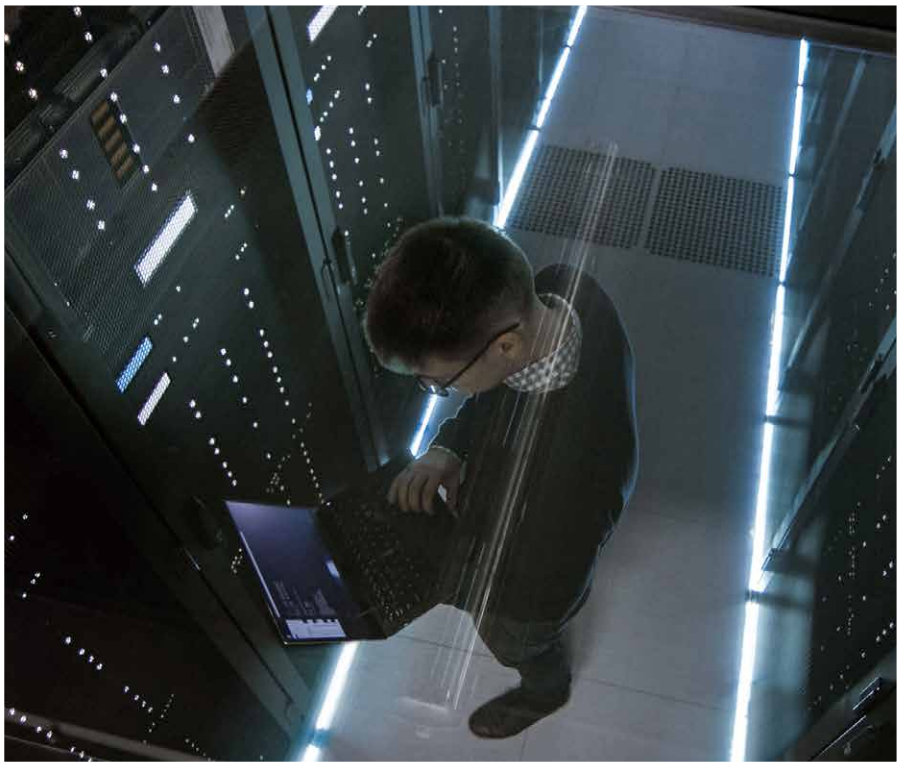
# The latest trends in supply chain cyber risk management at overseas financial institutions



pwc

www.pwc.com/jp/en

# Executive summary

In recent years, regulatory authorities have increasingly called upon financial institutions to strengthen cyber risk management for their supply chains, resulting in a need for both Japanese financial institutions and their subcontractors to update their risk management measures. A failure to sufficiently address supply chain cyber risk management could lead not only to impacts like information leaks and system outages, but also to medium- to long-term business impacts including damage to an institution's reputation and customer loyalty.

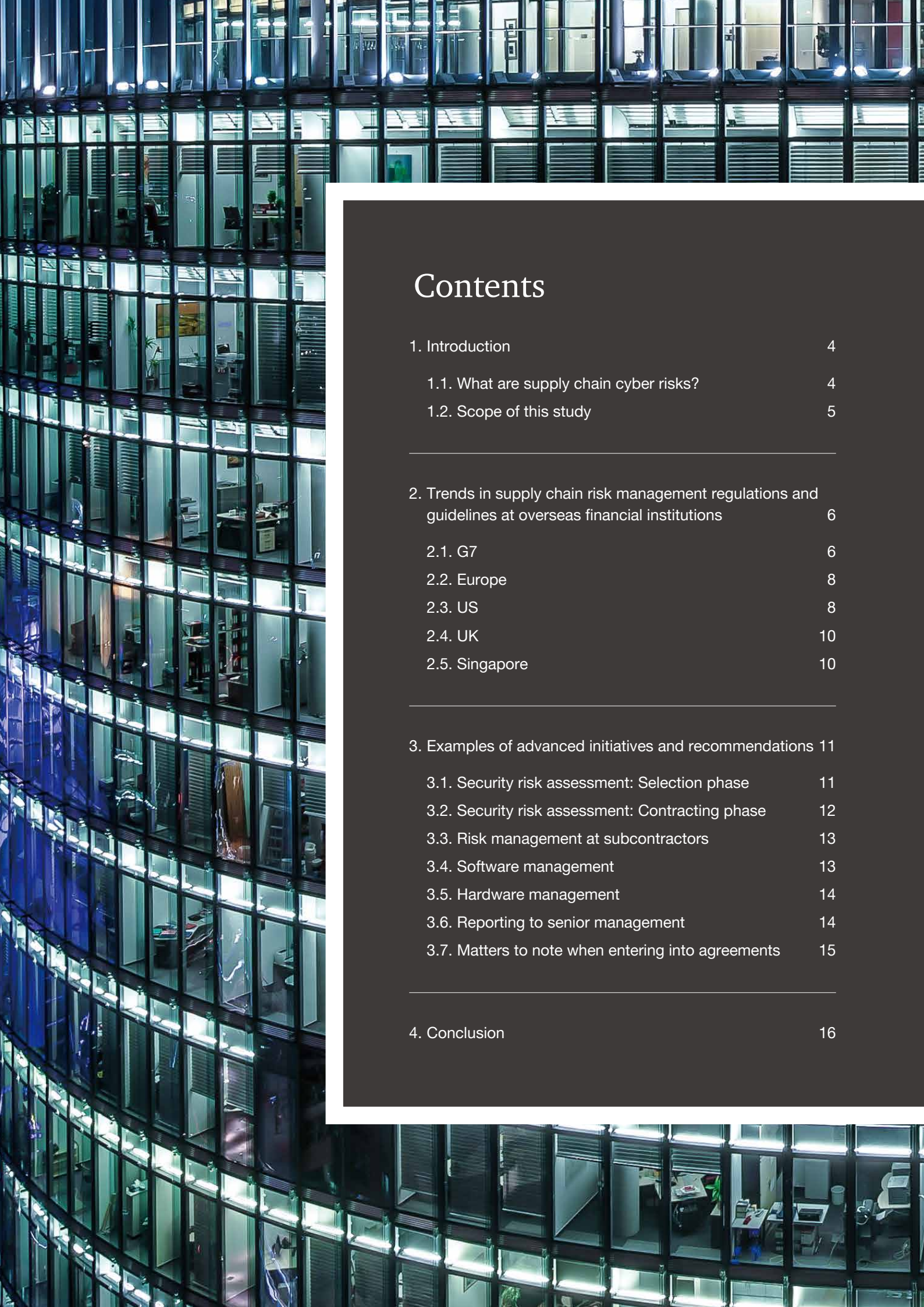
However, many security officers of financial institutions have concerns regarding issues such as the extent to which they can require subcontractors with whom their institution has no capital relationship to implement management measures and what kind of measures they need to take to implement efficient and effective management. To help those responsible for security at Japanese financial institutions obtain hints on how to address such issues, PwC Consulting LLC conducted interviews with experts at overseas financial institutions regarding their own past successes.

This report is intended for those responsible for cybersecurity at Japanese financial institutions. It presents examples of advanced initiatives taken overseas with regard to supply chain cyber risk management and compiles recommendations for actions to be taken by Japanese financial institutions in the near future.

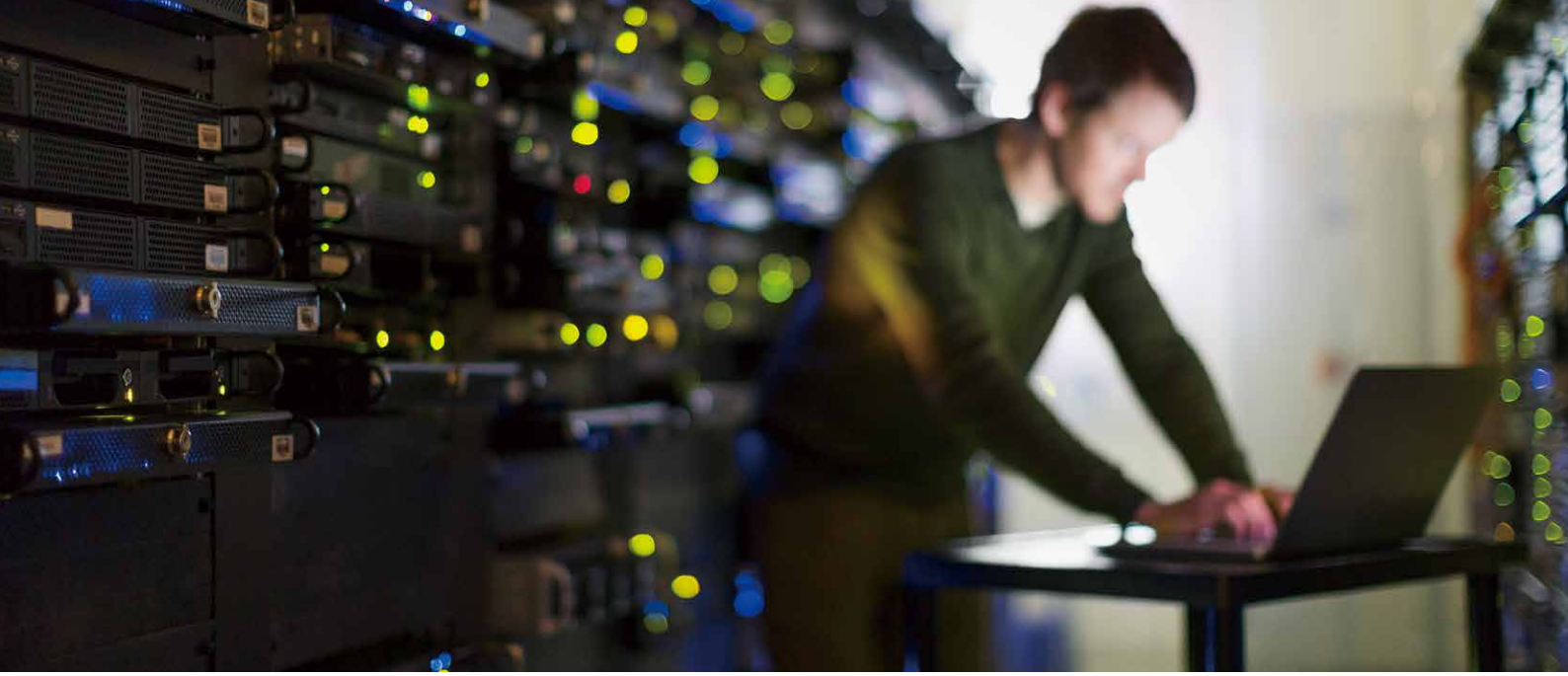
## Recommendations based on our discussions with experts

We conducted interviews with experts at overseas financial institutions that are pursuing advanced initiatives in supply chain cybersecurity, and arrived at the following recommendations for each phase of the process, which can also be adopted by Japanese corporations.

| Phase | Recommendations |
|---|---|
| Security risk assessment: Contractor/service selection phase | • Conduct security risk assessment for target companies and services by gathering and analysing publicly available information. Utilising third-party risk evaluation services might help to streamline the process. . |
| Security risk assessment: Contracting phase | • Assign personnel who are familiar with technical security to the assessment team and conduct assessment based on trending threat scenarios..<br>• Anticipate the occurrence of incidents and suspected incidents, and stipulate the scope of responsibilities and reporting time limits in a service level agreement (SLA). |
| Security risk management at subcontractors' | • Conduct on-site visits to subcontractors that handle high-risk systems to review their risk management processes.<br>• If work is sub-outsourced, demand that the original subcontractors conduct security management for the parties to which work is sub-outsourced (third parties). If work is sub-sub-outsourced etc., require all subsequent parties to implement security on the same level as that which your own company requires. |
| Software management | • Software configuration management should be conducted thoroughly when new products are implemented, and should be linked with vulnerability management. Also consider the use of software bills of materials (SBOMs).<br>• Utilise management tools for open source software (OSS) to streamline the selection of such software and identify dependencies. |
| Hardware management | • Be thorough in asset management, and develop a system to enable firmware to be updated promptly.<br>• Conduct threat scenario-based security tests. |
| Reporting to senior management | • In reports regarding security costs, avoid overuse of technical terms, prepare documents using business language and make reports based on the impacts on profits, customer satisfaction, reputation and customer loyalty.<br>• The optimal solutions regarding the routes for reporting cybersecurity risks to senior management vary from one organisation to another. Therefore, consider risk-based, monetary cost-based, IT-based and other approaches to determine the route best suited to your organisation. When doing so, take measures to ensure there is no conflict of interest between the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO). |



# Contents



# 1 Introduction

## 1.1 What are supply chain cyber risks?

In recent years, both damage caused by cyberattacks that exploit supply chains and concern about such attacks are on the rise. Rather than directly targeting institutions, these attacks target affiliated organisations whose security is comparatively weak, and use those systems as a springboard to attack the suppliers and users of widely-used hardware, software and services.

In '10 Major Security Threats', a document compiled by the Information-Technology Promotion Agency (IPA), Japan[1], the category 'Attacks Exploiting Supply Chain Weaknesses' is rising in rank, from third in 2022 to second in 2023. Potential cyber risks and their anticipated entry points are shown below.

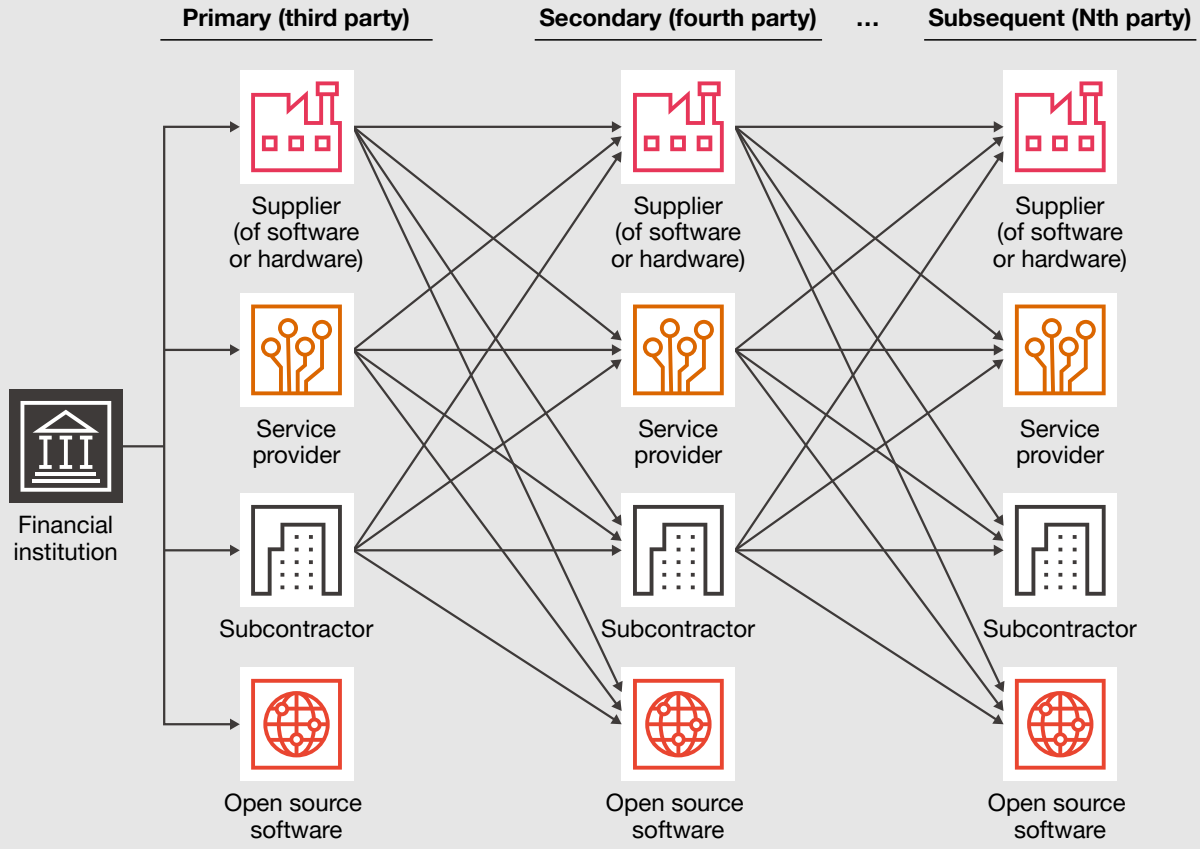
| Entry point | Examples of anticipated cyber risks |
|---|---|
| **Subcontractor** | • Information leakage caused deliberately or due to negligence on the part of subcontractor employees<br>• Theft or leakage of source code or intellectual property due to inappropriate access control for online services<br>• Knock-on effects of cyber incidents occurring at the subcontractor<br>• Unauthorised access via subcontractor |
| **Supplier (of hardware or software)** | • Unauthorised access through backdoors embedded at the pre-delivery stage<br>• Malware infection through contaminated software updates<br>• Unauthorised access through the exploitation of vulnerabilities |
| **Service provider** | • Malware infection through contaminated software updates<br>• Unauthorised access through the exploitation of vulnerabilities |
| **Open source software** | • Unauthorised access through the exploitation of vulnerabilities<br>• Embedding of malicious code at the time of development |

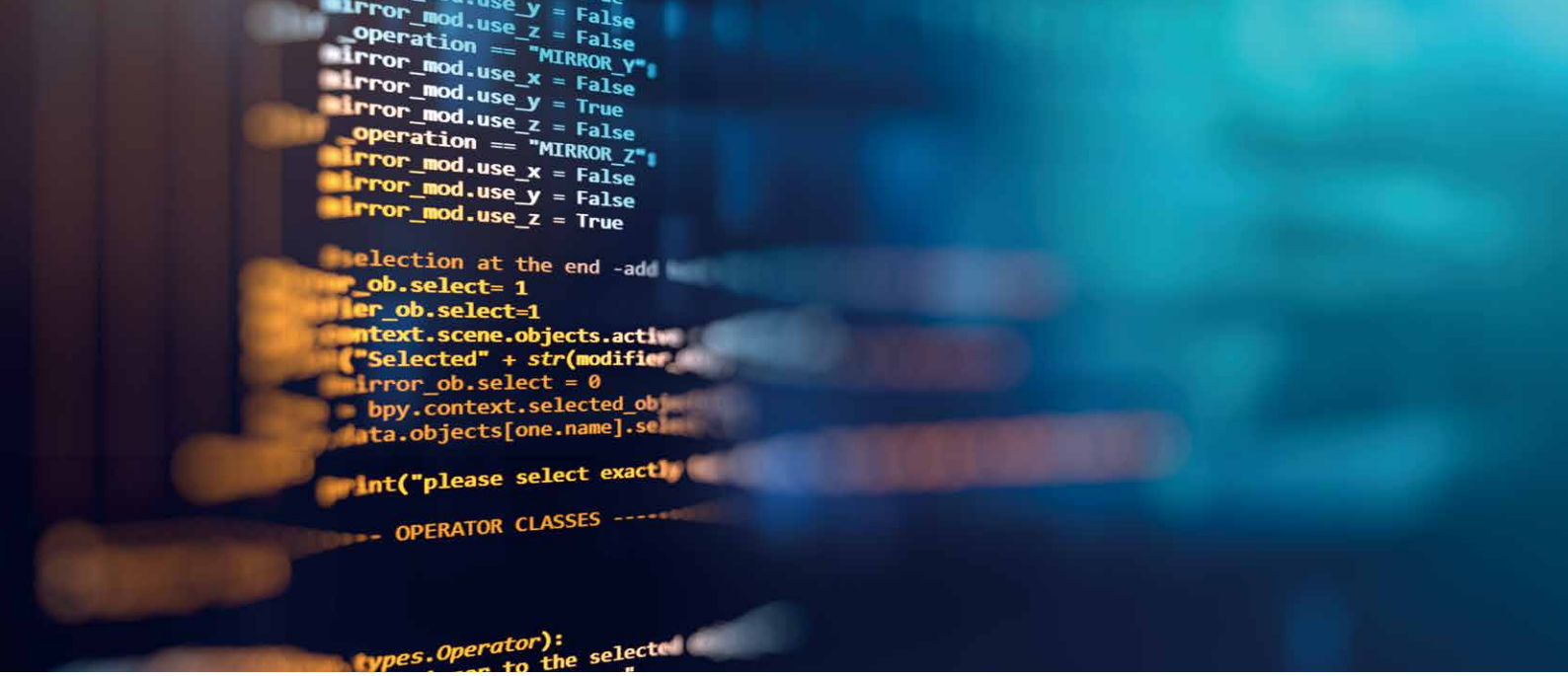
[1] https://www.ipa.go.jp/security/10threats/ps6vr7000000avp5-att/000099785.pdf

## 1.2 Scope of this study

In this study, we examined initiatives aimed at countering cybersecurity risks at primary entry points (third parties) as well as at fourth and subsequent parties, based on the anticipated supply chain patterns shown in the following figure. The targets of this study were experts engaged in cybersecurity initiatives at financial institutions.

**Supply chain risk management (SCRM)**



# 2 Trends in supply chain risk management regulations and guidelines at overseas financial institutions

Concerns about supply chain cyber risks are also on the rise at financial institutions, and in October 2022, the G7 Cyber Expert Group (CEG)[2] published an updated version of its policy paper 'G7 Fundamental Elements for third party cyber risk management in the financial sector'[3]. Various countries and regions are also implementing measures regarding the management of cyber risks in the supply chains of financial institutions. In this chapter, we introduce legal regulations and guidelines regarding supply chain cyber risks at financial institutions of the G7 countries, along with the EU and Singapore, which are pursuing advanced initiatives.

## 2.1 G7

- **The G7 Fundamental Elements for third party cyber risk management in the financial sector**

As the financial authorities of various countries and regions pursue a wide range of initiatives regarding cybersecurity, the G7 has established its Cyber Expert Group (CEG). In October 2022, the CEG updated the G7 Fundamental Elements for third party cyber risk management in the financial sector (hereinafter, the Fundamental Elements) that it originally published in 2018, focusing on overall ICT supply chain management not limited to third parties. The document defines third parties and ICT supply chains as follows.

| | |
|---|---|
| Third parties | Third-party relationships (…) are any business relationships or contracts between an entity and an organisation to provide a product or service, regardless of the organisation being an intra-group company or an external provider. |
| ICT supply chain | The ICT supply chain (…) comprises the interconnected web of third parties that form the ICT ecosystem that an entity uses in supporting its business. The ICT supply chain also contains all products, services, and infrastructure, as well as their providers, suppliers or manufacturers. |

[2] https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group
[3] https://www.fsa.go.jp/inter/etc/20221021/thirdparty_fe.pdf

The Fundamental Elements point out that, through the use of third party ICT services, financial institutions are increasing their potential for financial service innovations and are concentrating on their core business operations while also efficiently managing IT expenditures. However, due to the increase in the scale of use and complexity of such services, it has become increasingly difficult for financial institutions to understand, measure and mitigate cyber risks. In the updated Fundamental Elements, a new fundamental element (Element 7) has been added to the previous six to call attention to the increasingly important role of third parties in the financial sector. The document says that institutions and third parties can use these fundamental elements as part of their cyber risk management toolkit. An outline of the seven fundamental elements is provided below.

### Element 1: Governance

Financial institutions' governing bodies, such as their board of directors and senior management, are ultimately responsible and accountable for overseeing and implementing the management of the institutions' cyber risks, including those posed by its third-party relationships. This oversight and implementation includes:

- A documented strategy addressing reliance on third parties;
- Third party and cyber risk policies;
- Setting a risk tolerance for third-party relationships;
- Clear roles, responsibilities and accountabilities for third-party cyber risk management; and
- The establishment of appropriate communication and escalation processes as a normal course of business at all levels within the entity, and between the entity, the third party and relevant authorities.

### Element 2: Risk Management Process for Third-Party Cyber Risk

Financial institutions should identify, assess, monitor and report to the appropriate level of management the cyber risks associated with any third parties, and should have an effective process for managing third-party cyber risks through the entire third-party risk management life cycle. Specific recommendations for assessment, monitoring and reporting are as follows:

- Identify the criticality of all third parties and record this information in a list.
- Further assessment, using a risk-based approach, of ICT supply chains related to third parties is recommended (for example, obtaining a list of software libraries that comprise any software not strictly related to the relevant third party relationship (e.g. open source software [OSS)).
- Assess and manage any potential cyber risks and vulnerabilities that a third party or the ICT supply chain may introduce to the operating environment.
- Conduct cyber risk assessment prior to contractual agreements and during the lifespan of the third-party engagement.
- Structure contracts in consideration of any cyber risks stemming from subcontracting and the ICT supply chain.
- Report events in the ICT supply chain that could negatively affect the cyber risk profile of the third party.
- Perform rigorous and frequent monitoring according to the materiality of risks.

### Element 3: Incident Response

Financial institutions should establish incident response plans that include critical third parties and, where possible, the incident response plan should be used among institutions, third parties and relevant partners.

### Element 4: Contingency Planning and Exit Strategies

Institutions should have appropriate contingency plans and exit strategies in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber risks outside the entity's risk appetite, including responses by the entity itself and the transfer of operations to other third parties.

### Element 5: Monitoring for Potential Systemic Risks

Where multiple institutions use common third parties, third-party cyber risks could have systemic implications. . These potentially systemic risks should be identified and assessed so that they can be managed.

### Element 6: Cross-sector Coordination

Cyber risks associated with third-party dependencies across sectors should be identified and managed across those sectors.

### Element 7: Third Parties to the Financial Sector

Third parties that enter into contractual relationships with financial institutions should support those institutions in identifying, assessing, monitoring and mitigating cyber risks and in complying with relevant risk management requirements. Third parties are also encouraged to use these Fundamental Elements to address third party risks emanating from their respective third parties in the ICT supply chain.

## 2.2. Europe

### EU

- **The Digital Operational Resilience Act (DORA)[4]**

This is a new regulation in the EU concerning the digital operational resilience of the financial sector, and financial institutions with headquarters within the EU are required to be compliant with it by the beginning of 2025. The regulation focuses on the following five core pillars. With regard to 'ICT third-party risk', the Act includes requirements for monitoring subcontractor risks and considering the risks of re-entrustment, matters for attention when entering into agreements, and other factors related to the strengthening of the management of risks arising from third parties.

- ICT risk management
- ICT-related incident reporting
- Digital operational resilience testing
- ICT third-party risk
- Information sharing

### The European Union Agency for Cybersecurity (ENISA)

- **Threat Landscape for Supply Chain Attacks[5]**

This is a report compiling the current threat status based on the results of an analysis of 24 supply chain attacks identified over the period from January 2020 to July 2021. The report explains the methods used in the attacks and the assets targeted on both the supplier and customer side in each incident, and sums up the state of affairs. In addition, the report provides some recommedations for customers and suppliers, aimed at mitigating the risks of supply chain attacks.

## 2.3 US

In the US, Executive Order (EO)14025, issued in May 2021 with the aim of improving national cybersecurity, included requirements for the strengthening of software supply chains, and the relevant organisations are taking measures in response.

### National Institute of Standards and Technology (NIST)

- **NIST Special Publication, NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[6]**

This publication provides guidance to organisations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organisations. It integrates cybersecurity supply chain risk management (C-SCRM) into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services. The first version was published in 2015, and the first revised version in May 2022, based on EO14028. In the revised version, the scope was widened to include institutions acquiring products, software and services, as well as end users, and the primary measures that should be taken when organisations manage cybersecurity risk within their supply chains and across the whole supply chain were provided.

- **Cybersecurity Framework[7]**

The first version of the Framework for Improving Critical Infrastructure Cybersecurity (hereinafter, the 'Cybersecurity Framework') was published in 2014 as a framework for owners and operators of critical infrastructure, to help them voluntarily manage cybersecurity risks. The Cybersecurity Framework categorises the five Functions of Identify, Protect, Detect, Respond and Recover, and provides countermeasures and referential information. In Version 1.1 released in 2018, the importance of SCRM was added, with an explanation about how it is possible to use the framework to communicate cybersecurity requirements among supply chain stakeholders and requirements regarding purchasing decisions. The Concept Paper[8] published as a precursor to the creation of the Cybersecurity Framework 2.0 sets forth a policy which more strongly emphasises the importance of cybersecurity supply chain risk management.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=EN
[5] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
[7] https://www.nist.gov/cyberframework/framework
[8] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

## US Department of the Treasury

- **The Financial Services Sector's Adoption of Cloud Services**[9]

This document is a report compiling the potential benefits and challenges associated with the increased adoption of cloud services by financial institutions. It clarifies the current state of cloud adoption in the financial sector, and contains a framework that can be referred to and practised when adopting cloud services. In addition, it cites the following six challenges associated with the financial sector's use of cloud services.

- Insufficient transparency to support due diligence and monitoring by financial institutions
- Gaps in human capital and tools to securely deploy cloud services
- Exposure to potential operational incidents, including incidents originating at a cloud service provider (CSP)
- Potential impact of market concentration in cloud service offerings on the financial sector's resilience
- Dynamics in contract negotiation given market concentration of CSPs
- International landscape and regulatory fragmentation

The US Department of the Treasury established the inter-agency Cloud Services Steering Group to monitor and deal with the above challenges, and explains that it will cooperate with private sector financial institutions and related bodies in other countries to implement the following:

- Promoting closer domestic cooperation among US regulators on cloud services;
- Conducting tabletop exercises with CSPs and financial institutions;
- Reviewing sector-wide incident protocols in light of growing reliance on cloud services;
- Considering ways to appropriately measure cloud service dependencies across the sector and assessing systemic concentration and related risks on a sector-wide basis; and
- Identifying ways to foster effective risk management practices in the financial services industry.

## Federal Financial Institutions Examination Council (FFIEC)

- **Outsourcing Technology Services**[10]

This booklet provides guidance that explains the risks associated with the increase of outsourcing by financial institutions, establishes a risk management process to be used when financial institutions implement third-party outsourcing and shows the examination procedures for assessing the effectiveness of the process, based on laws and regulations and guidance from the relevant authorities.

[9] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
[10] https://ithandbook.ffiec.gov/media/pqtfvxxq/ffiec_itbooklet_outsourcingtechnologyservices.pdf

## 2.4 UK

One unique characteristic of the UK is that financial institutions have direct auditing rights concerning risk management not only with regard to the third parties with whom they directly enter into agreement with, but also with regard to fourth and subsequent parties to whom business is sub-outsourced.

### National Cyber Security Centre (NCSC)

- **Supply chain security guidance**[11]

This guidance was created to improve awareness of supply chain security and support the continuous implementation of risk management. It provides an explanation of 12 principles across the four sections of 'understand the risks', 'establish control', 'check your arrangements' and 'continuous improvement'. In addition, the guidance provides explanations based on case studies of attacks on supply chains. It should be noted that this guidance is also useful in compliance with the EU General Data Protection Regulation (GDPR).

### Prudential Regulation Authority (PRA)

- **Outsourcing and third party risk management**[12]

This Supervisory Statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations of how PRA-regulated firms should comply with regulatory requirements and expectations relating to outsourcing and third party risk management. With regard to the outsourcing of business to the service providers of third parties, it explains what requires implementation at each phase, namely: 'governance and record keeping', 'pre-outsourcing phase', 'outsourcing agreements', 'data security', 'access, audit and information rights', 'sub-outsourcing' and 'business continuity and exit planning'. In the 'sub-outsourcing' phase, the SS details the following matters to help financial institutions to judge whether or not sub-outsourcing is feasible. With regard to the sub-contractor and sub-outsourcing:

- Financial institutions should assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement;
- Financial institutions should request service providers to maintain up-to-date lists of their sub-outsourced service providers, and the institutions themselves should also ascertain this information;
- Sub-outsourced service providers should undertake to observe all applicable laws, regulatory requirements and contractual obligations;
- Sub-outsourced service providers should undertake to grant the financial institutions equivalent contractual access, audit and information rights to those granted to the service provider; and
- If the proposed material sub-outsourcing could have significant adverse effects on a material outsourcing arrangement or would lead to a substantive increase of risk, financial institutions should exercise their right to object to the material sub-outsourcing and/or terminate the contract.

## 2.5 Singapore

One unique characteristic of Singapore is that the government's guidance includes indications regarding the possibility of country risks regarding overseas business subcontracting based on the status of other nations, as well as specific mentions of matters requiring careful consideration.

### Monetary Authority of Singapore (MAS)

- **GUIDELINES ON OUTSOURCING**[13]

These are a set of guidelines regarding outsourcing by financial institutions, formulated with the objective of securing stability and security in the provision of financial services. Chapter 5 of the guidelines ('Risk Management Practices') explains the responsibilities of the board and senior management, assessment of risks, outsourcing agreements and other matters that need to be implemented in each phase of business outsourcing. Chapter 5, Section 10 ('Outsourcing Outside Singapore'), in particular, provides guidance on the following points when outsourcing business to a service provider outside of Singapore:

- Government policies;
- Political, social and economic conditions;
- Legal and regulatory developments in the target country; and
- The entity's ability to effectively monitor the service provider and execute its business continuity management plans and exit strategy.

[11] https://www.ncsc.gov.uk/collection/supply-chain-security

[12] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343

[13] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf

# 3 Examples of advanced initiatives and recommendations

In this chapter, we examine the elements of the advanced initiatives that we learned about during our interviews with experts that can be incorporated at domestic organisations, and provided our recommendations below. It should be noted that this chapter is not intended to provide an all-encompassing account of best practices, but is intended for use as a reference guide containing suggestions to be considered in accordance with your organisation's objectives.

## 3.1 Security risk assessment: Selection phase

This section assumes the assessment of potential contractors by using publicly available information.

| | |
|---|---|
| **Initiatives** | • When assessing security risks through the analysis of publicly available information, use assessment results obtained by external services for items for which such results can be used, in order to make the entire assessment process more efficient.<br>• Refer to any cybersecurity-related certifications each potential subcontractor has obtained. |
| **Recommen-dations** | **Assessment items and methods**<br>When evaluating the security risk of companies for the purpose of selecting subcontractors, collect and analyse publicly available information as well as checking any relevant cybersecurity-related certifications, and assess the security risk of each company. By using external security risk evaluation services where possible, the efficiency of the assessment process can be improved.<br><br>**Points to consider when evaluating security through the analysis of publicly available information**<br>The evaluation results that can obtained by analysing publicly available information are but one aspect showing the state of a company's security, and gaps or deviations may exist between such results and the actual situation. It therefore crucial that you keep such potential deviations in mind when using these evaluation results. |

## 3.2 Security risk assessment: Contracting phase

**Initiatives**

- Include personnel who are well-versed in security technology on teams that assesses subcontractors and external services.
- In addition to criteria-based assessment items, incorporate related assessments in accordance with trending threat scenarios.
- Use automated assessment tools where possible, according to the target and contents of the assessment.
- Where necessary, submit evidence and review the subcontractor's site.
- Check the subcontractor's methods for managing sub-outsourced services, and where necessary require evidence of the security assessment of sub-outsourced services.
- Anticipate situations in which incidents occur or are suspected to have occurred, and stipulate the scope of the subcontractor's responsibility and reporting time limits in the SLA.
- For systems with particularly high risk levels, stipulate the ability to conduct frequent assessments when entering into an agreement.

**Recommen-dations**

**Assessment team**

When entering into an agreement, the inclusion of technical members who are well-informed about the security of systems, along with regular procurement members, on the team evaluating the subcontractor, you can define security conditions more efficiently at the contracting phase.

**Assessment content**

In addition to assessment items corresponding to the usual general standards, it is essential to conduct an analysis specifically with trending threats in mind and to assess scenarios based on that analysis. Particularly in cases involving increasingly complex supply chains, it is becoming increasingly important to refer to actual attack precedents, anticipate the occurrence of similar attacks on your own company, and evaluate and take countermeasures accordingly. Note, as well, that for items where the security conditions are not satisfied it is crucial to ascertain the facts and manage them as residual risks.

**Subjects and scope of assessments**

We recommend that, according to the level of risk, you make on-site visits to the subcontractors to check the situation at the actual site. For important systems, we also recommend requiring not only subcontractors, but also any sub-outsourced services to provide evidence, and assessing that evidence as well.

**Responding to vulnerabilities and incidents**

We recommend concluding an SLA that specifically sets forth response measures to be taken when vulnerabilities are found or incidents occur at the subcontractor. The SLA should require reporting within a certain time frame after an incident is detected, and should stipulate matters such as the scope of responsibility of the subcontractor and the initial response time for inquiries.

**Review of requirements and termination of agreements**

The assessment of a subcontractor is accurate only at the time that it is made, and circumstances will naturally change over time. We therefore recommend that the ability to make assessments on a frequent basis, such as the ability to review high-risk level systems once every quarter, is included in the agreement. We also recommend that the agreement allows for the option of terminating the agreement in the event that security is threatened.

## 3.3 Risk management at subcontractors

**Initiatives**

- Determine the frequency of assessments based on the importance of each system, and make sure that high-risk systems are frequently assessed. When performing these assessments, incorporate assessments based on scenarios with new attack patterns.
- For subcontractors using high-risk systems, make on-site visits to their business sites to perform checks.
- Obtain information from the subcontractors about penetration tests (pen test) schedules, vulnerabilities and patch application periods. Where necessary, obtain the permission of the subcontractor and implement penetration testing on their website.
- When operations are sub-outsourced, demand that the subcontractor implement security management of the sub-outsourced service. If any further sub-outsourcing is conducted, request that all sub-outsourced services implement security management of the same level as that required by your company.
- When making large-scale releases in a cloud environment, obtain permission and conduct penetration testing.

**Recommendations**

**Determining management methods according to risk level**

When managing subcontractor risks, we recommend ranking subcontractors by level of importance, according to the related system services, and that security assessments are conducted with contents and frequency that are appropriate for each level. In high-risk cases, also consider making on-site checks at the subcontractor's business sites and gaining their permission to conduct penetration tests of the sites. Especially for routine security management, you can increase efficiency through the use of tools.

**Residual risk management**

We recommend formulating a prioritised improvement plan in accordance with the level of residual risks, and conducting regular reviews to reduce the risk levels to a tolerable level.

**Management of sub-outsourced services and beyond**

With regard to the security of fourth and subsequent parties that provide sub-outsourced services, we recommend managing each service in a way that ensures that each service adheres to the same criteria imposed on subcontractors. In high-risk cases, we also recommend requiring and checking evidence of the implementation of measures where necessary.

## 3.4 Software management

**Initiatives**

- Implement central control of source codes in a repository.
- Strictly implement software configuration management (SCM) through the introduction of products and other means to manage vulnerabilities. Also consider the use of SBOMs.
- When implementing software, conduct security based on threat scenarios.
- Use tools to manage open source software (OSS), and rationalise software selection decisions and identification of dependencies.
- When selecting software, including OSS, create indicators by combining third party assessments and research into the state of usage by other businesses.

**Recommendations**

**Asset management and configuration management**

Source codes should be managed centrally in your company's repository. We also recommend considering the use of multiple analytical tools for scanning, as this can help to effectively ensure security.

With regard to SCM, in the US in particular, management is typically conducted using SBOMs provided by subcontractors. However, it can often be difficult in practice to obtain all of the necessary SBOMs from the fourth and subsequent parties that provide sub-outsourced services. For this reason, we recommend first using SBOMs in areas where such use is possible. Asset management and configuration management are complex tasks, but they are essential in executing vulnerability management. If an SBOM is provided by a subcontractor, it essential that your company use and comprehensively and continuously manage the SBOM in-house. We also recommend installing management software to improve visibility and efficiency.

**OSS management**

The use of OSS management tools can reduce the burden of policy management and dependency identification when selecting OSS.

**Selection**

Our discussions with experts show that when selecting software, whether OSS or commercial, some institutions use not only third-party assessments, but also the statues of use of such software at other companies in the same industry and other large businesses as one indicator for their decision. Information obtained through inter-company connections can also be used as an indicator for reference.

## 3.5 Hardware management

**Initiatives**

- Conduct thorough asset management, and develop a system that enables firmware to be promptly updated.
- Conduct security tests based on threat scenarios.
- If you procure hardware from other countries or legal jurisdictions, check for soundness from perspectives including the source companies' security. Also be sure to check the latest legal regulations, including sanctions, and implement an appropriate response.

**Recommen-dations**

**Asset management**

Our discussions with experts show that even major organisations that conduct meticulous management are struggling with implementing asset management that is thorough enough to cover every device. Institutions must be thorough in their day-to-day asset management, and have in place a system that enables firmware to be updated promptly. As with software asset management, it is essential that institutions implement management software, improve visibility and efficiency, and continuously implement asset management.

**Tests**

For critical equipment, we recommend performing security tests based on hardware threat scenarios in conjunction with normal acceptance tests.

**Observance of regulations**

When procuring hardware from outside Japan, you will need to confirm the security regulations with which the procurement source complies, as well as their security reliability, and also observe import regulations. You will also need to stay abreast of the latest trends such as legal regulations corresponding to the state of society.

## 3.6 Reporting to senior management

**Initiatives**

- Although senior management is becoming increasingly aware of supply chain cybersecurity risks related to the control and management of subcontractors, it is important to organise and report the total costs of the impacts upon business, profits, customer satisfaction, business reputation and customer loyalty by using easy-to-understand business language.
- Because the optimal reporting routes for reporting cybersecurity risks to senior management differ from one organisation to another, consider reporting routes that are appropriate for your organisation based on factors such as risk, monetary cost and IT. When doing so, take steps to ensure no conflict of interest arises between the CIO and CISO.

**Recommen-dations**

**Effective reporting process**

Although in Europe and the US many members of senior management undergo technical training, and an increasing number of board members are well-versed in cybersecurity as a whole, including supply chain risks, we recommend that companies continue to compile and make reports using simple, clear and non-technical business language.

**Reporting routes**

Our interviews with experts revealed that financial institutions are currently trying out various reporting routes for reporting to senior management about cybersecurity risks including supply chain risks, in an effort to find the optimal route. Possible reporting routes include reporting via the CISO to the CRO, via the CISO to the CIO, and via the CISO to the COO. We recommend that you consider the best reporting path for your own organisation's operations that prevents any conflict of interest between promoting IT and ensuring security.

## 3.7 Matters to note when entering into agreements

When an institution contracts a subcontractor to implement cybersecurity measures, problems may arise under the Antimonopoly Act and the Subcontract Act, depending on the details of the contracted operations and the methods used. In October 2022, in a document entitled 'Towards the Creation of Partnerships among Business Partners for the Improvement of the Cybersecurity of the Entire Supply Chain'[14], the Japan Fair Trade Commission compiled its views on supporting and making requests to business partners as three key points. PwC's recommendations regarding these three points are as follows.

### Unilateral price-setting

Demanding that subcontractors implement cybersecurity measures without reasonably factoring in the accompanying increase in cost increment may raise problems under the Antimonopoly Act.

**Recommendations**

A problem may arise, for example, if no additional payment is made to a subcontractor despite the fact that they have implemented additional security measures that you have asked them to take due to the impact of new vulnerabilities and threats that were discovered after the conclusion of the agreement. We recommend making the decision to review security demands on a half-yearly or quarterly basis, entering into agreements that encompass the feasible workload during emergencies before such an emergency occurs, and establishing a practicable system for flexibly responding in the event that new threats emerge.

### Demands on subcontractors to bear the burden of security measure costs

A problem may arise under the Subcontract Act if a company demands that a subcontractor bear all or some of the cost burden associated with security measures without providing any evidence of the basis for the calculation of such costs, thereby placing the subcontractor at a disadvantage. In addition, in transactions that fall under the scope of the Subcontract Act, if a company unjustly harms the interests of the subcontractor by causing the subcontractor to provide cash or services, this is regarded as unjustly demanding provision of economic gains under the Subcontract Act.

**Recommendations**

If a contract with a subcontractor is unclear regarding the details of support to be provided in the event of a cyber incident and/or demands that the subcontractor provide excessive support for the incident, this may be a problem under the Subcontract Act. It is important that the agreement clearly states forth the support that is to be provided. We also recommend that reasonable terms of service, such as the business hours during which the subcontractor must be available to handle enquiries and the maximum number of hours engineers can spend providing emergency support, be clearly stipulated, and that the agreement be concluded through the agreement of both parties.

### Compulsory purchase or use of products or services

If a company requires a subcontractor to purchase specific products or to use specific services designated by the company in the implementation of cybersecurity measures, this may present a violation of Antimonopoly Act. If a company requires a subcontractor to purchase designated goods or to use designated services for transactions subject to the regulation of the Subcontract Act, this could also present a violation of the Subcontract Act (requiring the subcontractor to purchase designated goods or to use designated services).

**Recommendations**

A company may impose specific security requirements upon its subcontractors if the scope and requirements are clearly set forth, both parties agree to the terms, and the necessary costs are paid by the company. In recent years, it has become common practice for companies to lend their own devices and issue virtual desktop service accounts to those carrying out the outsourced work at their subcontractors, thereby providing environments in which the security requirements can be met even under remote working conditions. Some companies also provide an area within their own environment, where the necessary security conditions are met, that can be accessed by other companies, and grant access rights to that area to those who are to perform the outsourced work.

As these recommendations show, the relationships between financial institutions and subcontractors will ideally involve the overlapping of flexible measures, consisting not only of pre-determined security requirements, but also additional demands and incident responses corresponding to the social situation. Budgets for organisational security also need to be prepared in an adaptable form. We recommend that security officers and other stakeholders at both the contracting company and their subcontractors, as well as others in decision-making positions, regularly communicate with each other and create a relationship in which they can reach a shared understanding of any issues.

[14] https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

# 4 Conclusion

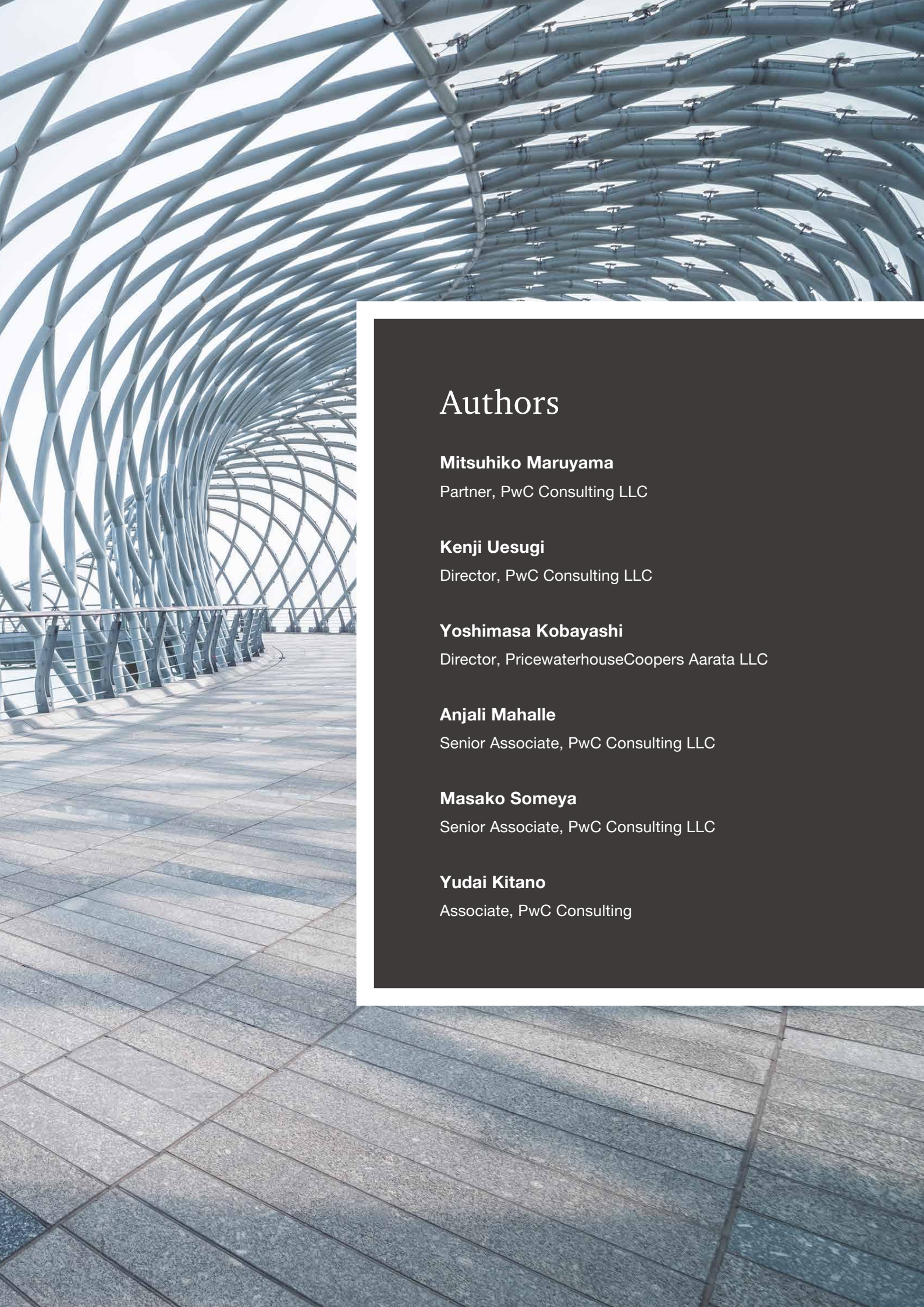
In this study we investigated advanced cases through interviews with cybersecurity experts at overseas financial institutions, and examined elements that could be incorporated by Japanese financial institutions with a view toward strengthening their supply chain risk management.

In Chapter 1, we organised anticipated cyber risks in the supply chain and defined the scope of the study.

In Chapter 2, we provided an introduction to the regulations and guidelines related to supply chain cybersecurity for financial institutions in the G7 countries, the EU,and Singapore.

In Chapter 3, we compiled some examples of advanced initiatives from our interviews with cybersecurity experts at overseas financial institutions, and compiled as recommendations the elements that we believe could be incorporated by Japanese financial institutions. Furthermore, based on documents published by the Japan Fair Trade Commission, we set out various recommendations concerning points that could prove to be problematic in legal terms when financial institutions enter into agreements with subcontractors.

Cyber attackers are continuously carrying out attacks through the exploitation of supply chains, and various nations, regions and organisations are pursuing initiatives to improve cybersecurity in the supply chain. Because we can predict ongoing changes, new releases of governmental guidelines and progress in companies' initiatives in the future, it is vital that financial institutions keep abreast of threat trends and promote the adoption of effective countermeasures while cooperating with other organisations.



# Authors


**Mitsuhiko Maruyama**
Partner, PwC Consulting LLC

**Kenji Uesugi**
Director, PwC Consulting LLC

**Yoshimasa Kobayashi**
Director, PricewaterhouseCoopers Aarata LLC

**Anjali Mahalle**
Senior Associate, PwC Consulting LLC

**Masako Someya**
Senior Associate, PwC Consulting LLC

**Yudai Kitano**
Associate, PwC Consulting

# Contact us

**PwC Japan Group**
https://www.pwc.com/jp/en/contact.html

## www.pwc.com/jp/en

The PwC Japan Group is a collective name for the member firms of the PwC global network in Japan and their affiliates. Each firm within the PwC Japan Group conducts its business as a separate, independent business entity.
In response to our clients' increasingly complex and diverse corporate management issues, the PwC Japan Group has put in place a system that consolidates our knowledge in the fields of auditing and assurance, consulting, deal advisory, tax and legal services, and encourages organic collaboration among our professionals in each field. As a professional services network with approximately 11,500 certified public accountants, tax accountants, lawyers and other professional staff, we strive to provide services that more accurately address our clients' needs.
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services.

Published: September 2023 Control No: I202307-03