One-year update on Japan's Economic Security Promotion Act

Jun Tsutsumi

23 July 2025

Iakyara vol.403

Nomura Research Institute, Ltd.

Executive Summary

Japan's Economic Security Promotion Act has now been in effect for over a year. IT governance frameworks that predate the Act have shortcomings and need to be reassessed in light of new risks.
Meanwhile, new issues have emerged, including treatment of ISMAP-certified cloud services and inclusion of network hardware in the reviews mandated by the Act.

Jun Tsutsumi
General Manager
Financial Risk Management Department

Japan's Economic Security Promotion Act[1] (ESPA) has been in effect for more than a full year as of May 2025. Financial institutions designated as essential infrastructure service providers[2] under the ESPA are required to notify the government of plans to introduce or significantly modify designated essential infrastructure or enter into or renew an agreement to outsource maintenance or management of such infrastructure. The government has been reviewing these submissions. The financial institutions that have undergone review generally seem to have all built risk management regimes compatible with their IT governance frameworks.[3] These frameworks have been a key focus of ongoing discussions between financial institutions and the Financial Services Agency.

However, the ESPA's legal provisions are reinforced by additional guidelines that explicitly prohibit the use of key infrastructure components by foreign actors in ways that could compromise the stable delivery of services. In light of growing geopolitical tensions and rising cybersecurity threats, precautions against state-sponsored malicious acts are becoming increasingly important. IT governance frameworks that predate the ESPA have shortcomings in terms of such precautions. The government reviews of financial institutions' infrastructure plans conducted to date have mostly pertained to infrastructure "maintenance or management" arrangements. Below we look at the main recommendations that have come out of these reviews.

Assessing risks across ESPA's broad purview

The ESPA is broadly targeted at supply chains and their constituent suppliers. In particular, it mandates vigilance in terms of potential infiltration of supply chains by malicious actors. The threat of such infiltration was seen as a new risk not addressed by pre-ESPA IT governance frameworks as illustrated by the following

NOTE

1) Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Act No. 43 of 2022)
2) Entities designated as essential infrastructure service providers are listed in https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_setsumeikai_eng.pdf (p44-58).
3) See https://www.fsa.go.jp/en/news/2024/20240510-2/2023.pdf.

three examples.

(1) Risk management with respect to design documents

In terms of design documents, pre-ESPA IT governance placed priority on version and revision controls to mitigate the risk of maintenance or management inefficiencies and quality problems. Having up-to-date, error-free design documents widely available to system operations staff at all times was considered best practice from the standpoint of minimizing system downtime. Under the ESPA, however, IT governance frameworks are required to assume that IT staff may have been infiltrated by a malicious actor and to therefore control when, why and by whom design documents may be accessed. Ideally, personnel authorized to access design documents should be limited to an absolute minimum number.

(2) Security cameras and other surveillance systems

Under pre-ESPA IT governance, security cameras and other surveillance systems served as a control on unauthorized access to restricted spaces. Now when companies designated as essential infrastructure service providers purchase such devices, the ESPA requires them to ascertain the supplier's country of domicile, research the country's laws and regulations and verify that the supplier is not on a US or European sanctions list. These requirements were imposed in response to past incidents in Japan and elsewhere and are intended to prevent installation of, e.g., security cameras that can be remotely disabled or are equipped with a clandestine backdoor that allows unauthorized access to the data feed. Availability of the requisite information is a key selection criterion when designated essential infrastructure service providers opt to use a third-party data center.

(3) Risk assessment of vendors' personnel

Under pre-ESPA IT governance, risk management of an outsourcing vendor's employees who will be involved in maintenance/management tasks consisted mainly of verifying their identity and their compliance with their authorized roles. The ESPA goes one step further by requiring designated essential infrastructure service providers to enter into agreements with their outsourcing vendors to gain access to information on the attributes and expertise of the vendor's employees. This disclosure enables more thorough risk assessments of individuals directly involved in maintenance or management tasks.

The ESPA requires information on outsourcing vendors' corporate officers, directors and shareholders' nationalities to be submitted to the Japanese government, which verifies that no external parties have undue influence over the vendor as part of its review process. Financial institutions should consider performing similar due diligence on not only the vendor (company) but also its individual employees.

Emergent issues to be addressed going forward

As financial institutions upgraded their IT governance regimes in compliance with the ESPA throughout the ESPA's initial fiscal year, several issues have emerged that should be addressed going forward.

(1) ISMAP

The Japanese government established the Information System Security Management and Assessment Program (ISMAP) to assess and certify the security of cloud services. By choosing an ISMAP-certified service, financial institutions can bypass the government's review process when introducing that service as part of designated essential infrastructure.

However, ISMAP certification does not exempt institutions from the requirement to undergo government review for maintenance and management arrangements involving the service. It remains unclear whether the use of an ISMAP-certified cloud service by a designated essential infrastructure service provider constitutes a maintenance/management arrangement subject to review. (Further clarification from the government is expected on this point.)

If cloud services are classified as maintenance/management arrangements, then information on their risk management frameworks and the subcontractors involved in service delivery would need to be submitted to the government for review. However, cloud services normally do not disclose such information to their customers. This lack of transparency would not pose an issue if ISMAP-certified cloud services were exempted from government review not only for their introduction as components of designated essential infrastructure, but also for related maintenance/management arrangements. The government has yet to give any indication of how it intends to decide this matter. It will presumably do so based on whether it deems the ISMAP review process sufficient to obviate the need for the review of maintenance/management arrangements.

(2) Assessment of risk management's operational status

The reviews mandated by the ESPA look at whether risk management measures are in place. They do not check whether the in-place risk management measures have been operationalized. Financial regulation in Japan has long been predicated on a relationship of trust between financial institutions and regulatory authorities. Regulators have confidence that if risk management measures are in place, they are of course operating properly. Regulators can verify the operational effectiveness of risk management measures through mechanisms such as internal audit frameworks and independent assurance reports provided by external auditors.

(3) Network hardware

In the financial sector, the ESPA-mandated reviews cover servers, business applications, operating systems and middleware. Network hardware was presumably considered for inclusion in the reviews but ended up being omitted across all of the initially 14 (now 15) sectors with designated essential infrastructure service providers.

Under Japan's new Active Cyber Defense Act[4], enacted May 23, 2025, designated essential infrastructure service providers will be required to provide the government with network configuration diagrams showing the subset of designated hardware (referred to in the Act as "key computing hardware") that is connected to the Internet. As a result, these providers must begin preparing such documentation without waiting for revisions to the scope of ESPA reviews. Both public and private entities have gained knowledge of ESPA over the past year. Meanwhile, the Active Cyber Defense Act was enacted and geopolitical tensions have prompted widespread recalibration of security postures. Given such developments, designated essential infrastructure service providers should be proactively implementing precautions against new risks, not merely complying with statutory mandates. Meanwhile, the knowledge gained since the ESPA took effect should be shared even with financial institutions not subject to the ESPA. We believe that doing so would benefit the entire financial sector.

4) Act on the Prevention of Malicious Acts Against Critical Computing Hardware.

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 Tokyo, New York, London, Beijing and Sydney, with over 16,700 employees.

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

Inquiries to : Financial Market & Innovation 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/list.html#lakyara