Japanese financial institutions to strengthen risk resilience through compliance with new economic security law

21 November 2023

Special Edition

Iakyara vol.378

Nomura Research Institute, Ltd.

Introduction

The post-Lehman contagion of the late 2000s was a wakeup call on the importance of systemic risk. Since then, regulators have been pushing financial institutions to identify and mitigate all types of risks that could impact them individually.

In Japan, for example, IT risk has become a key focus of risk management because system failures can severely disrupt financial services' availability. The scope of risk management has recently broadened to encompass misconduct in addition to human error as Japanese financial institutions have started to place more priority on not only compliance but also conduct risk.

With cybersecurity risks growing incessantly and geopolitical risks also escalating, financial regulators globally are stressing the importance of operational resilience. The spring, Japan's FSA published a discussion paper that highlighted cyber resilience, a framework to mitigate the impact of cyberattacks and ensure swift restoration of any disrupted services.

Against such a backdrop, Japan enacted its Economic Security Promotion Act (ESPA) in May 2022. Under the ESPA, Japan aims to ensure economic security by implementing economic policies through a combination of incentives and regulations. The first of the ESPA's four planks, ensuring stable supplies of key goods, is primarily incentive-based while the second, ensuring stable availability of Critical infrastructure services, relies mostly on regulations. This report offers pointers on ESPA compliance, focusing mainly on the second plank given the magnitude of its prospective impact on the financial sector.

In the interview that follows, attorney Hideaki Umetsu, a partner at Mori Hamada & Matsumoto, offers guidance on navigating the advance review process that is a core element of the ESPA's second

plank. Chapter 1 then provides an overview of the second plank as a whole. Chapter 2 delves deeper into the second plank's details vis-à-vis system development in particular. Chapter 3 discusses operating resilience through a forward-looking lens. Lastly, Chapter 4 presents an overview of economic security developments globally with an emphasis on Europe and the US.

We hope you find this report to be of value in your activities to ensure stable availability of financial services.

Masaaki Yamazaki

Senior Managing Director
Financial Technology Solution Division
October 2023

Special interview

How financial institutions should prepare before ESPA requirements for infrastructure providers take effect

Following the Economic Security Promotion Act's enactment in May 2022, its program for ensuring stable availability of key infrastructure services is being fleshed out in the form of policies and guidelines with the help of a panel of experts. With less than a year now remaining until the program goes live, NRI's Jun Tsutsumi spoke with Hideaki Umetsu, a partner at Mori Hamada & Matsumoto, about how financial institutions should prepare and points to keep in mind (interview date: July 6, 2023).

Hideaki Umetsu

Partner
Mori Hamada & Matsumoto

Licensed to practice law in Japan since 2004. Earned LLM degree from University of Chicago Law School in 2009. Admitted to New York State bar in 2010. Member of Japan Federation of Bar Associations' International Activities and Strategy Committee since 2021 and former co-chair of International Bar Association's Asia Pacific Regional Forum (2021-22). Practice areas include advising Japanese companies on cross-border M&A, overseas expansion, governance and compliance, international trade law and business human rights.

Jun Tsutsumi

General Manager
Financial IT Risk Management Department
Nomura Research Institute

Joined NRI in 1991. Initially worked on developing trading systems for securities brokerages. Involved in core system redevelopment project for Japanese investment bank's local subsidiary while on assignment at NRI Europe from 1996 to 2000. Seconded to Nomura Securities from 2003 to 2006. Returned to NRI from 2006 in risk management/IT governance consultant role. Appointed to current position in April 2023 after serving as general manager of ERM Business Planning.

Progress since ESPA's enactment

Jun Tsutsumi: How has implementation of the Economic Security Promotion Act (ESPA) been progressing since its passage in May 2022?

Hideaki Umetsu: The ESPA comprises four planks. The first involves strengthening supply chains for designated key goods. The second pertains to ensuring stable availability of key infrastructure. The third and fourth are respectively about developing advanced critical technologies through public-private cooperation and withholding certain patents from publication.

The ESPA seeks to achieve its aims through a combination of incentives and mandates. The incentives are being implemented first, with the first and third planks' provisions taking effect in August 2022. The government is now moving forward with the second and fourth planks' implementation. Its Expert Council on ESPA is likewise prioritizing the first and third planks over the second and fourth in its work. The government will issue guidelines for each of the four planks in the same chronological order.

JT: The plank that will be most impactful for financial institutions is the infrastructure one, guidelines for which were approved by the Cabinet in late April. Could you explain how the guidelines fit into the bigger picture?

HU: The guidelines articulate the basics as a precursor to detailed rulemaking. The guidelines for key infrastructure, titled *Ensuring Stable Availability of Designated Critical Infrastructure by Preventing Designated Disruptive Acts*, cover matters such as the definition of a designated critical infrastructure provider, designation criteria, the process of detailed rulemaking on designated disruptive acts and the basic design of the prior review process.

Regarding designated critical infrastructure providers, the guidelines say that companies will be designated based on their scale of operations or the availability of alternatives to their infrastructure. Because the guidelines present the government's basic approach, they do not quantify the scale-of-operations criteria in concrete terms but forthcoming detailed rules will. The other criteria are based on whether substitutable infrastructure is available from other providers.

Additionally, the government will abide by two principles when designating critical

infrastructure providers. The first is don't impede fair competition. The second is to treat SMEs more carefully than larger companies when making designation decisions.

In the case of banks, for example, the scale-of-operations criteria for designation as a ciritical infrastructure provider are ¥10trn or more of deposits or 10mn or more accounts or 10,000 or more ATMs. However, the guidelines say that designation isn't automatic for companies that meet the designation criteria. They instruct the minister with regulatory authority over the company in question to take into account other relevant considerations, such as the condition of the company's infrastructure and facts about the company's services. So a company may not be designated as a critical infrastructure provider even if it meets all the criteria. In such cases, the guidelines recommend that the minister explain why the company was not designated.

JT: What is the implementation timeline going forward?

HU: The Expert Council is fleshing out the details now. Since immediately after its June 12 meeting through mid-July, public comments are being solicited on a Cabinet Ordinance prescribing detailed provisions on designated critical infrastructure and on ministerial ordinances specifying designation criteria for designated critical infrastructure providers and standards for defining designated key infrastructure. The second phase of solicitation of public comments and other various FAQs are slated to be released this autumn. The program to ensure stable availability of key infrastructure is currently scheduled to be up and running in spring 2024.

Framework for prior review of key infrastructure

JT: How will the prior review process work?

HU: When a designated critical infrastructure provider plans to install designated key facilities or outsource key maintenance or management functions to a third party, it must submit its plans to the government to be reviewed beforehand. The government is currently deciding what should be contained in these installation/

outsourcing plans, including how much information to require on suppliers or, in the case of outsourcing of key maintenance or management functions, third-party OSPs (outsourcing service providers) and sub-OSPs. Submission of the plan will be the trigger that initiates the review process.

Once the plan has been submitted, the government will generally have 30 days from the date of receipt to complete its review. The review period may be extended to a maximum of four months under certain circumstances. However, the ministries that will review installation/outsourcing plans are set up help desks to interface with plan filers before they start accepting plan submissions.

JT: What if an installation/outsourcing plan doesn't pass the review?

HU: If, upon review, a plan is rejected or flagged for revision, its filer will have 10 days to notify the government of how it plans to proceed.

JT: I assume the Expert Council has extensively discussed the installation/outsourcing plans to be submitted for prior review. What is its position?

HU: The specifics of installation/outsourcing plans' required content will be dictated by ministerial ordinances, drafts of which are slated to be released this autumn or thereabouts. But information on the plans' content has been released in dribs and drabs. We know, for example, that plans to newly install designated key facilities must include the supplier or third-party OSP's name, address and domicile country. Other such corporate information required to be disclosed may be of concern to the companies involved. Examples include the names, nationalities and percentages of voting rights owned by parties that own a 5% or greater voting interest in a supplier of designated key facilities; and the names, birthdates and nationalities of suppliers and third-party OSPs' board members. Additionally, if over the preceding three years a supplier or third-party OSP derived 25% or more of its gross revenues from a foreign government entity, the definition of which includes state-owned institutions in addition to national and subnational governments, the installation plan must disclose the identity of the foreign government, the share of the supplier's revenues it accounted for and the country/region in which the key designated facilities will be manufactured.

In sum, installation/outsourcing plans must provide information for assessing suppliers' susceptibility to foreign influence. The same disclosure requirements will apply to parties to which key maintenance or management functions are outsourced.

JT: Information such as the nationalities of board members and shareholders could be regarded as sensitive information. One big question is whether suppliers and third-party OSPs would even be able to agree to disclose shareholders' nationalities.

HU: Board members and shareholders pose different issues, so let's distinguish between the two. And in terms of board members, we have to distinguish between infrastructure suppliers- and sub-suppliers' officers.

First, infrastructure providers normally should be able to disclose information on their own officers. They should also be able to disclose to the Japanese government information on suppliers' officers with those individuals' consent, at least if the supplier is a Japanese company. In such cases, I believe some legal arrangement could be worked out, at least under Japan's Personal Information Protection Act. Of course, a person's nationality could be highly sensitive information in some instances. Given such a possibility, disclosure of nationality information to Japanese government authorities must be strictly limited to a need-to-know basis.

JT: What about shareholders?

HU: Privately held companies generally have stock transferability restrictions in their articles of incorporation. In such cases, changes in share ownership must be approved by the company's Board of Directors. Privately held companies are therefore able to track changes in shareholder registries and readily identify shareholders owning 5% or more of their shares.

Publicly traded companies are a different story. It's essentially impossible to tell who owns 5% or more of a publicly traded company at a given moment. Normally, shareholder registries are definitively updated only as of record dates, the most common of which in Japan is March 31 for companies that hold annual shareholder general meetings in June. With the exception of record dates, publicly traded companies' shareholder registries are in a constant state of flux throughout

the year.

Additionally, what if a shareholder accumulates a large stake in a company, nominates a slate of directors via a shareholder proposal and the nominees are elected? The company may not know much about the new directors' backgrounds. It may not be privy to their nationalities. Such a scenario isn't outside the realm of possibility.

I think the 5% level is probably meaningful. The government's responses to public comments revealed that when the government chose 5% ownership as the ESPA's disclosure threshold, it took into consideration other similar disclosure thresholds. Its choice was likely influenced by the Large Shareholding Report, which shareholders are required file once they have accumulated a 5% stake. However, the 5% threshold differs in two minor respects between the ESPA and the Large Shareholding Report. First, the threshold is "5% or more" for the former versus "more than 5%" for the latter. Second, co-owned shares are counted toward the threshold for the latter but we do not know the details of counting yet for the former. We'll find out whether these two 5% thresholds really align with each other when more details are released.

JT: I was thinking along the same lines.

HU: The ESPA's requirement to report large shareholders' nationalities differs in intent from the Large Shareholding Report, the purpose of which isn't to identify foreign shareholders. Assuming shareholders can be identified, the next question is how their nationality information will be obtained.

When the shareholder in question is a company, its nationality is the country under whose laws it was established, which can usually be ascertained with reasonable certainty from publicly available information. However, when the shareholder is an individual or a company incorporated in a country without public incorporation records, the shareholder's nationality may not be ascertainable from documentation alone. But even in such cases, I personally think you may be able find some other way to ascertain nationality. For example, Japan's Broadcasting Act, Telecommunications Business Act and Civil Aeronautics Act contain restrictions on foreign ownership. Japanese broadcasters are prohibited from appointing foreigners to certain senior roles. Such regulations can indirectly shed light on nationality. So there are ways to determine board members and

shareholders' nationalities. However, there may very well be cases in which nationality cannot be feasibly ascertained.

If so, to what extent will the government permit nationality disclosures to be omitted when a party's nationality is unknown to the filer? In other words, how will the government respond when an installation/outsourcing plan is filed with "unknown" in the "nationality" field? Whether plans with such omissions can successfully get through the review process remains to be seen.

JT: Under the ESPA's risk management provisions, vendors will have to contractually agree to provide certain information to their financial institution customers. I guess such clauses would contain exceptions or limitations.

HU: I would expect any such promises to say the vendor will provide information to the extent possible, legally or otherwise. If information isn't available after every legal means to obtain it has been exhausted, I don't see what else the filer could do except fill in "unknown."

JT: I agree. Just because a contract requires information to be provided, it doesn't give you license to break the law to obtain the information.

HU: I believe a contract that held you in breach if you didn't resort to illegal means to obtain information would be unenforceable. Ultimately, I think what we're talking about here ultimately hinges on two questions. First, is the information legitimately accessible? Second, did you exhaust every means to obtain it? Retain proof that, for example, you contacted shareholders to ascertain their nationality. Explore other potential options such as providing indirect information.

JT: When dealing with nationality information, compliance with the Personal Information Protection Act is of course essential.

HU: Which in practical terms basically means obtaining the consent of the party in question. I don't think there's any way to legally compel someone to furnish personal information against their will.

Information that parties disclose to comply with the ESPA will be obtained on the

condition it will be shared with the government within the parameters set by the ESPA for the purpose of submitting an installation/outsourcing plan. As long as the party to which the information pertains has consented, disclosing that information to the government would basically never constitute an illegal third-party disclosure. But even if consent were not obtained for some reason, I expect certain reasons to perhaps be made exceptions under the Personal Information Protection Act.

Overseas laws, however, are trickier to navigate. If you have consent, I think you most likely would not run into any problems just about anywhere, but you might in a few countries. You would need to be careful to comply with each country's laws, including rules about what to do when you don't have consent or when previously given consent has been retracted.

JT: It's quite a minefield.

HU: Another important point is that even though the Japanese government is requiring disclosure of nationality, it claims it doesn't intend to discriminate based on nationality. In one of its responses to public comments, the government emphasized that nationality will be just one consideration in its review process and it won't reject any installation/outsourcing plans based solely on nationality.

Non-ESPA news

JT: Aside from the ESPA, what else is happening in the economic security space?

HU: Security clearances, initially reported to perhaps be included in the ESPA, are now under discussion by the Japanese government. It has assembled a panel of experts to work on an economic security clearance system. The panel released an interim report in June and there have been media reports of forthcoming legislation.

The Foreign Exchange and Foreign Trade Act (FEFTA) regulates both trade in goods and investment flows, the former of which encompasses imports and exports of data and technology in addition to physical goods. One recent development on the trade front is semiconductor export restrictions. Previously,

the Japanese government had been controlling exports to restrict access to weapons and goods used in weapons of mass destruction as a party to the Wassenaar Arrangement [on Export Controls for Conventional Arms and Dual-Use Goods and Technologies] within an international regime with many other participants . The new semiconductor export restrictions were adopted outside of this regime in coordination with certain allies, including the US and Netherlands.

Another recent development is human-rights-based export controls. In March 2023, Japan announced it has endorsed the Export Controls and Human Rights Initiative (ECHRI) Code of Conduct. The US-led ECHRI was launched in December 2021 with only a few subscribing states, the number of which has since increased to 24 as of March. While the ECHRI incorporates a human rights perspective into export controls, the FEFTA is based on a national-security export control framework that basically seeks to ensure a peaceful and safe international society. The new semiconductor export controls were likewise adopted in the aim of preventing diversion to military use. With human rights now a justification for export controls, I think the question of how to maintain policy coherence will have to be addressed.

The ESPA's first plank deals with designated key goods, which are to be added to the core sectors that are subject to investment controls under the FEFTA. This is as example of how linkages between ESPA and FEFTA are starting to emerge in what I view as an important portent of what the future holds.

JT: Is the US the driving force behind these recent developments?

HU: I think the US is indeed playing a central role in both human-rights-based and semiconductor export controls. The US regulates its IT and telecom sectors quite stringently. It seems to be waiting to see if other countries follow suit. Europe sometimes follows the US's lead and sometimes doesn't. Overall, I feel the US, Europe and Japan are increasingly harmonizing their policies.

JT: Thank you for sharing your expertise with us again[1]. You have reinforced my view that companies won't be able to comply with the ESPA on time unless they start preparing before the forthcoming ordinances are released.

NOTE

1) See https://www.nri.com/en/knowledge/publication/fis/lakyara/lst/2022/07/03 for the previous interview.

	ESPA implementation timeline
2022	May 11 Economic Security Promotion Act (ESPA) enacted (promulgated May 18)
	September 30 *Basic Policies on Promoting Economic Security Through Integrated Economic Policymaking* approved by Cabinet
	September 30 *Basic Guidelines on Ensuring Stable Supplies* (1st plank) and *Basic Guidelines on Designated Critical Technology R&D* (3rd plank) approved by Cabinet
2023	April 28 *Basic Guidelines on Designated Critical Infrastructure Services* (2nd plank) and *Basic Guidelines on Withholding Patent Applications from Publication* (4th plank) approved by Cabinet
	June 12 *Presentation on Implementation* released at 7th meeting of Expert Council on ESPA
Summer	June 15 FSA solicits public comments on Cabinet Office Ordinance on designation criteria for designated critical infrastructure providers and designated key facilities
	August 9 Cabinet Office Ordinance promulgated by FSA
	FSA to solicit public comments on Cabinet Office Ordinance/announcement on content of installation/outsourcing plans and designation of designated critical infrastructure providers
Autumn	Cabinet Office Ordinance/ announcement to be finalized by FSA
	Technical documentation to be prepared/released (timing TBD) FAQs, guidelines
2024 Spring	ESPA to fully take effect Installation/outsourcing plans must be filed when: • Key facilities are to be installed • Key maintenance or management functions are to be outsourced (including unmodified renewals of existing outsourcing arrangements) • Functional changes are to be made (policy on minor changes to be announced in autumn or thereafter)

Chapter 1

Overview of compliance with Japan's Economic Security Promotion Act in financial sector

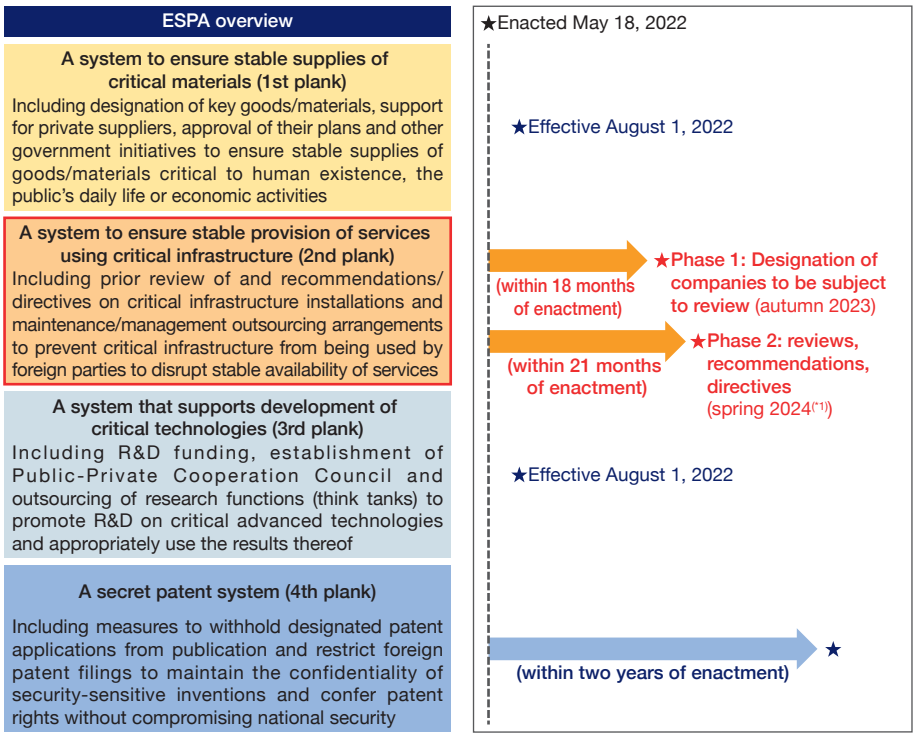
Economic Security Promotion Act: overview and timeline

Japan's Economic Security Promotion Act[1] (ESPA), enacted in May 2022, is being phased into effect since August 2022. It aims to effectively implement a comprehensive suite of economic policies to ensure Japan's national security from an economic standpoint in light of today's increasingly complex international landscape and recent changes in societal and economic structures.

The ESPA designates financial services, alongside, e.g., electric and gas utilities,

NOTE
1) The ESPA's official title is *Act for the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures.*

Exhibit 1-1: ESPA overview and timeline



*1: Designated infrastructure providers will be granted six months from their date of designation to comply
Source: NRI, based on information from Japan Cabinet Office website

as critical infrastructure for economic activities and the public's daily life. The ESPA comprises four planks, all of which involve the private sector. Its second plank is a system to ensure stable provision of services using critical infrastructure[2]. The second plank imposes detailed requirements on companies within its purview. The government is slated to designate the companies to be subject to these requirements this autumn and begin vetting their plans next spring. Given such a short timeline, the designated companies will have to prepare in advance to comply with the ESPA on time[3] (Exhibit 1-1).

While the companies to be subject to the ESPA's second plank will be limited to a subset selected largely based on their scale of operations, the government wants all providers of key services, irrespective of size, to ensure stable availability of the services[4]. Within the financial sector, many of the companies that will not be directly subject to ESPA oversight should still thoroughly familiarize themselves with the ESPA's second plank. The following is a brief overview of the second plank and recommendations for the financial sector based on guidelines[5] approved by the Cabinet on April 28, 2023, (the "Cabinet Guidelines") and a recent presentation[6] on the second plank's implementation.

ESPA second-plank requirements

The purpose of the ESPA's second plank is to protect infrastructure foundational to economic activities and the public's daily life from the threat of state-backed cyberattacks. Outside of Japan, infrastructure that has fallen prey to cyberattacks in recent years includes Ukraine's power grid (2015), a US oil pipeline and logistic companies, mainly in Europe. Some such attacks are backed by foreign governments. Amid the growing threat posed by organized, sophisticated cyberattacks, ensuring infrastructure's security and reliability is becoming an increasingly important element of Japan's national security. The ESPA's second-plank requirements can be summed up as follows.

Designated critical infrastructure providers must obtain the approval of the Cabinet minister with regulatory authority over their industry before installing designated key facilities involved in providing services related to designated critical infrastructure or outsourcing key maintenance or management functions for such facilities.

2) "Designated critical infrastructure services" are defined as services that are foundational to the public's daily life and economic activities and have security implications, meaning that disruptions to their stable availability could be detrimental to national security or public safety. Fourteen sectors are within the purview of the ESPA's second plank: electric utilities, gas utilities, petroleum, water utilities, railways, trucking, seaborne shipping, aviation, airports, telecommunications, broadcasting, postal services, financial services and credit cards. For brevity, "key services" (or simply "services") is used synonymously with "designated critical infrastructure services" herein.

3) As an interim measure, designated critical infrastructure providers will be granted a six-month preparatory period from their designation date, but in light of the review process's requirements, they will likely need to start preparing even before being officially designated.

4) The Cabinet Guidelines (5(1)) state, "It is advisable for all providers of designated critical infrastructure, even ones that are not designated critical infrastructure providers, to ensure stable availability of their designated critical infrastructure services. All providers, including SMEs, play an important role in stably providing designated critical infrastructure services. In light of such, the Prime Minister and ministers with authority over industries within the purview of the ESPA's second plank will provide appropriate information to a wide range of parties involved in supplying infrastructure facilities, including parties that do not meet the designation criteria.

5) *Basic Guidelines for Ensuring Stable Availability of Designated Critical Infrastructure by Preventing Designated Disruptive Acts* (approved by Cabinet April 28, 2023).

6) *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023).

Exhibit 1-2: Designated critical infrastructure provider designation criteria

[Scale of operations]

Designation	Designation criteria (trailing 3FY averages)	Designated key facilities	Key maintenance or management functions
Banks	• Deposits: ≥¥10trn or • Accounts: ≥10mn or • ATMs: ≥10,000	Deposit/EFT systems	• System maintenance • System operation
Money transmitters	• Users: ≥10mn and • Transactions: ≥¥400bn/yr	EFT systems	
Insurers	[Licensed life insurers] • Claims paid(*1): ≥¥1trn or • Policies: ≥20mn [Licensed non-life insurers] • Direct claims paid: ≥¥1trn or • Policies: ≥20mn	Claim payment systems	
Type-I financial instrument business operators	• Custodial assets: ≥¥30trn or • Accounts: ≥5mn	Order execution systems	
Trust companies	• Trust assets(*2): ≥¥300trn	Asset management systems	
Third-party prepaid payment instrument issuers	• Issuance: ≥¥1trn/yr and • Network: ≥10,000 merchants	Systems involved in prepaid payment instrument issuance	
Comprehensive credit purchase intermediaries	• Cardholders: ≥10mn and • Transactions: ≥¥4trn/yr	Systems involved in credit card payment authorization	

[Availability of alternatives]

Designation	Designation criteria	Designated key facilities	Key maintenance or management functions
Cooperative financial institutions	Parties engaged in cooperative financial institutions	Deposit/EFT systems	• System maintenance • System operation
Exchanges and financial instrument market operators	Parties that operate exchanges and other financial instrument markets(*3)	Trading systems	
Financial instrument clearinghouses	Licensed or otherwise authorized parties	Settlement systems	
Interbank clearinghouses	Licensed parties	Interbank settlement systems	
Businesses conducting operations specified in Article 34 of Deposit Insurance Act	Parties engaged in said operations	Systems used in resolution process	
Businesses conducting operations specified in Article 34 of Agricultural and Fishing Cooperatives Savings Insurance Act	Parties engaged in said operations		
EFT services	Designated parties	EFT systems	
Electronic monetary claim recorders	Designated parties(*4)	Electronic monetary claim recording systems	

*1: Excluding refunds of policies' cash surrender value, other refunds and reinsurance premiums
*2: Excluding re-entrusted assets
*3: Excluding parties with annual marketable securities trading volumes of less than ¥75trn over the most recent three fiscal years
*4: Excluding parties with custody of electronically recorded claims totaling less than ¥1trn over the most recent three fiscal years
Source: *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023) and *Cabinet Office Ordinance on Designation of Designated Critical Infrastructure Providers Pursuant to ESPA* (August 9, 2023)

"Designated critical infrastructure providers" are companies selected from the standpoint of either scale of operations (e.g., banks, insurers, securities broker/dealers, trust companies) or availability of alternatives (e.g., securities exchanges, payment infrastructure providers). The designation criteria for financial infrastructure providers are tabulated in Exhibit 1-2. The designation criteria based on scale of operations[7] were set in the aim of ensuring that designated providers collectively account for over 50% of the domestic market for the services in question.

7) *Cabinet Office Ordinance on Designation of Designated Critical Infrastructure Providers Pursuant to ESPA* (August 9, 2023).

"Designated key facilities" means key hardware, software and other facilities used to provide key services. In the financial sector, the term refers to information systems that play a core role in providing services. The ESPA seeks to prevent disruptive acts such as planting viruses in such systems or maliciously divulging information on hardware vulnerabilities. Such acts committed by parties outside of Japan to disrupt the stable availability of services related to designated critical infrastructure are termed **"designated disruptive acts"** in the ESPA.

"Key maintenance or management functions" means maintenance, management or operation of designated key facilities, including maintenance inspections, replacement of hardware/parts and software upgrades. In the financial sector, these functions correspond to IT system maintenance and operation. When such functions are outsourced, the ESPA will require safeguards against designated disruptive acts committed in connection with the outsourcing arrangement.

Prior review: scope

The ESPA will require designated critical infrastructure providers to provide advance notice of plans to install designated key facilities or outsource key maintenance or management functions. The plans will be reviewed to ascertain:

- whether they were inordinately influenced by any external entity,
- whether the provider has conducted a risk assessment and implemented risk management controls,
- whether any vulnerabilities in the facilities' constituent components, deficiencies

in maintenance or management or non-compliance with Japanese laws/regulations or international standards have been identified, and

- whether any concerns relevant to the plan have been raised by governments allied or otherwise aligned with Japan.

If the review finds that the designated key facilities pose a material risk of being used to perpetrate designated disruptive acts, the minister with regulatory authority over the provider may issue recommendations and/or directives. Even in the absence of such a material risk, if international conditions or other circumstances subsequently change, said minister may likewise advise or require the provider to take action in response.

The Cabinet Guidelines state that reviews conducted to assess the risk of disruptive acts perpetrated from outside Japan must carefully investigate whether vendors supplying facilities to be installed are inordinately influenced by foreign entities. The Cabinet Guidelines instruct ministries to be cognizant that Japan is now facing the most adverse and complex security environment in its postwar history, as evidenced by its National Security Strategy. However, the ESPA's second plank does not permit blacklisting. How thoroughly the government will investigate inordinate influence by foreign entities remains to be seen. During the review process, designated critical infrastructure providers should place priority on demonstrating that their risk management, discussed below, includes adequate safeguards against designated disruptive acts.

Prior review: notification content

The proposed content of plans that must be filed for the prior review process is shown in Exhibit 1-3. To assess the magnitude of any foreign influence, the plans are required to provide information on vendors involved in installation, maintenance and/or management of designated key facilities, including the names of any intermediaries between the manufacturer and the designated critical infrastructure provider and the names and addresses of suppliers of the facilities' constituent components in addition to information on the components themselves.

For key maintenance or management functions, the plans must include information on any outsourcing, including sub-outsourcing, arrangements. While

Exhibit 1-3: Proposed content of plans subject to ministerial approval

	Designated key facilities	Key maintenance or management functions
(1) Description of facilities	• **Facilities' type, name, function(s) and installation/usage location(s)**	–
(2) Plan content and timeline	• **Purpose** of installation, **names of companies** involved in supplying/installing designated key facilities(*1) • **Timeline** (scheduled completion dates of design, development, assembly, installation and commissioning into service)	• **Description** of key maintenance or management functions, their **purpose** and **location(s) where performed** • Outsourcing arrangement's **date(s) or date range** (depending on whether one-off, recurring, continuous, etc.) • **Information on any sub-OSPs**(*2)
(3) Information on supplier(s)/OSP(s) (as specified in applicable ministerial ordinance)	• Suppliers/OSPs' **names, addresses and countries of origin** • Information on parties directly owning **5% or more of voting rights** (**name, nationality, % of voting rights owned, etc.**) • Supplier/OSP **officers' names, DOBs and nationalities** • **Identity** of and **share** of revenue derived from **any foreign government**(*3) **that accounted for ≥25% of supplier/OSP's total revenues** over past 3 years	
	• **Country/region** where facilities are to be manufactured	• **Information on any sub-OSPs**(*4)
(4) Information on facilities' constituent components (as specified in applicable ministerial ordinance)	• **Description** of constituent component(*5): **type, name, function(s), etc.** • Constituent component **suppliers'**(*6) **names, addresses, etc.**	–
(5) Information on effective controls	• **Information on risk management regimes** (see Exhibit 1-4)	

*1: Including any intermediaries (e.g., if facilities are purchased from a supplier through a distributor, information on the distributor must be reported)
*2: Up to and including the final (n^{th}) sub-OSP in any outsourcing chain (per Expert Council's June 2023 presentation)
*3: Defined to include not only foreign governments but foreign government institutions, foreign subnational public entities, foreign central banks and foreign political parties or other political organizations
*4: Up to and including the final (n^{th}) sub-OSP in any outsourcing chain (per Expert Council's June 2023 presentation)
*5: Any of the facilities' constituent hardware or software that could be used as a means of committing designated disruptive acts
*6: Including suppliers that supply constituent components as part of a larger assembly (per Expert Council's June 2023 presentation)
Source: *Basic Guidelines for Ensuring Stable Availability of Designated Critical Infrastructure by Preventing Designated Disruptive Acts* (approved by Cabinet April 28, 2023) and *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023)

Japan's FSA has long required disclosure of this information, the ESPA will require the information to be disclosed in more detail. Vendor information required to be disclosed includes matters that vendors may deem sensitive, including 5+% shareholders' nationalities, board members' nationalities and dates of birth, foreign governments with which the vendor does business and the vendor's share of revenue derived from foreign governments[8] (Exhibit 1-3 (3)). Given the possibility of resistance to disclosing such sensitive information to customers, the ESPA allows vendors to submit the information directly to the Japanese government.

8) See the accompanying interview of Hideaki Umetsu for more information.

Prior review: risk management

Because designated critical infrastructure providers can effectively prevent designated disruptive acts by assessing and mitigating the risk of such acts, their risk management also will be reviewed during the prior review process. The review's risk management checklist consists of nine checkpoints collectively comprising a total of 28 more detailed checkpoints (Exhibit 1-4).

In addition to reporting on compliance with the 28 detailed checkpoints on a risk management report form (Exhibit 1-5), designated critical infrastructure providers will also have to attach supporting documentation. Additionally, they will have the option of disclosing their risk-management initiatives not included on the checklist. Based on such information, the prior review process will presumably place priority on assessing the substance and actual state of designated critical infrastructure providers' risk management.

The risk management checkpoints are discussed below in comparison with current IT/cybersecurity risk management regimes.

Prevention of unauthorized changes (checkpoints 1 and 4)

The first and fourth of the nine major checkpoints pertain to preventing unauthorized and unintentional changes. The first one mainly concerns manufacturing processes. For designated critical infrastructure providers in the financial sector ("financial infrastructure providers"), designated key facilities will be IT systems that play a core role in providing services. Financial infrastructure providers' process analogous to manufacturing is system development. While financial infrastructure providers adequately verify quality through testing in their current system development processes, they may not place much priority on detecting and removing malicious code (detailed checkpoint 1). Such malware can be dealt with using source code analysis tools. Source code inspections can detect serious security risks, dangerous software vulnerabilities and bugs likely to cause buffer overflows[9] or memory leaks[10], all of which can be inimical to stable system availability[11].

The fourth major checkpoint pertains to system operation and maintenance. The operational controls mentioned in detailed checkpoint 14 have already been rigorously implemented by many financial infrastructure providers. In the case of

9) Buffer overflows occur when data input to a memory buffer exceeds the buffer's capacity, resulting in an error or other malfunction.

10) A memory leak is a reduction in available memory that occurs because the programmer forgot to release memory allocated to a program once the memory is no longer needed. Memory leaks can detract from system performance or cause malfunctions.

11) See Chapter 2 below for more information.

Exhibit 1-4: Risk management

Risk management of installations of designated key facilities	
1	**Contractually or otherwise ensure that designated critical infrastructure providers have controls necessary to prevent unauthorized changes to designated key facilities and their constituent components during their manufacture.** (1) Check software for malicious code (set up testing (e.g., acceptance inspection) regime, do vulnerability testing before installation). (2) Check compliance with information security requirements (apply security patches, update anti-malware software). (3) Establish quality assurance program. (4) Regularly check for unauthorized changes in manufacturing process. (5) Check physical/logical controls in manufacturing environment. (6) Check policies for preventing unauthorized access via Internet. (7) Check safeguards against unauthorized changes to facility installations. (8) Verify suppliers' cooperation with in-depth investigations and on-site inspections if unauthorized changes or indications thereof are discovered.
2	**If designated key facilities or their constituent components are expected to require future maintenance/servicing, select suppliers taking into account whether such maintenance/servicing is available from the suppliers only or from third parties also.** (9) Check suppliers' service warranties. (10) Investigate alternatives if maintenance/servicing becomes unavailable from supplier.
3	**Implement controls to detect signs of malicious interference with designated key facilities and their constituent components and implement safeguards (e.g., redundancy) to prevent service interruptions in the event of malicious disruption.** (11) Take precautions against service interruptions due to cyber (e.g., ransomware) attacks (e.g., data backups and remote storage thereof, service restoration procedures, switchover to alternate facilities). (12) Establish information security incident (e.g., data leak) response team/policies (e.g., manual, periodic drills). (13) Implement access controls and unauthorized-access monitoring.
Risk management of outsourcing of key maintenance or management functions	
4	**Contractually or otherwise ensure that when outsourcing key maintenance or management functions (including when the functions are wholly or partially sub-outsourced; likewise below), designated critical infrastructure providers have controls necessary to prevent unauthorized changes to designated key facilities by both OSPs (including sub-OSPs) and their employees and are able to verify the specifics of said controls.** (14) Establish procedures for storing and monitoring system logs, task histories and other records; check for unauthorized acts at set intervals or as warranted. (15) Periodically apply latest security patches and otherwise keep assets up to date. (16) Physically/logically restrict access to design documents and other information on facilities. (17) Physically/logically restrict access of anyone other than designated operational staff. (18) Maintain/improve cybersecurity literacy through education/training.
5	**When key maintenance or management functions are sub-outsourced, contractually or otherwise ensure that information required to monitor sub-OSPs' cybersecurity compliance is available to the designated critical infrastructure provider through the primary OSPs and that sub-outsourcing arrangements are subject to the designated critical infrastructure provider's advance approval.** (19) Ensure designated critical infrastructure provider has right to approve sub-outsourcing arrangements and has knowledge of all sub-OSPs in outsourcing chain. (20) Verify that any sub-OSPs' cybersecurity defenses are equivalent to primary OSP's.
6	**Verify there is no material risk of key maintenance or management functions being interrupted or permanently halted by an OSP's contractual nonperformance.** (21) Verify OSPs' operational stability (e.g., business plans, condition of assets, track record)
Risk management required to check suppliers/OSPs' compliance regimes	
7	**Verify designated key facilities suppliers, constituent component suppliers and OSPs' (including sub-OSPs') current and past state of compliance with Japanese laws and regulations, internationally accepted standards, etc.** (22) Verify suppliers have not violated applicable Japanese laws/regulations or internationally accepted standards in past 3 years. (23) Verify OSPs have not violated applicable Japanese laws/regulations or internationally accepted standards in past 3 years.
8	**Verify that fitness for purpose of to-be-supplied designated key facilities and their constituent components or outsourced (including sub-outsourced) key maintenance or management functions will not be influenced by a foreign country's legal environment.** (24) Contractually or otherwise ensure that suppliers report any potential contractual violations due to a foreign country's legal environment or an external entity's directive. (25) Contractually or otherwise ensure that OSPs report any potential contractual violations due to a foreign country's legal environment or an external entity's directive. (26) If devices that capture visual information (e.g., security cameras, drones) are installed or used, verify that appropriate handling of said information is free from foreign/external influence.
9	**Contractually or otherwise ensure that the designated critical infrastructure provider has access to information that enables it to determine if suppliers of designated key facilities or their constituent components and OSPs (including sub-OSPs) are subject to any influences from outside Japan. Also contractually or otherwise ensure that the designated critical infrastructure provider is promptly informed if said information changes after a contract has been signed.** (27) Contractually or otherwise ensure access to information on suppliers and OSPs' names, addresses, executive officers, finances, business plans, operational performance, manufacturing sites, outsourced-service performance sites, involved employees' qualifications (e.g., information security credentials/training histories), etc. (28) Contractually or otherwise ensure receipt of timely updates on any changes to information covered by checkpoint 27.

Note: Detailed checkpoints 1-28 have been edited for brevity.
Source: *Basic Guidelines for Ensuring Stable Availability of Designated Critical Infrastructure by Preventing Designated Disruptive Acts* (approved by Cabinet April 28, 2023) and *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023)

Exhibit 1-5: Risk management report form

(Reference) Risk management checkbox form

Checkpoints	Checkbox	Notes
Designated critical infrastructure provider affirms that it(*1) or its supplier of designated key facilities has set up a testing regime inclusive of acceptance inspections to verify that said facilities contain no malicious code, etc., and that it will conduct vulnerability testing prior to said facilities' installation.	☑	If arrangements other than those specified in (1-1) have been made, please disclose them.

*1: Including cases where a party other than the designated critical infrastructure provider or designated key facilities supplier performed the verification during the facilities' pre-installation testing phase.
Note: Risk management attestations pertaining to sensitive matters may be submitted directly to the Cabinet minister with authority over the industry in question rather than via the designated critical infrastructure provider.
Source: Excerpted from *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023)

shared-use IT services, direct verification of checkpoint 14 may not be feasible for a variety of reasons, including that system logs contain another financial service provider's information. Financial infrastructure providers may need to explore alternative verification or reporting methods.

Additionally, to manage information used for system maintenance in compliance with detailed checkpoints 3, 4, 5 and 16, financial infrastructure providers will have to set up a system development environment with built-in controls, specifically including physical controls on access to certain rooms, logical controls on access to the development environment and air-gapping of development-use terminals. Although such controls are standard in a live system environment, requiring similar controls in development environments does not yet seem common. To cohesively implement such controls, system development operations could conceivably be confined to a single environment (e.g., one with minimum required functionality/ authority) set up and managed by a supplier or other third party.

Cyber resilience (checkpoint 3)

The third major checkpoint requires financial infrastructure providers to detect signs of cybersecurity breaches and build redundancy into their IT systems. Detection of signs of cybersecurity breaches pertains to cybersecurity measures' sufficiency and fitness for purpose. Such detection capabilities have to be continually upgraded in light of domestic and overseas developments and in sync with existing cyber defenses.

Redundancy, by contrast, goes a step beyond existing cyber defenses in that it has to incorporate a business-continuity perspective. Cybersecurity's cardinal

principle is to minimize harm. Some readers have likely taken part in drills to learn to swiftly and appropriately decide whether to shut down a service to minimize harm under hypothetical cyberattack scenarios.

Business continuity planning in the cyber realm has been garnering growing interest in recent years from a standpoint different than such harm minimization. Cyber resilience was mentioned even by Japan's FSA in an April 2023 white paper[12]. However, many Japanese financial infrastructure providers do not seem to have adequately incorporated a cyber perspective into their business continuity planning yet. As a first step, they should start by addressing discrete threats like ransomware (detailed checkpoint 11) before delving deeper into specifics[13].

12) *Discussion Paper on Ensuring Financial Resilience* (FSA, April 2023). Cyber resilience was briefly discussed in a sidebar entitled *Box 2: IT systems risk management and cyber security.*

13) See Chapter 3 below for more information.

Management of sub-OSPs (checkpoint 5)

The fifth major checkpoint pertains to oversight of sub-outsourcing service providers' (sub-OSPs') cybersecurity while detailed checkpoint 19 requires sub-OSPs to be approved by financial infrastructure providers. However, shared-use IT services used by many financial infrastructure providers may not be conducive to prior approval of sub-outsourcing arrangements by all their users. In such cases, financial infrastructure providers should diligently maintain/upgrade and functionally augment IT services while ensuring effective oversight in compliance with the fifth major checkpoint's intent. IT service providers will have to explain their sub-OSP selection criteria and oversight regime, including with respect to cybersecurity, so financial infrastructure providers can confirm from their own standpoint that the IT service providers' sub-OSP selection criteria and other controls are adequate.

Elimination of external influences (checkpoints 7, 8 and 9)

The seventh, eighth and ninth major checkpoints pertain to checking for influences from outside Japan and eliminating the risk thereof. Foreign influences are an important consideration in assessing the risk of state-backed designated disruptive acts. Information involved in this process may include sensitive information of the type mentioned above. Any such sensitive information may need to be handled with care, including how it is verified.

Vendors' role in business continuity (checkpoints 2 and 6)

Lastly, the second and sixth major checkpoints deal with the question of whether

vendors, including OSPs, are selected appropriately from a business-continuity standpoint. It should be acceptable for financial infrastructure providers to make such determinations within the context of their existing oversight regimes.

Requirements after commencement of operations/ outsourcing

Prior review is required not only for plans to install new designated key facilities and newly outsource key maintenance or management functions but also for material changes to such plans that have already been approved. Notice of the proposed change must be submitted to the minister with regulatory authority over the industry in question. The Cabinet Guidelines define “material change” as a change that could materially affect the outcome of an assessment of the risk of designated key facilities being used to commit disruptive acts. The examples cited include a change in the supplier of designated key facilities or a constituent component thereof[14)].

14) The Expert Council's presentation mentions "minor changes" that would not need to be reported. Examples of minor changes cited in the presentation included a revision or addition that does not affect operation of the functions described in an installation plan.

The ESPA does not impose any ex-post reporting duties for already installed designated key facilities and existing key maintenance or management functions outsourcing arrangements that predate the ESPA’s effective date. However, outsourcing agreement renewals, including automatic renewals, constitute commencement of a new outsourcing arrangement and accordingly require advance notice to be filed. Financial infrastructure providers must prepare in advance to file reports on already installed designated key facilities and existing key maintenance or management functions outsourcing arrangements by soon after the ESPA’s second plank’s effective date.

Changes in financial sector

Amid the adverse security environment and rising geopolitical tensions of recent years, ensuring infrastructure’s security and reliability through the ESPA’s second plank will become increasingly important to protect the public’s daily life and preserve economic and societal tranquility. Against such a backdrop, all financial services providers, not only those subject to the prior review process, will likely be expected to build out their compliance regimes based on risk management.

Meanwhile, there are concerns that such a trend toward more stringent controls could impose a heavy burden on both financial and IT services providers. The Cabinet Guidelines state that the government is committed to free and fair economic activity. The government is accordingly expected to seek to avoid unduly constraining economic activity and detracting from innovation and efficiency based on healthy competition and economic rationality. It wants companies to forge ahead with economic activities as vigorously as usual while upgrading their risk-management regimes.

The primary objective of the ESPA's second plank is to prevent designated disruptive acts and ensure the stable availability of societal infrastructure. It is crucial to avoid ineffectiveness due to compliance fatigue and a perfunctory form-over-substance approach to checklist-based risk management. The ESPA is targeted at malicious acts of aggression, not human errors and omissions that are elements of system risk. To adapt to technological progress and changes in the external environment, financial services providers should engineer their management cycles to verify individual initiatives' effectiveness and drive continuous improvement.

To both upgrade management controls and maintain if not step up economic activities in accord with the intent of the ESPA's second plank, one key issue that must be addressed is how to avoid confusion, bottlenecks and onerous management burdens due to a lack of cohesion among financial and IT service providers' separate activities. The financial sector should foster a universal consensus and move forward with ESPA compliance in unity based on that consensus.

Chapter 2

System development in financial sector today and prospectively

System development imperatives in financial sector

IT systems in the financial sector have to be highly stable, reliable and robust. Real-time processing is an absolute must for financial transactions. Even minuscule system glitches can lead to significant opportunity losses in trading.

To ensure stability, reliability and robustness, financial institutions are pursuing various quality-improvement initiatives, including multifaceted testing, in their system development processes. They are also beefing up IT security and have been since around 1990, when their systems started attracting heavy hacker traffic. Financial institutions often handle sensitive information, leaks of which undermine public trust in the financial institution at fault.

In cybersecurity, there is no silver bullet. The only option is to methodically deploy defense in depth, including precautions against vulnerabilities being built into systems during their design or development phase and operational safeguards to rapidly detect and recover from attacks. Multilayer defenses are covered in more detail in Chapter 3 below.

Pre-release vulnerability testing has become the primary approach to preventive cybersecurity in recent years. Ideally, security should be addressed at every stage of the system development lifecycle from design through software development and testing, in addition to assessing vulnerabilities before going live. Today, however, this ideal has generally been rendered unfeasible by a shortage of cybersecurity engineers and schedule constraints. In many cases, financial institutions rely on specialized vendors to assess systems' security vulnerabilities as a final step in the system development process.

ESPA raises bar in terms of cybersecurity

Cybersecurity in the financial sector has historically been focused primarily on preventing data leaks but with the enactment of Japan's Economic Security Promotion Act (ESPA) in response to growing geopolitical risks, disruptive acts perpetrated from abroad are now explicitly regarded as a risk. Japanese companies will have to place more priority on security in their system development processes. Under the ESPA, designated companies will be required to report on the status of their cybersecurity defenses in not only live systems but also development processes/programs to mitigate the risk of, e.g., malicious code be planted in the system during development (in the supply chain). Additionally, the reported cybersecurity defenses will have to be substantiated with documentation. While low-cost, short-iteration development has become popular in the wake of the digital transformation movement of recent years, system development teams still must upgrade security without sacrificing productivity.

How to comply with ESPA's risk management requirements

The ESPA's risk management requirements were fleshed out in the form of 28 concrete examples in a set of guidelines[1] approved by the Cabinet on April 28, 2023, and a subsequent presentation[2] on implementation of the second of the ESPA's four planks. Below we look at the first three of the 28 risk management controls covered by these documents. All three can be addressed by modifying the conventional approach to system development.

These documents' text on the first risk management control says that designated critical infrastructure providers shall make sure that a testing regime inclusive of acceptance inspection is set up by either themselves or their designated key facilities' supplier(s) to verify that the facilities are not infected with malicious code and that vulnerability testing is performed before the facilities are installed. These steps may be performed by either the designated critical infrastructure provider or the designated key facilities' supplier. They can be accomplished using state-of-the-art security tools available from specialist vendors. The tools enable automated vulnerability testing and can also output records of the tests, whereas a DIY approach would require the designated critical infrastructure providers to do everything from identifying checkpoints and formulating a methodology to interpreting test results.

NOTE

1) *Basic Guidelines for Ensuring Stable Availability of Designated Critical Infrastructure by Preventing Designated Disruptive Acts* (approved by Cabinet April 28, 2023).

2) *Presentation on Implementation of Program to Ensure Stable Availability of Designated Critical Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 2023).

The second risk management control is pre-installation verification that designated key facilities' supplier has met the information security requirements specified by the designated critical infrastructure provider when the facilities were ordered. The verification process may include, e.g., checking whether (1) the latest security patches have been applied to the facilities or their constituent components and (2) anti-malware software has been updated to its latest version. Automated tools are available that check for software vulnerabilities. Use of such tools should effectively identify any vulnerabilities and facilitate software patching.

The third risk management control is verification that designated key facilities' supplier had a reliable quality assurance program in place during the facilities' development process. Quality assurance can be strengthened by incorporating the tools already mentioned into the development process.

Quality assurance through Shift Left

To establish the quality assurance program required by the third risk management control, we recommend the Shift Left development model. Shift Left is applicable to the first and second risk management controls also.

The idea behind Shift Left is to detect security vulnerabilities early and prevent cost/time overruns by building cybersecurity defenses into systems earlier in the development process. Shift Left utilizes tools to perform security checks during development and testing processes instead of relying solely on pre-release vulnerability testing (Exhibit 2-1).

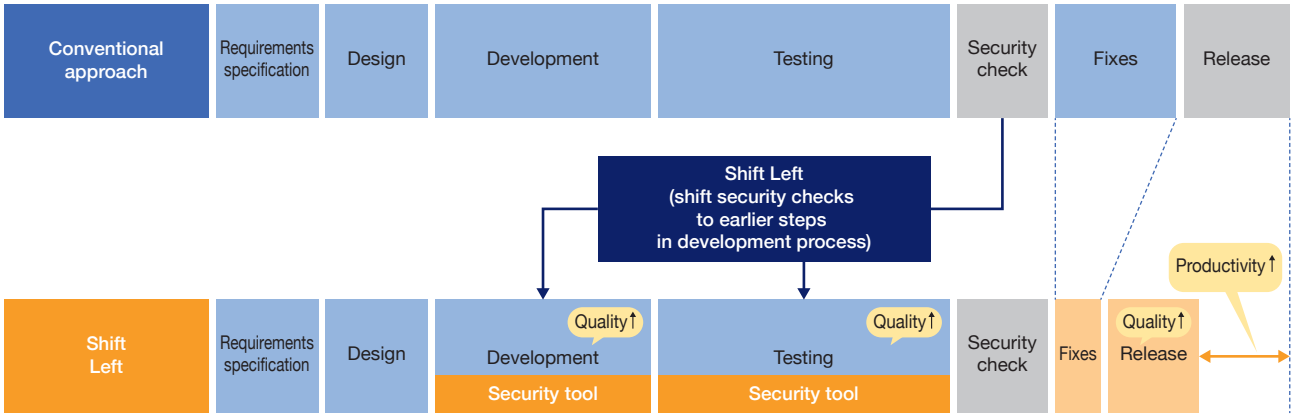
Successful deployment of Shift Left requires the following three elements, each of which is briefly explained below.

(1) Process: Establish specific workflows clarifying when, how and by whom security is implemented.

(2) Technology: Automate security checks to insource and improve the efficiency of security defenses.

(3) Culture: Foster a security culture throughout the project team or entire organization.

Exhibit 2-1: Shift Left model



Source: NRI

(1) Process

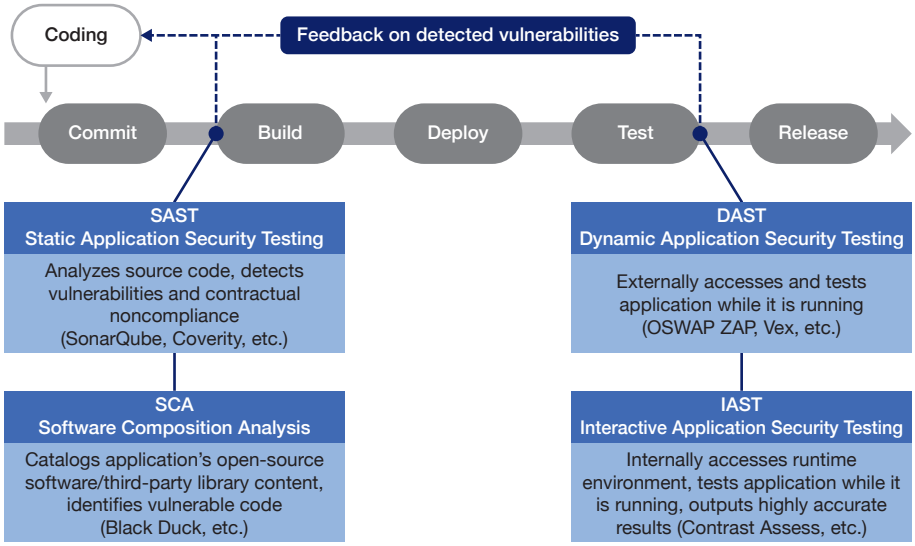
It is important for security to be built into development processes to ensure that security measures are implemented without fail during development. Before development begins, determine who will verify what when and set criteria to decide whether detected vulnerabilities require corrective action. To maximally take advantage of the security testing tools discussed below, they need to be set up to run automated tests during the development process.

Some vulnerabilities are hard to test for with tools alone. Development teams need to figure out how to iteratively improve security quality throughout the development process through such means as combining automated testing tools with design-stage vulnerability checks and pre-release manual testing.

(2) Technology

To avoid rework, select highly effective tools compatible with your development process. One such tool is static application security testing (SAST), which scans source code for security vulnerabilities in how the code is written. Because it can be deployed from the earliest phase of development, SAST effectively prevents rework. Many SAST tools check code from the standpoint of not only security but also quality. SAST can fulfill the acceptance inspection function mentioned above in connection with the first risk management control. By checking the completed source code with SAST before accepting delivery, you can determine if it contains any malicious code or other deficiencies.

Exhibit 2-2: Four types of security testing tools



Source: NRI

Another tool is software composition analysis (SCA), which checks for open-source vulnerabilities in a codebase. While SAST scans for vulnerabilities in internally developed source code, SCA checks for vulnerabilities in open-source software and third-party libraries within a codebase. SCA effectively prevents rework because it enables vulnerabilities to be rectified during development. SCA tools can also generate a software bill of materials[3], which will be required once the ESPA fully takes effect. SCA can play an effective role in both the acceptance inspections and security patching respectively mandated by the first and second risk management controls above. When SCA detects a software vulnerability, the development team can immediately decide whether to deploy a patch.

Two additional tools are dynamic application security testing (DAST) and interactive application security testing (IAST). DAST checks applications for vulnerabilities by simulating attacks on the application while it is running and observing how it responds. IAST tools detect vulnerabilities from inside an application by monitoring the application's behavior while running. While performing functional testing, they can simultaneously test for vulnerabilities. While DAST and IAST can identify vulnerabilities while an application is still in development, they are deployed later in the development process than SAST and SCA. They are consequently less effective than SAST and SCA at preventing rework. Their analyses, however, are highly accurate because they analyze applications while running. They can be used for the vulnerability testing mandated by the first risk management control

3) Software bills of materials are expected to come into widespread use in Japan, having been discussed at a February 28, 2023, meeting of the Ministry of Economy Trade and Industry's Task Force for Evaluating Software Management Methods Toward Ensuring Cyber/Physical Security.

above.

These four tools should be utilized in combination with each other. Select a combination aligned with your project's attributes in terms of budget, risks and other pertinent factors.

(3) Culture

One key prerequisite to practicing the Shift Left approach on an ongoing basis is a shared security consciousness across the development team. To get the most out of security tools, developers must understand the tools' diagnostic outputs and take bottom-up action in response thereto. However, recruiting and training cybersecurity professionals is a challenge and software developers tend to be insufficiently cognizant of security.

In light of such, we recommend appointing a security champion to assume overall responsibility for security and take the lead in fostering security consciousness. The security champion should upgrade the development team's security literacy by reviewing testing/analytical tools' outputs together development staff with and conducting training sessions to help get security novices up to speed. Such an approach should implant a security mentality within the development team. Fostering a security culture is essentially synonymous with establishing a quality assurance program as mandated by the third risk management control above.

Additional benefits of adopting Shift Left

We have discussed how to apply the Shift Left approach to a few of the risk management controls cited as examples by the government. Designated critical infrastructure providers will have to comply without fail with the ESPA's risk management requirements. Implementing the requisite controls all at once may not be feasible for some companies. In such cases, we would advise a step-by-step approach. First, adopt security assessment tools like SAST and/or SCA. Then gradually migrate to a Shift Left model by setting up processes and fostering a security culture before deploying other tools.

Potential benefits of adopting a Shift Left approach include not only compliance with the ESPA's risk management mandates but also better quality and increased

productivity. The following are two particularly promising payoffs.

- **By incorporating security checks into every step of the development process, Shift Left enables development to proceed apace while minimizing rework.**

The workload involved in fixing vulnerabilities increases at each successive stage of the development process. If a vulnerability is not discovered until the very end of development, fixing it could entail not only testing but even design modifications, depending on the nature of the vulnerability. Such rework can be avoided by practicing Shift Left. Additionally, by enabling vulnerabilities to be fixed with minimal rework, Shift Left frees up resources that can drive improvement in quality.

- **By keeping security top of mind throughout the development process, Shift Left cultivates security expertise in development staff.**

With pre-release vulnerability testing/fixing often largely outsourced to specialist vendors, in-house staff may not have enough opportunity to learn about security. By practicing Shift Left on an ongoing basis, in-house developers gain security knowledge through continual exposure to security testing tools' outputs. Such knowledge should reduce the incidence of vulnerabilities, thereby improving quality and boosting productivity.

The benefits that can be derived from Shift Left are outcomes to which every system development project should aspire. In an age of digital transformation coupled with growing geopolitical risks, Shift Left will likely become the predominant approach to system development.

Chapter 3

Cybersecurity imperatives of economic security and operational resilience

Multilayer cybersecurity required by economic security

Japan's Economic Security Promotion Act (ESPA) imposes a number of mandates with respect to cybersecurity, one of which is ensuring stable availability of designated critical infrastructure (see Chapter 1 for more details).

The ESPA requires companies designated as critical infrastructure providers subject to the ESPA's provisions to disclose the specifics of how they will manage risk when installing designated key facilities. As examples, a presentation released by a government panel[1)] listed nine risk management controls broken down into 28 more granular controls. Exhibit 3-1 provides an overview of the nine risk management controls and specific examples of how they translate to a cybersecurity context.

Implementation of these risk management controls will require anti-malware protection, vulnerability management and software tampering detection, among numerous other safeguards. Even more important, however, is the concept of multilayer defenses based on multilayer controls that extend from the design and development phases through the operational phase and also encompass third parties such as outsourcing service providers (OSPs).

In accord with such a multilayer approach, Japan's FSA has recently asked financial institutions to strengthen their operational resilience. Multilayer defenses and operational resilience have much in common from the standpoint of upgrading cybersecurity. In terms of complying with the ESPA, we believe companies would benefit from gaining a deeper understanding of operational resilience's requirements. Below we discuss how regulators in Japan and abroad are addressing operational resilience.

NOTE

1) *Presentation on Implementation of Program to Ensure Stable Availability of Designated Infrastructure Services* (Cabinet Secretariat's Expert Council on ESPA, June 12, 2023); https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai7/siryou1.pdf (in Japanese)

Exhibit 3-1: Risk management controls related to designated key facility installations and associated cybersecurity measures

	Risk management controls related to designated key facility installations	Examples of cybersecurity measures
1	Implement controls needed to prevent unauthorized changes during facilities' manufacturing process	• Controls throughout software development lifecycle • Anti-malware controls (backups, etc.) • Vulnerability management • Software tempering detection • eKYC/two-factor authentication for developers, etc.
2	Select suppliers taking into account whether maintenance/servicing of designated key facilities or their constituent components is available only from their suppliers or from others also	• Multi-vendor/alternative arrangements • Threat information collection/analysis
3	Implement controls that can detect signs of malicious interference and safeguards (e.g., redundancy) to prevent service interruptions in event of malicious disruption	• Cyber resilience upgrades • Backups/restoration arrangements in case of, e.g., ransomware attack • Cyber drills
4	Contractually or otherwise ensure that controls are in place to prevent unauthorized changes by OSPs or their employees	• Unauthorized commit monitoring • Privileged access log monitoring upgrades • Misbehavior detection • Security training
5	Contractually or otherwise ensure advance approval of sub-OSPs and access to information needed to verify sub-OSPs' cybersecurity defenses	• OSP/sub-OSP security visibility • Verification of OSPs' business continuity • More rigorous contract reviews
6	Verify there is no material risk of key maintenance/management services being interrupted or permanently halted by an OSP's contractual nonperformance	
7	Verify suppliers and OSPs' (including sub-OSPs') current and past state of compliance with Japanese laws and regulations, internationally accepted standards, etc.	• More rigorous corporate background checks for OSPs/sub-OSPs • Reviews of OSPs/sub-OSPs' legal/regulatory compliance • More rigorous contract reviews
8	Verify to-be-supplied or -outsourced (including sub-outsourced) key maintenance/management services' fitness for purpose will not be influenced by a foreign country's legal environment	
9	Contractually or otherwise ensure access to information sufficient to determine if suppliers of designated key facilities or their constituent components and OSPs (including sub-OSPs) are subject to any influences from outside Japan	

Source: NRI SecureTechnologies

Operational resilience for financial institutions globally

In April 2023, Japan's FSA published a *Discussion Paper on Ensuring Operational Resilience*. It sets forth Japan's policies in response to a global regulatory push to ensure financial institutions' operational resilience.

The FSA defines operational resilience as the ability to continue to deliver critical services at an at least minimally adequate level even in the event of a system failure, cyberattack, natural disaster or other such disruption. Operational resiliency is being discussed internationally as a framework for ensuring early restoration of

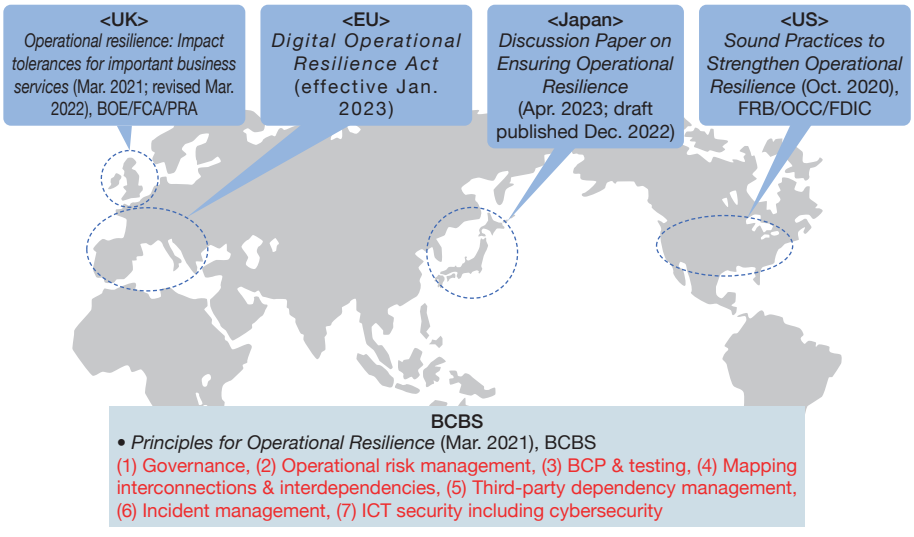
services disrupted by an unforeseen event and mitigating the disruption's impacts on the services' users.

Financial regulators around the world have published operational resilience regulations or guidelines modeled after a set of international principles formulated by the Basel Committee on Banking Supervision (BCBS) in March 2021 (Exhibit 3-2). Most notably, the EU enacted a Digital Operational Resilience Act (DORA) effective January 16, 2023. The DORA will apply from January 2025 to providers of ICT (information/communication technology) services to financial institutions physically located within the EU. It primarily requires financial institutions to manage ICT risks, including ICT third-party risk, as follows.

In terms of ICT risk management, the DORA requires financial institutions to formulate a digital resilience strategy that must:

1. establish an ICT risk tolerance level and analyze the maximum tolerable level of disruption to key services;
2. set information security objectives;
3. outline mechanisms put in place to detect ICT-related incidents;
4. implement digital operational resilience testing; and
5. devise a communication strategy in the event of ICT-related incidents warranting disclosure.

Exhibit 3-2: Operational resilience guidelines/legislation



Source: NRI SecureTechnologies, based on publicly available information

Financial institutions' senior management is charged with the responsibility of defining and approving the digital resilience strategy inclusive of the above five elements and periodically reviewing the strategy's implementation status.

Regarding ICT third-party risk, financial institutions are required to adopt and regularly review a strategy on ICT third-party risk and identify and assess third-party concentration risk. ICT third parties themselves fall within the DORA's purview. Third parties designated by a financial regulator as a critical ICT third-party service provider for financial institutions are required to be physically located within the EU if they provide ICT services to EU financial institutions (i.e., they must establish a subsidiary within the EU if they do not already have one).

In sum, the EU's approach to financial institutions' operational resilience is distinguished by statutorily mandated requirements, not directives or guidelines. Ensuring operational resilience is a key management priority for EU financial institutions.

Cyber mapping as third-party risk management tool

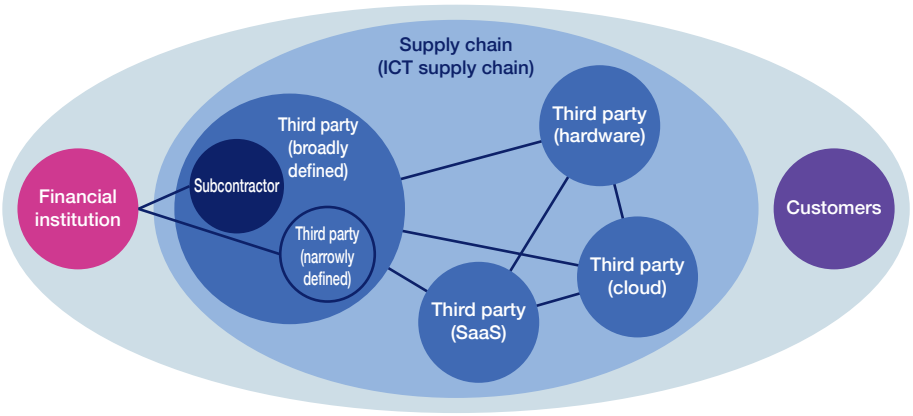
One particularly important part of ensuring operational resilience is third-party risk management. The *G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* define a third-party relationship as any contractual or other business relationship between a financial institution and an organization (whether affiliated with or external to the financial institution) to provide a product or service.

Two other similar terms used in the G7 document are "subcontractor" and "supply chain" (or "ICT supply chain"). Exhibit 3-3 shows how the three terms relate to each other. Financial institutions have to manage third-party risks in a manner that encompasses all of the third parties within their respective ICT supply chains and is aligned with those third parties', including any subcontractors', risk management.

Third-party risk management has become more of a regulatory priority in recent years. In addition to the EU's DORA, the BOE published a policy statement on financial market infrastructure outsourcing and third-party risk management[2] in February 2023 and a trio of US financial regulators jointly issued guidance on

2) Bank of England, *FMI Outsourcing and Third Party Risk Management Policy Statement* (February 8, 2023); https://www.bankofengland.co.uk/paper/2023/ps/fmi-outsourcing-third-party-risk-management-ps

Exhibit 3-3: Third parties in supply chain



Source: NRI SecureTechnologies, based on *G7 Fundamental Elements for Cyber Risk Management in the Financial Sector*

third-party risk management[3] in June 2023.

Such guidance places particular importance on mapping the entities involved in financial institutions' critical services/functions. As financial institutions enter into more and more third-party relationships, they find themselves faced with an increasingly complex web of interdependencies involving, e.g., cloud and FinTech services. Such complexity makes it all the more important for financial institutions to map out their third-party dependencies to prevent risks from being overlooked.

A mapping technique recommended by the European Systemic Risk Board as an effective way to reduce cyber risk in an operational resilience context is cyber mapping[4]. The ESRB gave examples of two approaches to cyber mapping: a functional approach used by Norway's Norges Bank and an institutional approach used by Germany's Bundesbank. The former identifies institutions that provide systemically core, critical functions and the systems these institutions depend on to do so. The latter identifies linkages between a financial network and third-party ICT service providers used by systemically important institutions. Using these approaches for reference, financial institutions should prepare their own cyber maps through an approach optimized to their respective management resources and then examine how effectively they are addressing risks posed by third parties involved in providing their critical services.

3) Federal Reserve Board, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 7, 2023); https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm

4) European Systemic Risk Board, *Mitigating systemic cyber risk* (January 2022); https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf

Cyber stress testing overseas

In the UK and EU, financial regulators have started to do cyber stress testing in conjunction with operational resilience compliance. The BOE's Financial Policy Committee announced plans to launch cyber stress testing in 2017. Following a successful pilot in 2019, the BOE's Prudential Regulatory Authority (PRA) in 2021 began conducting cyber stress tests of financial institutions that volunteered to participate. The PRA's report on the results of its 2022 cyber stress tests[5], published in March 2023, characterized cyber stress testing as "a separate but complementary exercise to operational resilience policy" and urged UK financial institutions to incorporate relevant aspects of the cyber stress tests' findings into their ongoing implementation of operational resilience policies.

5) Bank of England, *Thematic findings from the 2022 cyber stress test* (March 29, 2023; https://www.bankofengland.co.uk/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test

The ECB has announced that it too will conduct cyber stress testing, starting in 2024[6]. The testing is expected to strengthen European financial institutions' cybersecurity, mainly in the eurozone.

6) European Central Bank, *Interview with Helsingin Sanomat* (April 4, 2023); https://www.bankingsupervision.europa.eu/press/interviews/date/2023/html/ssm.in230404~ff3fe1816e.en.html

Operational resilience in Japan's financial sector

With European and US regulators thus imposing operational resilience mandates on financial institutions and launching cyber stress testing, Japanese financial regulators may follow suit.

The FSA's April 2023 *Discussion Paper on Ensuring Operational Resilience* does not tell financial institutions how to specifically address operational resilience. They must individually decide for themselves. Many of them are now experimenting through trial and error. Meanwhile, the specifics of the risk management controls required to comply with the ESPA have still largely yet to be determined, though cybersecurity risk management requirements should soon be clarified by forthcoming guidelines. Accordingly, many Japanese financial institutions will presumably select the pragmatic approach of strengthening their operational resilience by complying with the ESPA based on the forthcoming guidelines. Until the guidelines become available, Japanese financial institutions would benefit from studying the risk management controls required by the EU's DORA as preparation for ESPA compliance.

The financial institutions that will be subject to the ESPA are those designated

as critical infrastructure providers. Financial institutions not so designated will be exempt. Operational resilience, by contrast, applies to a broader cross-section of financial institutions. A certain number of financial institutions will likely have to meet operational resilience requirements but not have to comply with the ESPA, but even they could basically benefit from familiarizing themselves with the ESPA's requirements. Upgrading risk management based on the ESPA's requirements in the aim of becoming more operationally resilient therefore may be an effective approach even for financial institutions not designated as critical infrastructure providers.

Chapter 4

Economic security in the US and EU: Trends Impacting Financial Services

The Status Quo of Economic Security in the US and Europe

The United States and Europe have long recognized the potential threats to economic security that arise from today's highly complex and interconnected global economy. As early as 1998, then US president Bill Clinton issued a presidential directive on the topic of protecting critical infrastructure. This groundwork is still used today with Sector Specific Plans (SSPs), including for the financial services sector, regularly updated. In the EU, the European Programme for Critical Infrastructure Protection (EPCIP) and the Directive on European Critical Infrastructures published in 2008—provides a general framework for the bloc as a whole while national level governments have their own plans—one of which is the German IT Security Act 2.0. All frameworks acknowledge the core role that financial services providers play in protecting critical infrastructure and, more generally, economic security.

Economic Security: Suddenly, more important than ever

Recently, there has been a renewed focus on economic security and critical infrastructure protection. This stems, in part, from current geopolitical tensions between the US, Europe, China, and Russia, but it also stems from the fact that the definition of "critical infrastructure" has broadened as data and digital technology become the lifeblood of modern economies. The sheer complexity of this modern critical infrastructure, however, means that it is both inherently harder to control (leading to more risk) and more interconnected (leading to higher dependencies).

Recent examples from the US and Europe

The growing concern about economic security—and, in particular, the risks associated with modern data-driven critical infrastructure networks—can be seen in several high-profile incidents. In the US, this includes the recent banning

of Huawei and ZTE technology and debates about banning Chinese-owned ByteDance (parent company of TikTok) out of fears that China could use these to access critical infrastructure. Also relevant is the protectionist legislation of the CHIPS Act, which bans the sale of advanced chips and chipmaking technology to China out of fears that continued Chinese use of the technology could pose economic and national security threats.

European nations have faced similar debates and incidents—for instance, over Chinese ownership of 5G technology components and networks—but there is also an added concern about a growing Chinese economic presence in Southern and Eastern Europe where China has invested heavily, for example, in ports and transportation hubs in countries like Greece, Hungary, and Georgia as part of the Belt and Road Initiative. Meanwhile, Russia also represents a threat to European economic security and, especially, a risk to critical infrastructure—for example, through cybersecurity threats as well as threats to physical infrastructure such as gas and oil pipelines.

The importance of economic security for the bloc can be seen in a new European Economic Security Strategy framework, proposed as part of a joint communication by the European Commission in mid-June. This communication draws together much of the existing EU thinking on economic security into a concrete strategic framework that focuses on four risk types: resilience of supply chains, risk to critical infrastructure, risks associated with technology security, and risks of the "weaponization" of economic dependencies. While the communication is non-binding, the debate around the framework by the EU Council at the end of June shows the importance of this subject on the EU's agenda.

Two different approaches to ensuring economic security

It is important to note that the US and EU's approach to economic security is not identical. While the US has shown a tendency to act unilaterally to address what it sees as clear threats to economic security from China, the EU has taken a more multilateral approach. The recent EU Economic Security framework, for example, makes clear the threat it sees to economic security from Russia but does not directly mention China. Instead, the document speaks about de-risking European economic relationships and reducing economic dependencies. This cautious approach to China can be linked, in part, to the lack of consensus in the bloc itself as to the nature of the risk to economic security that China poses. For

example, the new German National Security Strategy (NSS) published in mid-June acknowledges the integrated nature of national security with economic security and names China a “partner, competitor, and systemic rival”.

Government versus industry: Not always on the same page

It is also important to note another key fault line in the debates over economic security is between governments and the private (business) sector. In the US, for instance, key sectors of technology and manufacturing have been vocal opponents of the government’s shift toward economic protectionism. Jensen Huang, the Taiwanese-American president and CEO of US technology firm Nvidia, recently warned of “enormous damage” to US industries if the Chinese market becomes closed to their products. The same goes in many European economies where the Chinese market represents key opportunities for future growth and where China represents a key supplier for everything from solar panel components to rare-earth minerals key to green technologies like electric vehicles. For example, half of German automaker Volkswagen’s profits stem from the Chinese market alone, according to recent reports, and the company reported a 20% market cap in the rapidly expanding Chinese automotive market in 2020.

Current State: Financial institutions and economic security risk

Whereas the role of more traditional industries like technology and manufacturing in the discussions surrounding economic security and critical infrastructure is well-known, the financial services industry, too, has taken on an increasingly important role—albeit a relatively non-public one. Financial institutions find themselves in the middle of a complex, high-risk situation. First, they have been tasked with protecting economic security more generally—for example, by engaging in investment screenings or sanctions lists. This means that as geopolitical tensions rise, economic security and national security become more entwined, and financial institutions find themselves in the middle of political maneuvers. Secondly, financial institutions are also responsible for protecting core parts of critical infrastructure—payment systems, communication systems, and the like. The growing technological complexity of this critical infrastructure makes the job of protecting it more difficult. Let’s take a look at each in turn.

Financial services under increased governmental scrutiny

First, the current geopolitical situation means that protecting economic security has become quite complicated on both sides of the Atlantic. When Russia invaded Ukraine in 2022, a coalition of US and European countries imposed a series of financial sanctions against Russia. US and European financial institutions are on the frontlines of enforcing these sanctions: Russian banks have been barred from using the SWIFT payment system for cross-border transactions, Western banking institutions are largely prohibited from doing business with Russian business entities and are responsible for ensuring adherence to a growing list of sanctions against Russian firms and individuals alike.

Meanwhile, as economic relations between China and the US sour, US financial institutions find themselves performing a balancing act. Like with other industries, the Chinese financial services market represents clear opportunity for future growth and many US financial institutions have invested heavily in China in the past several years. However, for US government officials, this growth-opportunity does not mitigate the potential risks. Concretely, this has led to some financial institutions—especially US based ones—to pull back from their Chinese expansion plans. Citigroup, JPMorgan, and Bank of America CEOs all testified before the US House Financial Services Committee in 2022 that they were prepared to “follow government guidance” and decrease efforts in China if asked to do so by the US government. Meanwhile, there have been reports that large investment banks like Goldman Sachs and Morgan Stanley have been considering decreasing the number of employees on their investment banking teams in the region.

Dealing with increasing technological complexity

But financial institutions aren’t just responsible for protecting economic security more broadly. They are also frontline defenders of critical infrastructure. For western financial institutions, the past five years have been characterized by rapid technological transformation and the technological underpinnings of today’s financial institutions are both part of the problem with protecting critical infrastructure and the solution. Today, data is the key driver of modern financial services operating models, and these operating models are increasingly complex. They include elements like ensuring data security and operational resilience in the face of cybersecurity threats. Meanwhile, financial industry supply chains have also expanded to as third-party providers support institutions via a network of

managed and outsourced services.

This increasing level of technological complexity means that financial institutions are more vulnerable to attacks linked to this technology and, as the next section shows, we see many US and European financial institutions spending significant resources to decrease the vulnerabilities linked to these modern, tech heavy operating models. For example, spending on vulnerability management and security analytics made up over 20% of IT security budgets at EU banking and financial services institutions in 2021, according to an ENISA (European Union Agency for Cybersecurity) report.

Future State: How Financial Institutions Can Mitigate Economic Security Risks

In the US and Europe, financial institutions act as frontline defenders of critical infrastructure but the ongoing nature of technological advancements and digital transformation within the industry mean that fulfilling this duty is more difficult than ever. The answer, perhaps paradoxically, is to complete these transformations as quickly as possible. This means more spending on things like data security, automation, and technology systems. A 2022 study by the European Central Bank found that most institutions (61%) do not yet have a dedicated digital transformation budget; for those that do, 22% of the IT budget is dedicated to digital transformation. Meanwhile, Statista, a German statistics platform, reports that new technology as a percent of banks' IT budgets has grown from around 25% in North America in 2013 to 37% in 2019 and they estimated this to grow to almost 50% by 2022. The numbers are slightly lower for Europe—13% in 2013 and 27% in 2019 with estimates of 33% for 2022.

In addition to a general increase in technology and digital transformation spending, we also see Western financial institutions allocating more resources to cybersecurity, mitigating regulatory risk, and modernizing their risk and compliance frameworks. These three areas are all key to protecting critical infrastructure.

Cybersecurity is key to protecting critical infrastructure

"I'm worried about cyber more than I am about markets…We're seeing many more attempts, more attacks [that are] increasingly sophisticated." (NBIM CEO Nicolai

Tangen, speaking with the Financial Times, August 2022)

While not all cybersecurity threats are due to the role that financial services institutions play in protecting critical infrastructure, all threats do impact the ability of institutions to fulfill their duty as a frontline protector of critical infrastructure and the number of threats that financial institutions face is growing. Norges Bank Investment Management (NBIM), which is responsible for the world's largest sovereign wealth fund, told the Financial Times in 2022 that they were facing an average of three "serious" hacking attempts per day and that this number had doubled in the past two or three years. Another 2022 study found that 63% of surveyed financial institutions experienced a year-on-year increase in destructive attacks while 60% of these institutions experienced an increased number of "island hopping" attacks where attackers gain access to the financial institutions network via managed service providers.

Given this, it should come as no surprise that spending on cybersecurity has skyrocketed. For example, Bank of America CEO Brian Moynihan, in 2021, stated that the US bank spend over USD 1 billion on cybersecurity alone. A 2022 survey of 130 security leaders in the global financial services industry found that 20-30% were planning budget increases this year to combat rising cybersecurity threats and 51% of organizations reported that they were already engaging in weekly "threat hunts" to proactively seek out cybersecurity threats.

Ensuring regulatory compliance

Next, a key part of critical infrastructure protection is ensuring that the financial institution keeps up to date and compliant with all regulation—even when the regulatory landscape changes rapidly. For example, financial institutions need to act quickly to adhere to changing regulations on outbound or inbound investment screening or to react quickly when new individuals or business entities are added to sanctions lists. The need to remain compliant has led to more spending on so-called RegTech (Regulatory Technology) solutions. Some estimates suggest that global spending by financial institutions on RegTech could increase three-fold between USD68 billion in 2022 to over USD200 billion by 2026 while other reports find that some major financial institutions are spending upwards of USD500 million or more annually. However, it should be noted that these levels of spending aren't necessarily new—as far back as 2015, major institutions were reporting that spending on regulatory compliance was climbing dramatically.

Modernizing risk and compliance frameworks

Finally, many Western financial institutions are in the process of overhauling their non-financial risk and compliance frameworks and while this may not be directly due to critical infrastructure protection concerns, these systems are indirectly key to protecting critical infrastructure. GRC—Governance, Risk, and Compliance—is a key topic among large financial institutions and most large institutions have implemented a "three lines of defense" model. Additionally, more institutions are turning to automated risk management technology platforms that can help monitor risk across the entire organization. Centralized compliance functions are also becoming more popular as is a focus on fostering a "culture of risk" that is intended to mitigate non-financial risks. For instance, training all employees on risk management including how to mitigate risks stemming from behavior (e.g., avoiding sanctions violations when onboarding new clients).

The importance of updating legacy technology and spending on new technologies is seen in the spending data. An ENISA (European Union Agency for Cybersecurity) report from 2021 found that 19% of banking and financial services IT security spending during 2020 was on GRC—second only to vulnerability management and security analytics.

Conclusion

As the geopolitical situation continues to evolve, forcing new risk assessments on the part of governments, financial institutions will continue to play a key role in the protection of critical infrastructure and, in turn, economic security more broadly. Digitalization and technology, on the other hand, has become an additional driver of vulnerability within the financial services sector, prompting financial services institutions to ramp up spending on regulatory compliance, cybersecurity, and the like.

Author's Profile

Nobutaka Uesugi

Expert Researcher

Financial Digital Business Promotion Department

focus@nri.co.jp

Author of Chapter 1

Shunsuke Miyahara

Senior Systems Consultant

aslead Business Department

focus@nri.co.jp

Author of Chapter 2

Hideyuki Fujii

Expert Security Consultant

NRI SecureTechnologies

focus@nri.co.jp

Author of Chapter 3

Onawa Lacewell, Ph.D.

Director, Chief Researcher

Cutter Associates

focus@nri.co.jp

Author of Chapter 4

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.1 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 16,500 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Digital Business Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/