of third party, there were cases where, for third parties connected to the institution's systems or networks, a framework was established to enable the necessary procedures such as network disconnection in the event of an incident. • Additionally, some cases were observed in which institutions **conducted joint trainings with critical third parties** to enhance the effectiveness of incident response. • All FIs participated in trainings organized by industry associations for incidents at third parties such as FMIs.	• Incident response plans and specific response procedures that assume cyber incidents at third parties should be developed. • To enhance effectiveness, regular tabletop trainings should be conducted within the organization, including the contract management department that acts as the point of contact for third-party contracts. • Critical third parties should be identified and joint trainings with them should be considered.

© 2026. For information, contact Deloitte Tohmatsu Group.

Improvement measures in Japanese FIs were considered based on insights obtained from interviews with major FIs in the US, EU, and UK

(6) Incident response (supplementary information)

Cyber Incident Response		
Normal Operations	Development of Response Plans and Procedures for Cyber Incidents	➢ Examples of items included in cyber incident response plans are as follows: • Reporting flow in the event of a cyber incident at a third party • Escalation flow to the authorities • Reporting procedures, including confirmation of the cause of the incident and any leaked information • Alternative third parties, procedures for switching to alternative third parties, and approval processes (response to cyber contingency plans) • Conditions and procedures for network reconnection
	Joint Trainings with Third Parties	➢ Conduct tabletop trainings and similar activities based on the cyber incident response plan at least annually ➢ Conduct joint trainings with critical third parties ➢ For FMIs and similar entities, participate in trainings organized by industry associations, rather than planning and conducting trainings independently
Emergency Operations	Response at the Time of an Incident	➢ In the event of an incident, the department in charge of managing contracts acts as the point of contact with the third party ➢ The contract should clearly state the obligation of the third party to provide notification in the event of a cyber incident ➢ The cyber incident response team is responsible for early detection of cyber incidents through threat intelligence activities and provides expert knowledge ➢ The contract department and cyber incident response team cooperate to respond

© 2026. For information, contact Deloitte Tohmatsu Group.

Considerations for improvement measures in Japanese FIs were derived based on insights obtained from interviews with major FIs in the US, EU, and UK

(7) Insurance company's management policies for intermediaries and other third parties

Research Items	Hypothesis on Challenges Faced by Japanese FIs	Research Findings	Considerations for Improvement Measures in Japanese FIs
Management Policies for Intermediaries	• Although insurance companies have been conducting inspections of intermediaries based on management programs that they have developed since before, insurance companies are now facing increased challenges in risk management due to the increasing spread of cyber threats, especially where intermediaries and providers of services associated with insurance products handle critical information.	• It was often observed that intermediaries have traditionally been managed outside the framework of TPRM **and assessment/management of related risks have been conducted in the same manner as TPRM**. Overseas, due to differences in business practices, intermediaries are primarily involved in intermediary functions and often do not retain policyholder information. As a result, their inherent risk is frequently assessed as "low." • On the other hand, **there were some cases where intermediaries access policyholders' information for activities** such as insurance renewals. 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.** There were also examples where the scope of TPRM and Cyber Threat Intelligence monitoring were extended to intermediaries by unifying the assessment of inherent risks, management standards, 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 administration and claims payment, within the TPRM framework.** There have also been instances in which **whether to include brokers within the scope of TPRM was under consideration**.	• Mechanisms that, as seen in examples from overseas insurance companies, assess inherent risks should be considered and a risk-based approach should be taken to prioritize risks and allocate resources to third parties that require enhanced management since the number of entities to be managed is expected to be large. (It should be considered to expands the scope of TPRM to include intermediaries) • The utilization of Cyber Threat Intelligence monitoring should also be considered since 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.
Management Policies for Third Parties Providing Services Associated with Insurance Products		• **Approaches differed among insurance companies regarding providers of services associated with insurance products**, such as those offering second medical opinions to policyholders. In some cases, insurance companies limited their role to outsourcing services associated to their products to third parties, and since policyholders contacted the service provider directly, **these providers were excluded from management**. On the other hand, there were cases where, because service providers handled information about the insurance company's policyholders through mediation, **they were managed within the TPRM framework**.	• Management policies for third parties providing services associated with insurance products (for example, cases where a third party provides IoT devices such as cameras and processes information collected from those devices) should be considered based on the type of information handled and the relationships among the insurance company, third party, and policyholders.

© 2026. For information, contact Deloitte Tohmatsu Group.

Appendix

© 2026. For information, contact Deloitte Tohmatsu Group.

List of Laws, Regulations and Guidelines Covered in this Research

No	Document	Publishing Organization	Jurisdiction	Overview
1	Consultative Document Principles for the sound management of third-party risk	• Basel Committee on Banking Supervision (BCBS)	International Organization	✓ This consultative document sets forth principles for the sound management of third-party risk in the banking industry and is intended for banks and supervisory authorities.
2	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities	• Financial Stability Board (FSB)	International Organization	✓ This is a toolkit for third-party risk management and supervision intended for financial authorities, FIs, and service providers.
3	FCA Handbook - SYSC 8 Outsourcing	• Financial Conduct Authority (FCA)	UK Authority	✓ This is one of the sections comprising “Senior Management Arrangements, Systems and Controls (SYSC)” in the FCA Handbook, which summarizes the laws and other provisions of the FCA. This section stipulates how FIs (such as banks, securities firms, and investment firms) should design and operate their outsourcing arrangements and systems.
4	Supervisory Statement | SS2/21 Outsourcing and third party risk management	• Bank of England (BoE) • Prudential Regulation Authority (PRA)	UK Authority	✓ This document sets out the expectations of the PRA regarding how FIs should comply with regulatory requirements and expectations related to outsourcing and third-party risk management.
5	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector	• FCA • BoE • PRA	UK Authority	✓ This document sets out the expectations of regulators regarding how critical third parties should comply with the obligations and responsibilities imposed by the Financial Services and Markets Act 2000 (FSMA) (as amended) and the rules of regulatory authorities.

© 2026. For information, contact Deloitte Tohmatsu Group.

List of Relevant Laws, Regulations and Guidelines Covered in this Research

No	Document	Publishing Organization	Jurisdiction	Overview
6	Final Report on EBA Guidelines on outsourcing arrangements	• European Banking Authority (EBA)	EU Authority	✓ This document sets out governance frameworks and related management expectations and processes concerning outsourcing arrangements for all FIs within the EBA's remit.
7	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 EBA's "Guidelines on outsourcing arrangement" and covers a broader range of third-party contracts not just limited to outsourcing contracts, setting out the risk management methods, standards, and roles that FIs and competent authorities should implement for these arrangements.
8	Digital Operational Resilience Act (DORA)	• European Commission • European Parliament • Council of the European Union	EU Policy-making Bodies	✓ This regulation was introduced with the aim of strengthening the digital resilience of FIs by integrating requirements related to ICT risk, which had previously been addressed individually by various EU laws. It sets out the rules on ICT risk management capabilities, incident reporting, operational resilience testing, supervision of ICT third-party risks, and similar areas.
9	Interagency Guidance on Third-Party Relationships: Risk Management	• Board of Governors of the Federal Reserve (FRB) • Federal Deposit Insurance Corporation (FDIC) • Office of the Comptroller of the Currency (OCC)	US Authority	✓ This guidance is intended for banking organizations regarding risk management in relationships with third parties. This document presents the fundamental principles and considerations for implementing risk management, required activities and considerations for each stage of the lifecycle for third-party risk management, organizational oversight frameworks and responsibilities, and supervisory framework of the authorities.
10	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."

© 2026. For information, contact Deloitte Tohmatsu Group.

List of Relevant Laws, Regulations and Guidelines Covered in this Research

No	Document	Publishing Organization	Jurisdiction	Overview
11	Solvency ii Directive	• European Parliament • Council of the European Union	EU Policy-making Bodies	✓ This is a prudential regulation for insurance and reinsurance companies in the EU that was established by the European Parliament and 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.
12	Draft Application Paper on operational resilience objectives and toolkit	• International Association of Insurance Supervisors (IAIS)	International Organization	✓ This document provides guidance on the objectives of operational resilience for insurance companies and the practices and toolkits that support these objectives. More specifically, this document is structured to show the relationship between operational resilience, governance, and operational risk, key elements to promoting operational resilience, and goals of supervising insurance companies.
13	NAIC Insurance Data Security Model Law	• National Association of Insurance Commissioners (NAIC)	US Authority	✓ This is a model law at the state level regarding the establishment of information security programs and related matters for insurance companies and other such entities licensed by the various state insurance departments in the US. More specifically, this document is structured to show, for example, the development and implementation of information security programs, investigations carried out when a cybersecurity incident occurs, notifications sent to state health committees, and supervisory authority of insurance committees.
14	Industry Letter: Guidance on Managing Risks Related to Third-Party Service Providers	• New York Department of Financial Services (NYDFS)	US Authority	✓ This guidance is addressed to FIs 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.

© 2026. For information, contact Deloitte Tohmatsu Group.

Summary of Findings Confirmed in Each Law, Regulation, and Guideline

Ongoing monitoring after contracting with third parties

Research Items	Overview
Requirements for the ongoing monitoring process	■ Continuous assessment and monitoring of the performance and risks related to service delivery in accordance with agreements or contracts with third parties are to be implemented. ■ Regular reporting to the board of directors and management is to be conducted, as well as identification of significant issues and establishment of processes for reporting to senior management and responding in the event of an incident. ■ For arrangements with critical third parties, more comprehensive and frequent monitoring should be conducted.
Examples of items implemented for ongoing monitoring	■ Third-party performance (such as execution of operations and fulfillment of SLAs) and the occurrence of significant issues or concerns are to be confirmed. Examples include monitoring incidents such as major or repeated findings, deterioration of financial conditions, data loss or leakage, and service interruptions as well as indicators of compliance violations, concentration risk, and other risk manifestations. ■ Regular visits and meetings with third-party representatives to discuss performance and operational challenges are to be held. ■ It should be confirmed that the availability, integrity, and confidentiality of data and information are ensured.

© 2026. For information, contact Deloitte Tohmatsu Group.

Summary of Findings Confirmed in Each Law, Regulation, and Guideline

Audit rights over third parties

Research Items	Overview
Examples of audit rights to include in contractual provisions of FIs	■ Audit rights over and information access rights to third parties, as well as access rights to service providers' relevant facilities (e.g., headquarters and operation centers) and equipment used for service delivery (e.g., systems, networks, and data) ■ Service performance indicators and KPIs ■ The right for the FI to receive accurate and timely information regarding critical services (e.g., information on incidents, service details, and significant changes) ■ Provisions regarding operational resilience (e.g., business continuity, emergency response plans, maximum downtime, Recovery Time Objective (RTO), and Recovery Point Objective (RPO)) ■ Obligation to notify the FI in the event of compliance violations, law enforcement actions, regulatory procedures, or incidents that pose significant risks to the FI or its customers. ■ Obligation to provide notice of mergers, acquisitions, business transfers, major personnel changes, or other significant changes that may affect the relevant activities ■ Types and frequency of reports to be received from third parties (e.g., operational reports, financial reports, security reports, and control assessment results) ■ Right to continuous monitoring ■ Conditions governing subcontracting to subcontractors
Examples of items reviewed by supervisory authorities regarding the management of third parties by FIs	■ Evaluation of the FI's management ability to oversee their relationships with third parties ■ Evaluation of the impact of third-party relationships on the FI's risk profile and key aspects of its financial and business operations, including compliance with relevant laws and regulations ■ Execution of transaction testing related to third-party activities, or review of the test results, and assessment of compliance with relevant laws and regulations ■ Evaluation of whether appropriate discussions are being conducted with management or the board of directors and findings are being pointed out regarding significant risks or deficiencies in the institution's risk management processes ■ Evaluation of whether the FI has developed appropriate and sustainable corrective actions for deficiencies related to audits of third parties involved in particularly important activities ■ Evaluation of whether the FI has identified and managed all relevant risks ■ Evaluation of whether the FI has identified, evaluated, and appropriately managed conflicts of interest in arrangements such as outsourcing contracts

© 2026. For information, contact Deloitte Tohmatsu Group.

Glossary

Glossary Term		Overview
1	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.
2	Cyber Threat Intelligence Monitoring	A structured investigative method that gathers, correlates, and analyzes information regarding the trends and techniques of cyberattacks, for the purpose of informing and enhancing an organization's cybersecurity countermeasures.
3	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.
4	FMI (Financial Market Infrastructure)	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.
5	SBOM (Software Bill of Material)	A machine-readable inventory that lists all software components, along with information about their dependencies.
6	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.
7	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.
8	BCP (Business Continuity Planning)	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.
9	Systemic Risk	A risk that has the potential to cause significant adverse effects on the entire financial sector or the 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.
10	SLA (Service Level Agreement)	The standards and commitments regarding service quality, availability, and other performance metrics agreed upon in a contract between an organization and a third party.
11	KPI (Key Performance Indicator)	A quantifiable metric used by an organization to measure and evaluate progress toward achieving its objectives and to assess performance outcomes.

© 2026. For information, contact Deloitte Tohmatsu Group.

Deloitte.
デロイト トーマツ

This survey was conducted with the aim of extracting advanced initiatives from major banks and insurance companies in the United States, the EU, and the United Kingdom, and obtaining insights for Japanese financial institutions. Many of the organizations surveyed have a global presence, with tens of thousands to several hundred thousand employees. This report refers to the practices of these banks and insurance companies; however, please note that matters related to organizational structure and human resources are based on organizations of this scale and may not necessarily be directly applicable to financial institutions of all types and sizes.

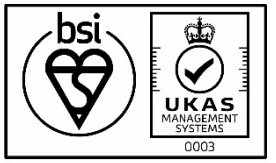
Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Group Japan LLC., Deloitte Tohmatsu Tax Co., and DT Legal Japan. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With approximately 17,000 people in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp/en.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication and any attachment to it is for internal distribution among personnel of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization").
It may contain confidential information and is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, please notify us immediately, do not use this communication in any way and then delete it and all copies of it on your system.
None of DTTL, its member firms, related entities, employees or agents shall be responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

IS 669126 / ISO 27001



BCMS 764479 / ISO 22301

certification scopes of IS and BCMSHttp://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited

© 2026. For information, contact Deloitte Tohmatsu Group.