INTERNATIONAL MONETARY FUND

IMF Country Report No. 24/113

JAPAN

FINANCIAL SECTOR ASSESSMENT PROGRAM

May 2024

TECHNICAL NOTE ON CYBER RESILIENCE AND FINANCIAL STABILITY

This Technical Note on Cyber Resilience and Financial Stability for the Japan FSAP was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed on April 16, 2024.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

JAPAN

FINANCIAL SECTOR ASSESSMENT PROGRAM

April 16, 2024

TECHNICAL NOTE

CYBER RESILIENCE AND FINANCIAL STABILITY

Prepared By
Monetary and Capital Markets Department, IMF

This Technical Note was prepared by Emran Islam (IMF) in the context of the Financial Sector Assessment Program (FSAP) in Japan, led by Mahvash Qureshi (IMF). It contains the technical analysis and detailed information underpinning the FSAP findings and recommendations. Further information on the FSAP program can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

FIGURES

TABLES

APPENDIX

Glossary

BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plan
BOJ	Bank of Japan
CERT	Computer Emergency Response Team
CF	Critical Function
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIR	Cyber Incident Response
CIRR	Cyber Incident Response and Recovery
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CSD	Central Securities Depository
CSG	Comprehensive Supervisory Guidelines
CSP	Cloud Service Provider
CSSA	Cybersecurity Self-Assessment
DDoS	Distributed Denial of Service
DOS	Denial of Service
FFIEC	Federal Financial Institutions Examination Council
FISC	Center for Financial Industry Information Systems
FMI	Financial Market Infrastructure
FSA	Financial Services Agency
FSB	Financial Stability Board
FSR	Financial System Report
G7	Group of Seven
GTL	Generic Threat Landscape
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISAC	Information Sharing and Analysis Center
IT	Information Technology
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
KRI	Key Risk Indictor
NISC	National center of Incident readiness and Strategy for Cybersecurity
NPA	National Police Agency
PFMI	Principles for Financial Market Infrastructures
PPC	Personal Information Protection Commission
RTGS	Real-Time Gross Settlement
RTO	Recovery Time Objective
TLPT	Threat-led Penetration Testing
TTP	Tactics, techniques, and procedures

EXECUTIVE SUMMARY

Japan's financial system is digitalizing rapidly, increasing exposure to cyber risk. As in other jurisdictions, the pace of digitalization in Japan has increased substantially, but cyber incidents have also surged in recent years. The tight interdependencies within its financial system, and beyond, make Japan vulnerable to evolving cyber threats. The Financial Services Agency (FSA) and Bank of Japan (BOJ) have made progress in enhancing the cyber resilience of the financial sector, but further work and enhancements are needed.

The cyber ecosystem is mature in Japan, with a range of stakeholders involved in ensuring the cybersecurity of the financial sector. At governmental level, the National center of Incident readiness and Strategy for Cybersecurity (NISC) works with the public and private sectors on a variety of activities to create a "free, fair, and secure cyberspace." The NISC plays its leading role as a focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and public and private sectors, and is responsible for developing the Cybersecurity Strategy and the Cybersecurity Policy for Critical Infrastructure Protection.

The FSA is responsible for developing and operationalizing the cyber strategy for the financial sector. The FSA achieves this objective through close coordination and cooperation with a range of other stakeholders, such as the BOJ, NISC, Financial Information Sharing and Analysis Center Japan (Financials ISAC Japan), National Police Agency, and industry trade associations. The close interaction between these different stakeholders allows a free flow of threat information and intelligence between the public and private sectors. Additionally, the FSA and BOJ are active in the international arena, with close cooperation with G7 authorities and other international standard setting bodies. Overall, Japan is a good example of coordination and cooperation within the financial sector in the field of cybersecurity, in comparison to international peers. This said, the FSA could further enhance its cyber strategy with industry guidance around testing and exercising, which would allow the heterogeneous financial entities to conduct a variety of proportionate tests on themselves, thereby strengthening their cybersecurity capabilities.

Cyber risk regulation and supervisory practice need further improvements. The FSA should update its Comprehensive Supervisory Guidelines (CSG) for all its supervised financial entities on cyber risk. The FSA should also implement a more structured, risk-based approach to cyber risk supervision, supported by adequate tools. The FSA should align its supervisory tools and methodologies to the updated CSGs, which would enhance the overall approach to on-site inspections and off-site monitoring. Furthermore, the FSA should prioritize the cyber supervision of financial market infrastructures (FMIs), which are critical to ensuring the financial stability of Japan. Finally, the FSA cyber supervision unit should be given sufficient resources to discharge its responsibilities and use a mix of different regulatory tools (e.g., use of independent auditors), thereby maximizing efficiency with its limited resources.

The BOJ should strengthen the cyber risk oversight of FMIs. The BOJ oversight function should leverage the CPMI-IOSCO Cyber Guidance as a tool to gather self-assessments from the overseen

FMIs and to conduct cyber assessments of the FMIs, including the central bank operated systems. In addition, the oversight function would benefit from securing cyber expertise within the cyber-related teams, which would increase the capabilities and effectiveness of the oversight function with regards to cyber resilience.

The FSA would benefit from deepening its analysis of the operational interconnectedness of the financial system. While **"**cyber mapping" is an emerging field, it will help deepen the understanding of how financial entities and FMIs are operationally and technologically interconnected, and the transmission channels which could trigger financial instability via cyber-attacks. Based on this analysis, the FSA should develop a range of cyber contagion scenarios and use these to build stronger sector-wide crisis preparedness through scenario-based testing and incident response.

Further improvements in the response and recovery capabilities are recommended. The FSA and BOJ should keep upgrading, as necessary, a range of extreme but plausible cyber scenarios along with their existing Business Continuity Plans (BCP) and/or Cyber Incident Response and Recovery Plans (CIRR) (i.e., BCP or CIRR for the FSA; and Cyber Incident Response (CIR) framework and BOJ-NET BCP for the BOJ)), for the financial sector. By updating these documents, Japan will be better placed to manage a systemic cyber incident. In terms of exercises, the FSA conducts the annual Delta Wall exercise, which brings together more than 160 financial entities that are tested on their incident response capabilities to a number of different cyber scenarios, thus providing the FSA with deeply insightful information on the financial sector's capacity (strengths and weaknesses) and providing a robust basis to drive sector-wide improvements. The BOJ is in a unique position as the overseer of FMIs and the operator of FMIs (e.g., BOJ-NET) and therefore, the BOJ should consider conducting cyber simulations/table-top exercises with BOJ-NET participants and FMIs with BOJ-NET connections to ensure that all stakeholders are well prepared to manage a systemic incident.

The authorities currently have strong cyber incident reporting regimes in place, with clear definitions, taxonomies, thresholds, and communication channels. However, as the Financial Stability Board (FSB) completes its work on Cyber Incident Reporting and develops a standard for reporting, the Japanese authorities may benefit from reviewing their existing framework and aligning it further with the FSB if appropriate, thereby contributing to global convergence in this field.

Table 1. Japan: Recommendations on Cyber Resilience and Financial Stability

Recommendations	Timing[1]	Authorities
Strategy and Governance		
Enhance the cyber strategy over the longer term by developing industry guidance for a broader testing and exercising regime e.g., threat-led penetration testing (TLPT), purple team testing, and cyber simulations, among others. (¶47)	MT	FSA
Strengthen the governance arrangements and establish a more structured joint supervisory approach between the horizontal (i.e., IT Cyber Monitoring Team) and vertical (i.e., supervisory divisions) functions, including better information sharing between them. (¶48)	ST	FSA
Continue to explore means of increasing its capacity to fulfill its role in strengthening the cyber resilience of the Japanese financial sector. (¶49)	ST	FSA
Interconnectedness and Financial Stability		
Further strengthen the analysis of how the financial sector is operationally interconnected. This would entail developing network analysis of how the different critical sub-sectors are connected through common technologies and service providers, thereby allowing the identification of critical nodes. (¶53)	MT	FSA
Cyber Regulatory Framework and Supervisory Practices		
Update its Comprehensive Supervisory Guidelines (for all its sub-sectors), comprehensively covering cybersecurity; align the lessons learnt from on-site inspections, Cybersecurity Self-Assessment (CSSA), and supervisory methodologies/tools to the supervisory guidelines; and include a section in supervisory reports that explains the risk/impact of the findings materializing and the severity of the findings, to facilitate better prioritization by the financial entity, as well as the reference to the supervisory expectation/requirement. (¶77)	MT	FSA
Increase its off-site and on-site cyber supervision of the FMIs, with the relevant responsible divisions working in close collaboration with the IT Cyber Monitoring Team. (¶78)	I	FSA
Further increase/enhance the skills and expertise of its FMI overseers with regards to cyber to address the changing cyber threat landscape surrounding the overseen FMIs. (¶79)	ST	BOJ
Strengthen its oversight approach on cyber resilience for FMIs (including the BOJ-operated FMIs) against the CPMI-IOSCO Cyber Guidance (Guidance). (¶80)	ST	BOJ
Enhance their coordination and cooperation to strengthen their supervisory/oversight approach on cyber for commonly supervised/overseen FMIs. (¶81)	I	FSA and BOJ
Develop a set of Key Risk Indicators (KRIs) to improve its off-site monitoring of financial entities. (¶82)	ST	FSA and BOJ

[1] I Immediate (within 1 year); ST Short Term (within 1-2 years); MT Medium Term (within 3−5 years).

Table 1. Japan: Recommendations on Cyber Resilience and Financial Stability (concluded)		
Monitoring, Response and Recovery		
Consider developing a Generic Threat Landscape (GTL) Report. The report could set out the specific threat landscape of the Japanese financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. (¶111)	MT	FSA and BOJ
Make progress on red team testing on its ICT environment. (¶112)	ST	BOJ
Update its BCP or develop a standalone Cyber Incident Response and Recovery (CIRR) plan, with a playbook of different cyber scenarios, that are regularly tested. The BCP or CIRR plan should set out the governance arrangements and thresholds for cyber incidents that could potentially trigger systemic risk. (¶113)	ST	FSA
Continue upgrading its BOJ-NET BCP with a range of cyber-specific extreme but plausible scenarios that are regularly tested. (¶114)	ST	BOJ
Test the BOJ's CIR framework regularly. (¶115)	ST	BOJ
As overseer of FMIs and operator of BOJ-NET, consider conducting cyber exercises/simulations (e.g., table-top exercises) for BOJ-NET with relevant parties (e.g., BOJ-NET participants and other FMIs having link/connection with BOJ-NET) to strengthen the responses to potential cyber incidents that could have material impacts on broader payment and settlements systems. (¶116)	ST	BOJ
Information Sharing and Incident Reporting		
Review whether their existing incident reporting regime is appropriate in light of trends in international CIR discussion, such as those at the FSB, and bring it into alignment with the FSB's cyber incident reporting framework, once completed, if appropriate. (¶121)	ST	FSA and BOJ

INTRODUCTION[1]

A. Background: Cyber Risk as a Financial Stability Concern

1. Constantly evolving cyber threats require vigilance from the financial entities, regulators, and supervisory authorities alike. Tackling cyber risk remains a global challenge, with most authorities embarking on significant work programs to strengthen resilience in this dimension. Malicious cyber actors with varying level of sophistication continue to evolve and innovate their tactics, techniques, and procedures (TTP). The recent global threat landscape has been characterized by the exploitation of a series of critical zero-day vulnerabilities, supply chain attacks, ransomware attacks, and distributed denial-of-service attacks. Additionally, non-malicious incidents like accidental data disclosures and configuration, implementation, or processing errors continue to be an important source of cyber risk.

2. The Japanese government has recently stepped up its efforts to support digital transformation in the economy, particularly under the "New Form of Capitalism."[2] It accentuates the need for a cyber resilient economy. On financial services, according to a survey by the Bank of Japan (BOJ) for regional financial institutions, digital channels in doing business had been increasing notably even before the pandemic. Moreover, about two-thirds of these regional financial institutions (regional, shinkin, and shinkumi banks) expect internet banking services and mobile apps to be adopted more widely as a mode of business in 2023 and beyond.

3. Within the context of this increased digital transformation, a high number of cyber incidents, even if they are not systemic, could feed into broader mistrust in digital adoption and hinder productivity growth. According to an OECD survey, the fraction of firms and individuals who have experienced online security incidents seem significantly higher in Japan than many peer economies (OECD Digital Economy Papers No. 283). Moreover, the number of phishing and ransomware attacks have nearly doubled every year since 2019, as shown in the latest BOJ's Financial System Report (BOJ, 2023, Chart IV-5-4).

4. Consequently, the Japanese authorities have identified cyber risk as a risk with the potential to impact financial stability. A cyber incident impacting the confidentiality, integrity, or availability of a financial entity's critical activities may have the potential to destabilize the financial system. Strong capabilities to timely detect anomalies and compromises, as well as respond to and recover from them, are critical in the current cyber threat landscape.

[1] This Technical Note is prepared by Emran Islam (IMF, Monetary and Capital Markets Department, Financial Supervision and Regulation Division). The FSAP thanks the authorities for the constructive dialogue and the many insights that they have shared.

[2] https://www.cas.go.jp/jp/seisaku/atarashii_sihonsyugi/pdf/ap2023en.pdf

B. Review Scope: Banks, Securities, Insurance, and Financial Market Infrastructures

5. This note reviews key elements of the cyber regulatory and supervisory framework for the financial sector in Japan. This includes: (i) the role and practices of the Japanese authorities in the development of a cyber strategy for the financial sector; (ii) development and maintenance of the cyber regulatory framework; (iii) on-site and off-site supervisory processes; (iv) interconnectedness and financial stability; (v) cyber risk related information and intelligence sharing; and (vi) cyber incident reporting, monitoring, response, and recovery. This review is limited to the framework for financial entities that fall within the mandate of the Financial Services Agency (FSA) and Bank of Japan (BOJ).

6. The FSAP team collected information from several sources. These include questionnaire answers provided by the FSA and BOJ, interviews with both authorities, NISC and Financials ISAC Japan, the study of relevant national laws and reports published by the authorities, as well as documentation of their work.

7. Conclusions and recommendations of the FSAP review are aligned with international regulatory and supervisory good practices. As there are no binding international regulatory standards on cyber risk management, the FSAP team used internationally recognized regulatory good practice as the basis of this note. The following documents were used as a benchmark in the assessment: the FSB "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices" in 2017; the BCBS "Cyber-resilience: Range of practices" in 2018; the IMF Departmental Paper on "Cybersecurity Risk Supervision"; the G7 "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector"; the "Basel Principles for Operational Resilience"; and the revised "Principles for Sound Management of Operational Risk". The basis of the review in the case of FMIs was the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

STRATEGY AND GOVERNANCE

A. Cyber Strategy

8. The Cybersecurity Strategic Headquarters was established under the Cabinet in November 2014 for the purpose of effectively and comprehensively promoting cybersecurity policies. The Cybersecurity Strategic Headquarters is headed by the Chief Cabinet Secretary, with the Minister in charge of Cybersecurity as a deputy head, and composed of the Chairman of the National Public Safety Commission, the other relevant Ministers, and knowledgeable experts from academia and business sectors.

9. The National center of Incident readiness and Strategy for Cybersecurity (NISC) has been established since 2015, as a secretariat of the Cybersecurity Strategy Headquarters. It works together with the public and private sectors on a variety of activities to create a "free, fair and secure cyberspace." The NISC plays its leading role as a focal point in coordinating intra-government

collaboration and promoting partnerships between industry, academia, and public and private sectors, and is responsible for developing the Cybersecurity Strategy and the Cybersecurity Policy for Critical Infrastructure Protection (CIP).

10. The Cybersecurity Strategy—published in September 2015 and revised in July 2018 and September 2021—was decided by the Cabinet based on Article 12 of the Basic Act on Cybersecurity. The Strategy describes the national cybersecurity policy and its objectives, as well as the goals and implementation policies for the next three years. In addition, based on the Strategy, the Cybersecurity Strategic Headquarters, which is created by Article 25 of the Basic Act on Cybersecurity, formulated the Cybersecurity Policy for Critical Infrastructure Protection (the latest version was published on June 17, 2022) that designates the financial sector as one of 14 critical infrastructures.

11. The primary aim of the Cybersecurity Strategy is to ensure a cyberspace which is "free, fair, and secure" and adheres to five key principles. The principles include: (i) assurance of the free flow of information; (ii) the rule of law; (iii) openness; (iv) autonomy; and (v) collaboration among multiple stakeholders. Based on these principles, the Cybersecurity Strategy aims to focus on three key policy areas: (1) advancing digital transformation and cybersecurity simultaneously; (2) ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected, and interrelated; and (3) enhancing initiatives from the perspective of Japan's national security.

12. The NISC is also responsible for the 'Cybersecurity Policy for Critical Infrastructure Protection' which is a common action plan shared between the government agencies. It bears responsibility for promoting independent measures by critical infrastructure (CI) operators relating to CI cybersecurity and implementing other necessary measures, and CI operators which independently carry out relevant protective measures. The current edition was published in 2022 and identifies 14 sectors as critical infrastructure and it expects stakeholders to undertake the five measures as follows: (i) enhancement of incident response capability; (ii) maintenance and promotion of the safety principles; (iii) enhancement of information sharing system; (iv) utilization of risk management; and (v) enhancement of the basis for CIP. The financial sector has been designated as CI and the FSA has been designated as the competent authority for critical infrastructure operator for the financial sector.

13. In order to discharge its responsibilities for the financial sector, the FSA published "The Policies to Strengthen Cyber Security in the Financial Sector (Ver. 3.0)" in February 2022. Its prior versions were published in July 2015 and October 2018. The policy document, also considered to be FSA's cyber strategy, is a well drafted document which sets out progress made since 2018 and the future policy actions to be taken. The FSA noted significant improvements have been made in six key areas: 1) response to accelerated digitalization; 2) engagement in international discussions; 3) response to the Tokyo 2020 Games; 4) strengthening the cybersecurity of financial entities; 5) improvement of the information sharing framework; and 6) improvement of human resources development in the financial sector.

14. Going forward, the FSA aims to focus its efforts in the following five areas: 1) advancement of monitoring and exercises; 2) preparing for new risks; 3) organization-wide efforts to ensure cybersecurity; 4) strengthening cooperation with related organizations; and 5) Economic Security Responses.

15. The FSA will look to address these five areas by:

- Increasing its inspections and monitoring of financial entities to enhance their cyber risk management and incident response capabilities;
- Developing and using a self-assessment tool on cybersecurity for regional financial institutions, to assess their cyber posture and direct improvements in their cybersecurity measures;
- Continuing to run the cyber exercise (Delta Wall) to help improve the ability of the financial sector to respond to cyber-attacks;
- Developing forward looking policy on new risk areas, such as cloud usage and cashless payment services;
- Emphasizing the need of senior management at financial entities to prioritize cyber risk, through their own increased involvement and investment in human resources; and
- Strengthening collaboration with other agencies (e.g., NISC).

16. The BOJ annually publishes the "On-Site Examination Policy," which sets out its policy on on-site examination including cyber risk. The policy is based on observations made through its off-site and on-site monitoring, as well as domestic and overseas developments. The content of the policy is determined by the Policy Board.

17. With regard to the status of cybersecurity management frameworks, the BOJ sets out in its On-Site Examination Policy that it will examine (1) the appropriateness of the collection and sharing of information on developments in ever-changing cybersecurity threats, (2) the effectiveness of countermeasures against vulnerabilities, (3) the appropriateness of the management of access rights for important data such as customer information, and (4) the effectiveness of measures to prevent cyber-attacks and limit damage caused by such attacks. Moreover, given that it is difficult to prevent cyber-attacks completely, it will examine the effectiveness of frameworks and contingency plans to recover critical operations in preparation for the occurrence of cyber incidents, the implementation of drills, and the review of management frameworks reflecting the outcomes of such drills.

18. Based on the outcomes of the joint survey with the FSA and BOJ on some major financial institutions, the FSA and BOJ will deepen its dialogue, particularly on (1) governance (the commitment of the boards of directors and senior management, the securing of resources including budgets and staff, and cooperation among business units), (2) the development of group-wide global frameworks (such as with regard to information gathering, defenses, monitoring,

responses, and drills with respect to cybersecurity threats), (3) the use of threat-led penetration testing (TLPT), (4) improvement of cyber resilience (such as through developing contingency plans for ransomware attacks), and (5) the management of third parties including outsource companies. Finally, the FSA and BOJ will jointly continue to implement a self-assessment survey on regional financial institutions' cybersecurity management frameworks and encourage them to ascertain their preparedness and strengthen their countermeasures.

19. The FSA takes a structured approach in developing its cyber policy/strategy. The driver for the policy/strategy is the Cybersecurity Strategy and the Cybersecurity Policy for Critical Infrastructure Protection, which serve as a basis for FSA's own thinking. Furthermore, approximately every three years, the FSA assesses its progress in the field, and takes into consideration the current and future threat landscape, to help determine which areas require focus going forward. Finally, the FSA will discuss its cyber policy/strategy with a range of different stakeholders, such as the BOJ and NISC, before finalizing its approach for the next three years.

20. The BOJ effectively uses its on-site and off-site monitoring of financial entities, as well as joint work conducted with the FSA, to determine its On-Site Examination Policy for the forthcoming year. By using this information, the BOJ can focus its efforts on key risk areas.

21. However, the FSA could enhance the overall cyber strategy for the financial sector by developing some industry guidance on TLPT and other forms of testing.[3] It will ensure that the financial entities have a standardized framework that they can refer to when conducting these tests. Currently, mega banks conduct TLPT; however, the approach to such testing by the different financial entities differs in the absence of any industry framework, and therefore it can be difficult to determine whether a financial entity has conducted a legitimate TLPT. Furthermore, the FSA has largely relied on its own Delta Wall exercise to gain assurance on financial entities' capabilities to respond to cyber incidents. By producing guidance on a broad range of different types of tests (e.g., scenario-based testing, red team testing, grey box testing, purple team testing, gold team testing, etc.), the FSA may be able to catalyze the industry to conduct a broader range of tests, from which the regulator can obtain greater assurance on the resilience of financial entities and the sector more broadly. Finally, by broadening the scope of the types of tests, the FSA will be able to apply a degree of proportionality on the types of tests that different types of financial entities could and should conduct. This is particularly important as TLPT can be particularly expensive and resource intensive, and therefore not all financial entities can or need to conduct such a test.

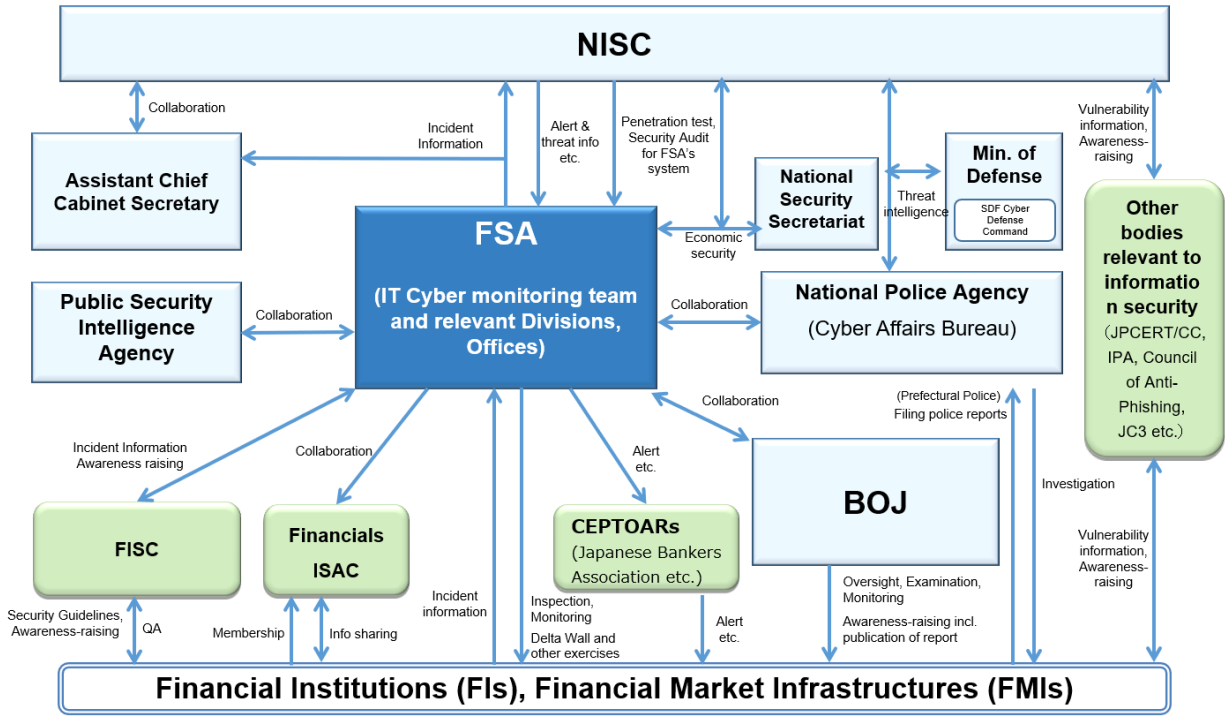
B. Institutional Framework

22. Japan has a mature cyber ecosystem, with a broad range of stakeholders—both public and private—coordinating and cooperating effectively to ensure the cybersecurity of the Japanese financial system. The NISC, FSA and BOJ have made significant strides in building

[3] TLPT is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes, and technology, with minimal foreknowledge and impact on operations.

capacity throughout the industry and have built strong public-private structures to ensure free-flowing information and initiatives between all parties. Furthermore, the structures in place play a variety of different but crucial roles – policymaking, supervisory and operational. The roles and responsibilities of all the stakeholders are well defined and there is a clear atmosphere of collaboration in place (Figure 1).

Figure 1. Japan: Overview of Japanese Cyber Ecosystem



Source: FSA.

23. The FSA is responsible for ensuring stability of Japan's financial system, protection of depositors, insurance policyholders and securities investors, and smooth finance through such measures as planning and policymaking concerning the financial system, inspection and supervision of private sector financial entities, and surveillance of securities transactions. Under Article 3 of the Act for Establishment of the Financial Services Agency, the FSA "has a mission to secure the stability of financial functions in Japan and protect depositors, policyholders, securities investors, and any equivalent persons, and facilitating financing". In order to discharge this responsibility, the FSA must supervise the control framework for cyber risk management, similarly to the control framework for credit, market, and operational risk management in financial entities (Table 2).

24. The BOJ is responsible for ensuring the smooth settlement of funds among banks and other financial institutions, thereby contributing to the maintenance of stability of the financial system. The BOJ has a pivotal role in operating the RTGS system, overseeing FMIs on a moral suasion basis and ensuring financial stability of the system. Additionally, under Article 44 of

the Bank of the Japan Act, the BOJ "…may conclude a contract with financial institutions, etc. which would be the counterparty in that business (hereinafter referred to as the "counterparty financial institutions, etc." in this Article) concerning on-site examinations (examinations which the Bank carries out regarding the business operations and the state of the property of the counterparty financial institutions, etc. by visiting the premises thereof…)". Under this Article, the BOJ monitors financial entities that have a contract with it. The BOJ conducts both on-site examinations and off-site monitoring with regard to cybersecurity.

Table 2. Japan: Overview of Roles of Cyber Stakeholders

Role	Stakeholders
Policy	NISC
Regulation/Supervision	FSA
Oversight/Examination and Monitoring	BOJ
Industry Guidelines	FISC, Industry Associations
Technical Operation/Facilitation of Mutual Assistance	Financials ISAC Japan

Source: IMF staff.

25. In Japan, there are some non-financial stakeholders with a role in the cybersecurity of the financial sector. They include the NISC, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), National Police Agency (NPA), Financials ISAC Japan, Center for Financial Industry Information Systems (FISC), CEPTOARs (Japanese Bankers Association, Life Insurance Association of Japan, General Insurance Association of Japan, Japan Securities Dealers Association, and Japan Payment Service Association), Ministry of Defense, Public Security Intelligence Agency, and the Personal Information Protection Commission (PPC).

26. Although not an authority, the FISC is a public interest incorporated foundation accredited by the Prime Minister and engaged in cybersecurity-related activities. The FISC, with the involvement of the FSA and the BOJ, has developed information security guidelines for the financial industry, which have become the de facto standard in the areas of risk management and cybersecurity for IT systems in the financial industry.

27. The FSA is a member of the Cyber Security Council established under Article 17 of the Basic Act on Cybersecurity, and JPCERT/CC serves as the Secretariat of the Council. Therefore, the FSA has a cooperative relationship with JPCERT/CC o strengthen cybersecurity in Japan through the activities of the Council.

C. Coordination and Cooperation

28. The FSA cooperates and coordinates with the NISC through two-way information sharing (threat intelligence, incident reporting, etc.) and participation in meetings hosted by the NISC. This relationship is underpinned by the Basic Act on Cybersecurity. When a cyber incident occurs, the FSA receives an immediate report from the affected financial entity. And if the financial

entity falls under critical infrastructure (i.e., deposit-taking institutions including banks, insurance companies, securities companies, payment service providers and FMIs), the FSA shares the matter with the NISC, in accordance with Article 32 of the Basic Act on Cybersecurity and the agreement with the NISC.

29. With regard to public-private cooperation and coordination in the financial sector, the FSA recognizes that there are various communication channels between regulatory authorities and regulated financial entities. In addition, the FSA recognizes that it is important to encourage information sharing and the establishment of a response framework for cyber events based on such information. Based on this recognition, the FSA launched the "Liaison Council for Cybersecurity Stakeholders" in June 2019 in order to enable mutual information coordination in the event of cyber incidents, including large-scale incidents, in collaboration with related organizations such as the BOJ, the respective sub-sector's CEPTOAR, the Financials ISAC Japan and the FISC. Using the Liaison Council, the FSA shares cooperation procedures with related public and private organizations and assesses the effectiveness of the cooperation framework in the event of an incident through a desktop exercise.

30. Apart from the Liaison Council, the FSA and the BOJ established the Financial Monitoring Council in June 2021. It is a senior-level meeting platform between the FSA and the BOJ to promote initiatives for enhanced coordination in order to conduct effective monitoring (including cybersecurity). In the Council, the FSA shares information with the BOJ, and coordinates the status of coordination and policies of initiatives between the two, thereby ensuring coordination and cooperation.

31. Furthermore, the FSA holds monthly meetings with financial industry associations to share information. At these meetings, the FSA shares information and holds Q&A sessions on matters that should be shared between the FSA and financial industry associations (including cyber risk issues). For example, at the February 2023 meeting, the FSA called on financial entities that participated in the Delta Wall VII cross-industry cybersecurity exercise held in October 2022 to make use of the results of the exercise to further improve their incident response capabilities. The FSA also called on non-participating financial institutions to make use of common challenges and good practices across sectors identified through the exercise to enhance their incident response capabilities, including enhancing exercises and training.

32. The FSA also coordinates closely with other intelligence agencies, such as the National Police Agency and the Public Security Intelligence Agency. This coordination enables to strengthen intelligence gathering, particularly on cyber threats, and uses information/intelligence gathered in a timely manner in the supervision of financial entities.

33. In Japan, cybercrime is defined by the Penal Code, and Special Acts such as the Act on Prohibition of Unauthorized Computer Access. However, the FSA is not the competent authority for such criminal laws. The FSA and law enforcement authorities cooperate and collaborate primarily at the operational level, as there is a common interest and need for collaboration to achieve their respective administrative objectives. Specifically, law enforcement authorities have intelligence on

cyber threats through cybercrime investigations, and expect financial entities to take actions to prevent incidents and mitigate damage from the viewpoint of crime prevention. On the other hand, the FSA expects financial entities to take actions to prevent incidents and mitigate damage by utilizing intelligence on cyber threats for the benefit of the financial system, financial entities, and their customers. As one of the concrete results of cooperation, the FSA issued requests to financial entities and the general public to prevent cybercrime based on the National Police Agency's intelligence on phishing.

34. In the Japanese criminal justice system, public prosecutors have a monopoly on the right to file criminal charges. Public prosecutors and the primary investigative authorities such as the prefectural police conduct investigation activities, including the collection of evidence necessary for prosecution, based on their legal authority. The FSA and financial entities cooperate in such investigation activities in response to requests from public prosecutors and the police. The investigation activities necessary for criminal charges are in accordance with laws and regulations, and no arrangements are required between the law enforcement authorities, the FSA, and financial entities to cooperate in this process.

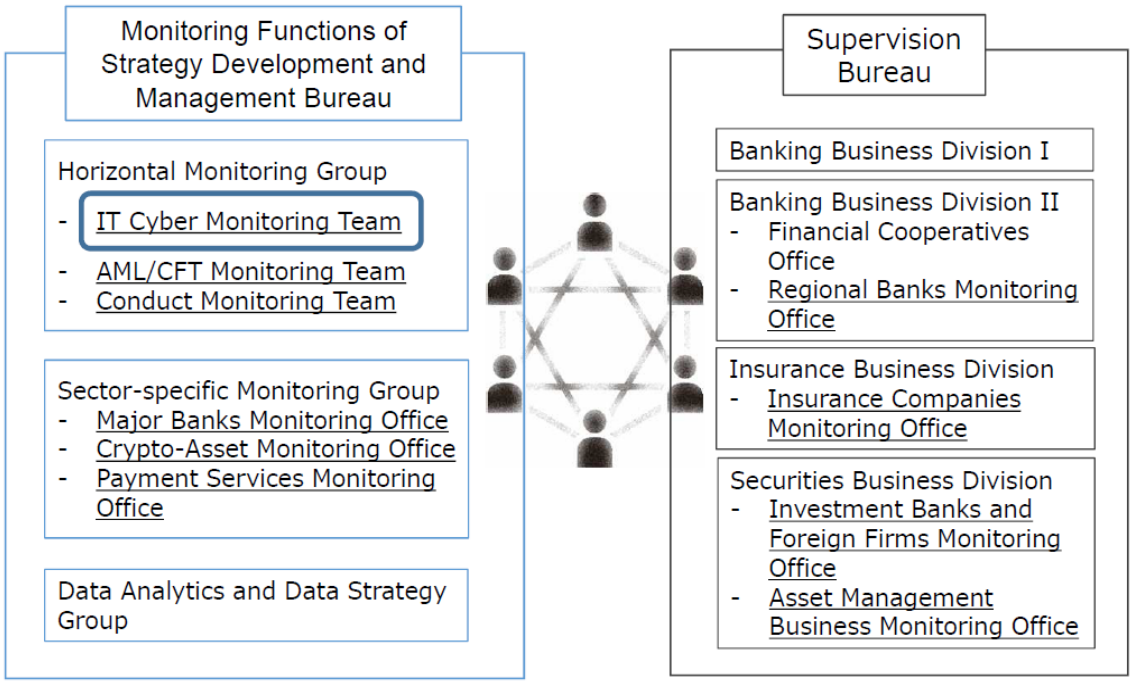
D. Governance Arrangements

35. The FSA has established the IT Cyber Monitoring Team as a Cybersecurity Center of Excellence to enhance its cyber risk supervision capabilities (Figure 2). The IT Cyber Monitoring Team consists of a mixture of experienced personnel recruited from the market and those who have been internally trained by the FSA and with an extensive knowledge in cybersecurity. The IT Cyber Monitoring Team has sufficient knowledge not only of cyber security and IT security but also of financial regulations, business profiles of financial entities, and the financial system itself. The IT Cyber Monitoring Team aims to further improve its staff capabilities through on-the-job training and internal training.

36. The IT Cyber Monitoring Team has extensive responsibilities regarding the cyber supervision of the financial sector. These include: (1) developing and operationalizing the cyber strategy for the financial sector; (2) monitoring and inspecting the risks related to cyber and IT system, including data management, of financial entities; (3) planning and implementation of cyber exercises; (4) development of supervisory guidelines and regulations for cyber risk; (5) dialogues on IT governance with stakeholders; (6) analysis of the incidents related to IT system failure; (7) dissemination of threat information to financial entities; and (8) international cooperation.

37. To discharge these responsibilities, the IT Cyber Monitoring Team works closely with external stakeholders, such as NISC, governmental ministries, the BOJ, FISC, Financials ISAC Japan and foreign authorities. The team must work in close collaboration with the vertical supervisory functions, which are responsible for the prudential supervision of different sub-sectors, such as banking, securities, insurance and FMIs. Prudential supervisors of banks, securities, insurance and FMIs are generalist supervisors and do not necessarily have the requisite specialist skills for cybersecurity, and therefore will rely heavily on the expertise of the IT Cyber Monitoring Team.

Figure 2. Japan: Overview of FSA's Internal Organization



Sources: FSA; and IMF staff.

38. Although the roles and responsibilities of the IT Cyber Monitoring Team is clearly defined, it is essential that there is close collaboration between the IT Cyber Monitoring Team and the vertical functions responsible for the supervision of the sub-sectors. Currently, there is interaction between the two sides, and if the IT Cyber Monitoring Team is asked for assistance in supervision, they will provide this. However, there is no structured co-ordination between the horizontal and vertical functions. For example, there have been no on-site cybersecurity inspections of FMIs, and therefore there has been limited collaboration between the IT Cyber Monitoring Team and the supervisory divisions responsible for FMIs.

39. Furthermore, the information gathered between the different divisions and functions (e.g., incident information, threat information, off-site and on-site supervisory data, etc.) could be better used between the different functions to determine the supervisory approach and actions required with regards to cyber risk. For example, weaknesses in access control could have been used to take different types of supervisory action to address such basic hygiene failures.

40. Although the internal governance arrangements at the FSA are well defined, there would be benefit in strengthening the internal coordination between the different functions to ensure that cyber supervision can be more effective and risk-based, and there can be increased awareness of cyber risk amongst all internal stakeholders.

41. The BOJ has established a dedicated IT and cyber monitoring unit staffed with experts. The team is responsible for monitoring and inspecting financial entities that have an account with the BOJ, as well as international cooperation. Furthermore, the BOJ's Payment and Settlement Systems Department is responsible for the oversight of nine FMIs, including the central bank operated FMIs (i.e., its RTGS system—BOJ-NET Fund Transfer System—and the CSD-BOJ-NET JGB Services) on a moral suasion basis.

E. Resources

42. The FSA has an IT Cyber Monitoring Team. There are several team members dedicated to examining and monitoring IT and cyber risks in the securities sector. These teams, together with supervisors of individual financial entities, fulfill various cybersecurity functions that the FSA should fulfill.

43. The BOJ has a financial institution IT and Cyber Monitoring team. It conducts on-site operational risk examinations, including IT and cyber risk.

44. As in most jurisdictions around the world, the central bank and financial regulator in Japan require significant additional resources and tools to fulfill their respective mandates regarding cyber risk. Given the criticality of the risk area and breadth of mandates and responsibilities between the two institutions, there is a critical need for substantial additional resources, approaches, and tools for them to effectively mitigate cyber risk to acceptable risk tolerance levels.

45. In particular, the IT Cyber Monitoring Team at the FSA is under-resourced. The team has responsibilities for supervising more than 1,000 financial entities, as well as developing and operationalizing the cyber strategy for the financial sector, updating the supervisory guidelines, managing cyber incidents, conducting the Delta Wall exercise, etc. Despite the lack of resources, the IT Cyber Monitoring Team has made significant strides in developing the cyber supervision capacity. Nonetheless, the limitation in staff numbers has impacted the capacity to conduct effective regulation and cyber supervision. And given the increase in cyber risk and the criticality of the financial sector, it is essential that the FSA increases its investment and resources in this area.

F. Recommendations

46. The FSA could enhance the cyber strategy over the longer term by developing industry guidance for a broader testing and exercising regime, e.g.**,** threat-led penetration testing (TLPT), purple team testing, and cyber simulations, among others.[4]

47. The FSA should strengthen the governance arrangements and establish a more structured joint supervisory approach between the horizontal (i.e., IT Cyber Monitoring Team) and vertical (i.e., supervisory divisions) functions. Establishing such a process will increase the

[4] Purple teaming means that the testers and the defenders regularly meet and exchange information during the test to maximize the benefits of the exercise.

awareness of cyber risk amongst supervisors and allow a more focused and risk-based supervisory approach. Furthermore, information sharing between the different functions could be improved to facilitate more focused and risk-based supervision of the different types of financial entities.

48. Although the FSA has expended significant efforts to increase its cyber skills and expertise, it should continue to explore means of increasing its capacity to fulfill its role in strengthening the cyber resilience of the Japanese financial sector. The FSA could take into consideration a range of different approaches, such as increasing specialized staff numbers, recruiting highly skilled personnel, upskilling generalist supervisors in cyber risk to reduce pressure on cyber risk specialists, increasing the number of secondments from other agencies, or using different approaches and tools to obtain increased assurance of the financial sector participants (e.g., increased use of third-party independent assurance reports).

INTERCONNECTEDNESS AND FINANCIAL STABILITY

A. Interconnectedness of the Financial System

49. The FSA would benefit from deepening its analysis of the cyber interconnectedness of the financial system. It should be noted that analysis of the cyber interconnectedness, which some refer to as "cyber mapping", is an emerging field, with very few jurisdictions around the world having made any progress in its development. Analyzing financial and technology connections across the sector will help identify potential systemic risks from interconnectedness and concentrations. Assessing interconnectedness of the financial system network is essential for understanding how a shock to one supervised entity/service provider can spread to others. Identification of key nodes in the financial system—for example, the payment and settlement system, financial entities that carry out key services such as clearing and the technology systems underpinning them—could be done to understand cyber risk on a system-wide basis. The mapping of the financial sector network can be used to estimate the impact of a cyber-attack on any of the nodes.

50. The FSA collects relevant information and data, such as identifying vendors and service providers of IT systems used by financial entities for their core business and identifying the status of major external systems (e.g., connections to other systems, participating entities, and providers' operating systems). Therefore, it is possible for the FSA to estimate the approximate extent to which an incident occurring at a particular vendor or service provider could spill over into the financial sector. The FSA continuously collects relevant and important information that can be used as material for conducting the interconnectedness analysis. The FSA would benefit from using the information and data it gathers to carry out analysis of interconnectedness in the financial system, understanding financial network exposures, and identifying the operational dependencies and critical nodes, which would thereby assist in managing potential systemic cyber risk.

51. The FSA has analyzed and documented the different transmission channels that could trigger financial instability via cyber-attacks, including the range of different contagion scenarios that could cause disruption to the financial sector. In each case, the FSA has

documented the potential impact on the system and developed mitigation strategies or actions that will be taken by the FSA to manage the crisis. The FSA has developed a robust set of scenarios and demonstrated clearly that cyber risk can trigger financial instability. It should be noted that conducting interconnectedness analysis, as cited above, will further strengthen the FSA's ability to document additional and more detailed transmission channels and the different potential contagion scenarios.

52. To determine the potential financial stability risk, the BOJ regularly identifies and analyzes the latest trends in cyber threats. It collects data on crime trends such as phishing, ransomware attacks, and fraudulent money transfers, as well as distinctive cyber-attacks through various published materials and interviews with security vendors and utilizes the information from its on-site and off-site monitoring. In addition, ad-hoc surveys are conducted based on latest cyber threat trends, and results of surveys conducted for financial entities are also used to encourage financial entities to implement necessary cyber security measures by, for example, publishing them externally in the Financial System Report (FSR) Annex Series.[5] In publishing such materials, the BOJ demonstrates the importance of cyber risk and provides useful insight to the industry on the risk and actions that can be taken to mitigate the risk.

B. Recommendations

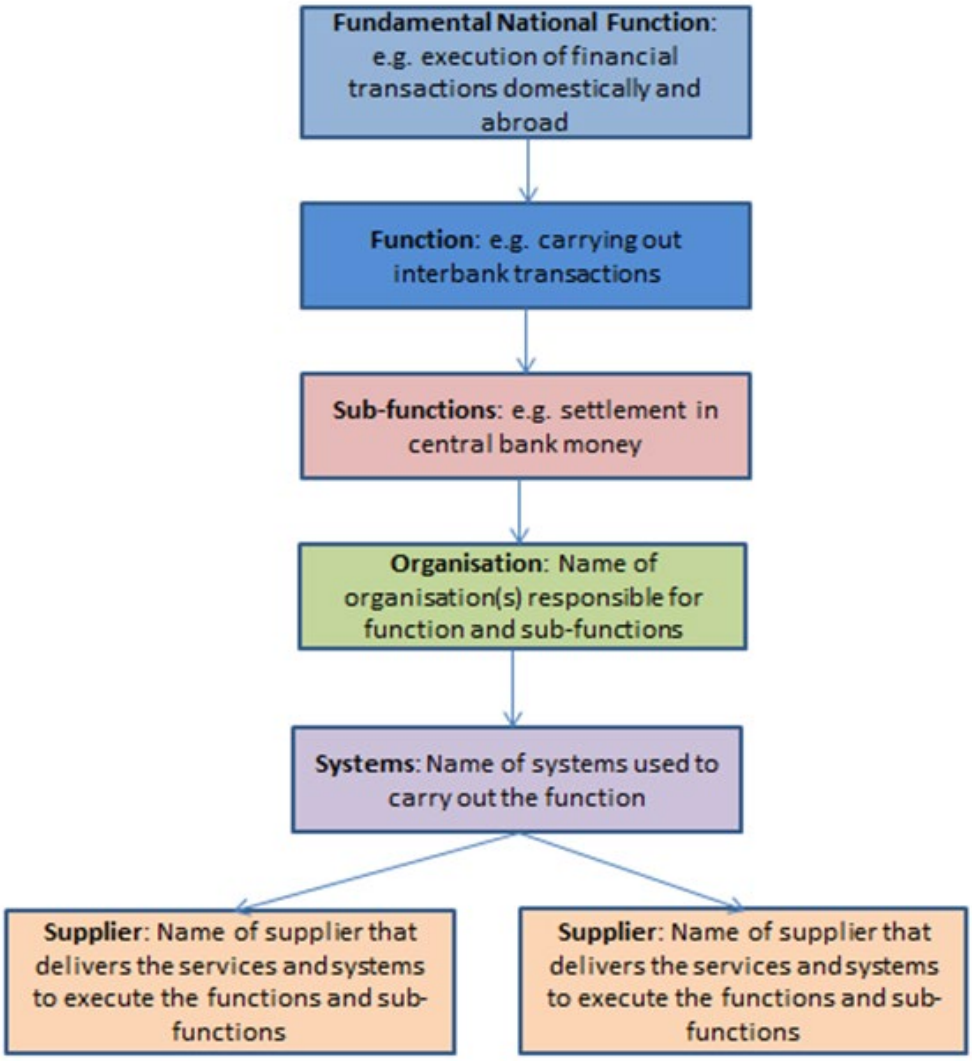
53. The FSA could further strengthen its analysis of how the financial sector is operationally interconnected. This would entail developing network analysis of how the different critical sub-sectors are connected through common technologies and service providers, thereby allowing the identification of critical nodes. The FSA should use this analysis to:

- Identify threats and their impact on the sector;
- Develop a range of different scenarios that could threaten the sector(s) on a systemic level and develop mitigation strategies accordingly;
- Conduct scenario-based tests or stress testing based on cyber scenarios; and
- Improve incident response capabilities.

In developing the cyber map, the FSA could consider the approach described in Figure 3.

[5] https://www.boj.or.jp/en/research/brp/fsr/data/fsrb231019-1.pdf

Figure 3. Japan: Structure of Possible Financial Sector Cyber Map



Source: IMF staff.

CYBER REGULATORY FRAMEWORK AND SUPERVISORY PRACTICES

A. Cyber Supervision

54. The FSA has developed Comprehensive Supervisory Guidelines (CSG) for different sub-sectors in the financial sector that include supervisory expectations regarding risk management posture related to IT systems and cybersecurity. The CSG make explicit reference to the FISC Security Guidelines for guidance related to risk management of IT systems, including cybersecurity. The FISC Security Guidelines were developed by the FISC in cooperation with the FSA,

BOJ, relevant industry participants, and IT system vendors, and have been legitimized as the de facto standards for the financial sector.

55. The CSG has a dedicated section on Information Technology (IT) System Risk. This includes expectations for:

- Governance;
- Control environment for managing IT risk;
- Assessment of IT risk;
- Management of information security;
- Management of cybersecurity;
- IT system planning/development/management;
- IT system audit;
- Management of outsourcing relating to IT system;
- Contingency plan; and
- Response to IT system failures.

56. Of the ten sections in the CSG, one is dedicated to cybersecurity. Although the expectations are detailed and cover some key control areas, they have not been updated since 2015. Currently, the lack of up-to-date and comprehensive cybersecurity requirements on one hand, and the highly detailed and overly- prescriptive FISC Security Guidelines (which exceed 550 pages) on the other hand, may cause a degree of confusion for the financial entities and make it difficult to apply a degree of proportionality.

57. Given the changes in the threat landscape and the increased complexities from technology and digitalization, the FSA should update the CSG for all its sub-sectors to cover cybersecurity requirements more comprehensively. The FSA may consider the categories contained in Annex 1 as part of its update and take into consideration international standards and best practices. In general, advanced financial systems with mature risk management practices benefit more from a principles-based approach. A focus on outcomes rather than prescriptive rules allows for more proportionality and risk-based supervision.

58. From a supervisory perspective, the lack of up-to-date CSGs can stifle effective supervision. For example, large financial entities generally conduct cybersecurity maturity assessments by external vendors based on the U.S. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool. In August 2016, the FSA published a research report titled "Research Study on the FFIEC Cybersecurity Assessment Tool" and provided a tentative Japanese translation of the tool to help those who need to understand it. The FFIEC is a highly complex maturity assessment, which has been designed for the U.S. financial sector. In parallel, the Fundamental Elements by the G7 Cyber Expert Group are used widely, including by entities other

than large financial institutions. In supervising financial entities, the FSA reflects the G7 Cyber Expert Group's Fundamental Elements and the Principles for Financial Market Infrastructures (PFMIs) to its supervisory viewpoint and takes them into consideration. The G7 Fundamental Elements and PFMIs are more principles-based and differ extensively from the FFIEC. In addition, small and medium-sized financial institutions (e.g., regional banks, Shinkin banks) are conducting risk assessments using the Cybersecurity Self-Assessment (CSSA) checklist prepared by the FSA and BOJ. The CSSA is a well-constructed survey, which poses financial entities with 42 questions on their cybersecurity practices. This is a very useful tool to obtain a high-level view of the cyber posture of financial entities. The FSA applied the CSSA for securities companies and insurance companies from 2023 and the BOJ also, jointly with the FSA, does it for securities companies.

59. The tools used by supervisors and financial entities vary significantly from each other, whilst all are sound and credible to provide an insight on the cyber posture of financial entities. There is value in developing a set of tools that are aligned to the CSG, once they have been updated. For example, the CSSA is a very useful tool; however, the 42 questions are not aligned to the CSG and therefore do not provide the supervisor with a view of the financial entities' compliance with the existing CSG. Once the CSG have been updated, the CSSA could be updated with questions that reflect the requirements set out in the CSG. This will enable the FSA to conduct more structured and systematic supervision, as there will be a greater alignment between the regulatory and supervisory frameworks.

60. In February 2022, the FSA published "The Policies to Strengthen Cybersecurity in the Financial Sector (Ver. 3.0)." One of the FSA's policy goals is to enhance monitoring and exercises in order to respond to the new circumstances surrounding the financial sector, including the increasing threat of cyber-attacks.

61. The FSA conducts this monitoring via its on and off-site supervision. During the off-site cyber risk supervision process, the FSA looks at the following areas: (1) corporate governance; (2) risk and internal controls and risk; (3) technical response, third party risk management, and other risk assessments and measures commensurate with the environment surrounding the institution; (4) resilience (including contingency plan, training, and incident response); and (5) audit.

62. On top of this, the FSA conducts through-the-year monitoring of the three mega banks in accordance with the FSA Strategic Priorities July 2022-June 2023. The monitoring focuses on: (1) enhancing group-wide and global cybersecurity risk management posture (three lines of defense, monitoring systems, etc.), (2) third party risk management, and (3) responding to changes in risk profiles, while paying attention to changes in the threat of cyber-attacks.

63. The FSA conducts on-site inspections in accordance with laws and regulations to assure financial stability and customer protection. The FSA selects financial entities to be inspected on a risk basis, taking into account all information it collects and holds. In conducting on-site cybersecurity inspections, the FSA conducts tests to verify the effectiveness of controls at the financial entities in question.

64. Inspections are conducted in accordance with the procedures prescribed in the CSG.

- The FSA will request the submission of necessary documents within approximately 12 business days after the notification of the inspection and investigate the matters to be focused before the on-site inspection through pre-hearing interviews. The on-site inspection lasts approximately four weeks.

- During the inspection period, (1) problems identified up to the pre-hearing will be verified in light of the evidence, discussed with the financial entities, and their background causes will be investigated and identified; (2) facts and problems will be clearly documented and confirmed with the financial entities; (3) a report of inspection results will be prepared by integrating the confirmed facts and problems and it will be sent to the FSA back office for quality control review process including consistency with other inspections; (4) after the review, a high rank official of the FSA will deliver the Inspection Results Notice to the senior management of the financial entity to articulate points requiring improvement.

- When the Inspection Results Notice is delivered, the financial entity will be ordered based on Article 24 of the Banking Act to report the facts behind the findings, self-analysis of the causes, measures for improvement and correction, etc. within a month.

- During subsequent follow-up, the FSA evaluates the concreteness and effectiveness of the improvement plan, requests submission of evidence as necessary, and verifies whether the root cause of the identified problematic issue has been resolved.

- In cases where the entity's cybersecurity management posture is deemed to have a serious problem based on inspection results, etc., the supervisory departments should take actions such as issuing an order for business improvement under Article 26 of the Banking Act.

- Thereafter, the progress of improvement shall be periodically reported to the supervisory departments, and the progress shall be examined until the rectification plan is completed.

- The FSA will make additional interventions (such as business improvement orders) if the self-rectification mechanism does not work and if it is deemed that there will be a serious impact on the soundness of the financial entity, customer interests, or financial stability.

65. The FSA began conducting on-site inspections from 2020 and have recently summarized the lessons learnt from on-site inspections based on experience gathered over the three-year period. However, to facilitate a more standardized and effective on-site inspection, the FSA should update the lessons learnt to align them with the updated CSG. Aligning the CSG and the lessons learnt will allow supervisors to evaluate financial entities more effectively against the supervisory requirements and enable a more standardized and systematic approach to supervision.

66. Following on-site inspections, the FSA produce a supervisory report outlining the findings from their review. Supervisory reports are well drafted and clearly articulate the issues and facts. However, the reports do not link the findings to the risk and impact of the weaknesses

materializing, nor do they indicate the risk rating/severity of the finding and how they should be prioritized, nor which supervisory guidelines/requirements the findings relate to. The FSA could enhance the supervisory reports by including a section that explains the risk/impact of the findings materializing and the severity/rating of the findings, to facilitate better prioritization by the financial entity, as well as the reference to the supervisory expectation/requirement.

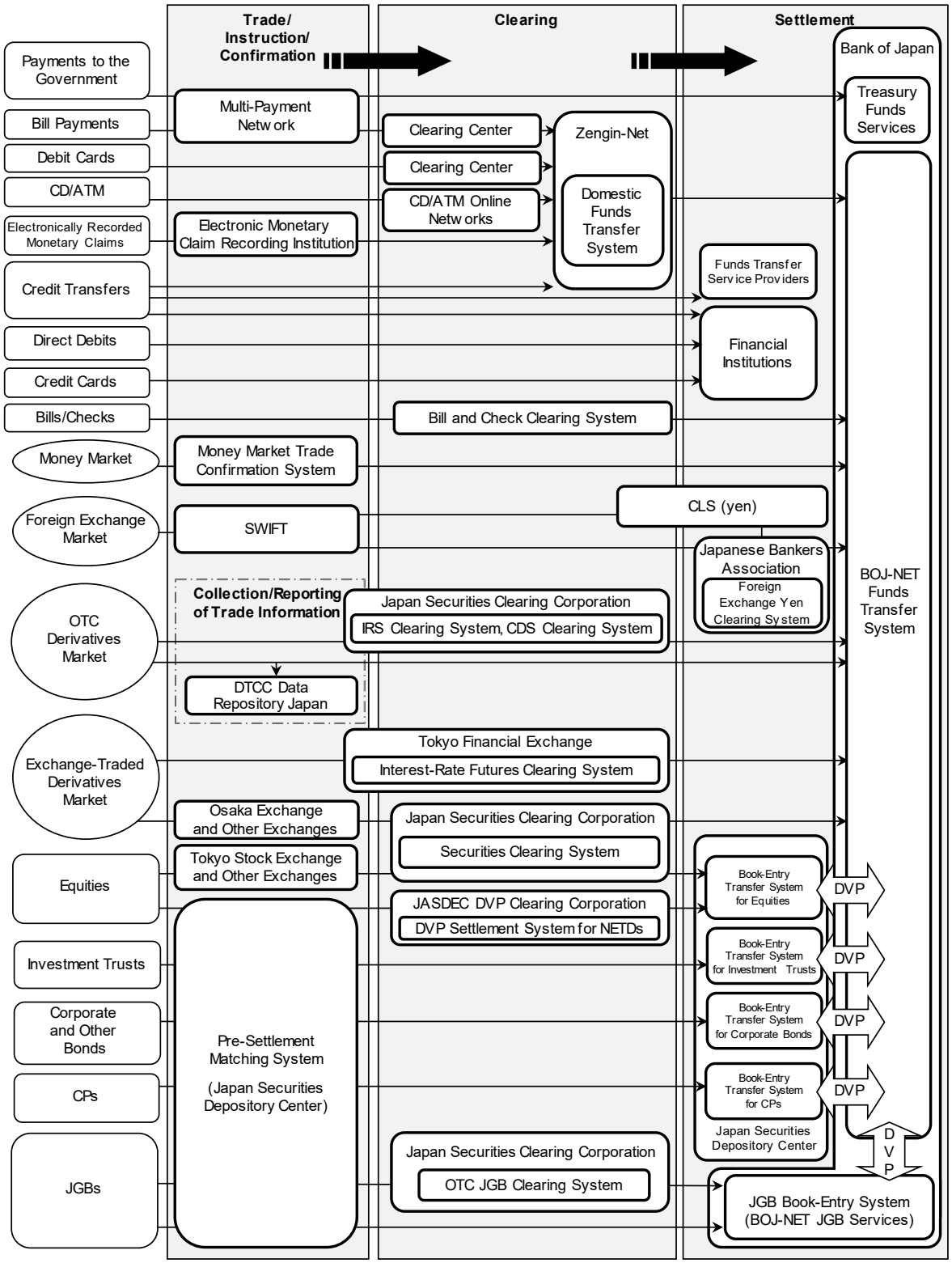
67. In recent years, the FSA has prioritized its supervisory efforts on deposit-taking institutions and securities firms and now intends to assess insurance firms, through off-site, on-site, and surveys (i.e., CSSA). However, there has been less focus on FMIs than banks. The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.

68. Within this context, the Japanese FMI ecosystem is complex, and its smooth functioning is critical for the financial stability of Japan. The FSA regulates and supervises the following FMIs except foreign Central Counter Party Clearing Houses (CCPs): Japan Securities Clearing Corporation; JASDEC DVP Clearing Corporation; Tokyo Financial Exchange, Inc.; Japanese Banks' Payment Clearing Network (Zengin-Net); DTCC Data Repository (Japan) K.K.; Japan Securities Depository Center, Incorporated; and JGB Book-Entry System (BOJ-NET JGB Services).

69. The ecosystem of the payments and settlement systems in Japan is depicted in Figure 4.

70. It should be noted the FSA, in recent years, has not conducted a cyber assessment or on-site cybersecurity inspection of FMIs in Japan, whilst off-site monitoring has been minimal. It is critical that the FSA prioritize the cyber supervision of FMIs, given their critical role in the financial system.

Figure 4. Japan: Overview of Payment and Settlement Systems



Source: BOJ.

B. FMI Oversight - BOJ

71. It should be noted that the BOJ is not a regulator nor prudential supervisor of financial entities. Notwithstanding this, the BOJ oversees nine domestic FMIs, including two central-bank operated FMIs (i.e., its RTGS system—BOJ-NET Fund Transfer System —and the CSD-BOJ-NET JGB Services) on a moral suasion basis.

72. The cyber oversight approach of the BOJ could be substantially strengthened, as set out below:

- The Payment and Settlement Systems Department conducts annual assessments against the PFMIs, which includes Principle 17 (Operational Risk) but there has been no formal cyber-specific assessment of FMIs, including of the central bank operated FMIs
- Not all the FMIs have conducted a self-assessment against the CPMI-IOSCO Cyber Guidance (Guidance) for FMIs
- The FSA and BOJ have not conducted any joint cyber supervision/oversight of commonly supervised/overseen FMIs.
- In the team of nine overseers at the BOJ's Payment and Settlement Systems Department, there is no dedicated cyber expert; although, assistance is provided by senior-official(s) of the Department, as well as the IT and Cyber Monitoring teams in other departments when requested.

C. On-Site and Off-Site Examination of the BOJ

73. In conducting on-site cybersecurity examinations, the BOJ assesses the content of relevant materials (evidence) submitted by financial entities and conducts interviews with the relevant personnel when on-site. In addition, the BOJ visits relevant business departments to visually check whether the cybersecurity-related rules are appropriately operated. On-site cybersecurity examinations are conducted over a period of three weeks to one month, depending on the size of the financial entity.

74. The BOJ checks the status of improvements of any identified issues at the time of the next examination. In addition, the BOJ develops a follow-up policy for each entity identified as having a serious deficiency in its cybersecurity management frameworks and monitors the status of improvement through on-site and off-site monitoring.

75. When conducting the on-site examination, the BOJ uses an On-site Practice Manual and a pre-defined checklist of documents, which provide the basis for its on-site examination. The manual and checklist are well drafted documents and provide adequate coverage for the on-site.

76. The FSA and BOJ conduct off-site monitoring, but there is no structured set of Key Risk Indicators (KRIs) that the FSA and BOJ requests from its financial entities. Cyber threat

preparedness can change rapidly given the activity of the hackers and other digital disrupters. Assessments by supervisors during their on-site examinations give snapshots at infrequent intervals. Given the lack of resources available to conduct on-site examinations, monitoring financial entities on an ongoing basis via KRIs is a useful tool and can increase the overall efficiency of the monitoring activities for the Japanese financial sector. The FSA and BOJ would benefit from establishing an assessment framework that will give them an assessment of the efficacy of controls based on a set of key risk indicators revolving around the required controls and mapped to the inherent risk of the business.

D. Recommendations

77. The FSA should:

- Update its Comprehensive Supervisory Guidelines (for all its sub-sectors), comprehensively covering cybersecurity;
- Align the lessons learnt from on-site inspections, CSSA, and supervisory methodologies/tools to the supervisory guidelines; and
- Include a section in supervisory reports that explains the risk/impact of the findings materializing and the severity/rating of the findings, to facilitate better prioritization by the financial entity, as well as the reference to the supervisory expectation/requirement.

Updating its regulatory framework and its supervisory processes and tools will enable a more structured and systematic approach to supervision.

78. The FSA should increase its off-site and on-site cyber supervision of the FMIs, with the relevant responsible divisions working in close collaboration with the IT Cyber Monitoring Team.

79. The BOJ should further increase and enhance the skills and expertise of its FMI overseers with regards to cyber to address the changing cyber threat landscape surrounding the overseen FMIs.

80. The BOJ should strengthen its oversight approach on cyber resilience for FMIs (including the BOJ-operated FMIs) against the CPMI-IOSCO Cyber Guidance.

81. The FSA and BOJ should enhance their coordination and cooperation to strengthen their supervisory/oversight approach on cyber for commonly supervised/overseen FMIs.

82. The FSA and BOJ should consider developing a set of Key Risk Indicators (KRIs) to improve its off-site monitoring of financial entities.

MONITORING, RESPONSE, AND RECOVERY

A. Monitoring

83. The FSA and BOJ monitor the threat landscape by using a variety of different sources, based on collaboration with public, private, domestic, and international agencies. The authorities assess threats to the financial sector based on threat information provided by (i) the NISC, (ii) the NPA, (iii) financial institutions and FMIs, and (iv) information gathered by the FSA and BOJ themselves.

84. The NISC, which plays a role as the command center for cybersecurity in Japan, widely collects and analyzes cybersecurity threat information (cyber-attack threat trends and product vulnerability information). The NISC disseminates collected and analyzed cybersecurity threat information to the FSA and other ministries and agencies responsible for critical infrastructure. The threat information provided by the NISC is the most important source of information for the FSA and BOJ and plays a central role in assessing cybersecurity threats. The NISC alerts financial entities to threats that are observed to be increasing in severity.

85. The FSA, in cooperation with the NPA, is working to prevent crimes and minimize the damage caused by fraudulent internet banking remittances. Specifically, the NPA shares phishing techniques and damage information with the FSA. In response to increased risks, the FSA encourages users of financial services to exercise caution and requests financial entities to strengthen measures.

86. Financial entities are required by orders pursuant to law to report cyber incidents to the FSA. The FSA analyzes the cyber incidents reported by financial entities, and if a risk is identified that is not limited to damage at an individual financial entity but is common to a wide range of the financial sector, it urges them to exercise caution. In addition, the FSA shares vulnerability information with the Financials ISAC Japan through the Information Sharing Tool (SIGNAL).

87. The FSA's senior adviser in cybersecurity and the Financials ISAC Japan provide the FSA with threat information but on an irregular basis. In addition, FSA staff conduct daily web patrols, including social media and open source, to check the emergence of threats. Based on the information obtained through these activities, the FSA takes appropriate actions, including exchanging opinions and consulting on response with experts, and providing information to relevant organizations.

88. The FSA and BOJ confirmed that like in other jurisdictions, cyber threats in Japan since the COVID-19 crisis have become more sophisticated and malicious. Recently, cyber threats have shifted from the level of money-grubbing and crime for fun by individual actors to attacks aimed at disrupting critical infrastructure operations through sophisticated means by organized criminal groups and actors suspected of state involvement. According to reports from the financial sector to the FSA, the types of attacks that have been seen frequently in recent years include DoS/DDoS attacks and unauthorized logins to their services. On the other hand, looking at the

emerging trend of major cyber incidents according to the degree of materiality, there have been (1) customer data leakage, (2) unauthorized withdrawals of funds due to the misuse of authentication information stolen through phishing, (3) ransomware attacks, and (4) incidents that led to the suspension of business operations, such as the suspension of websites and online transactions. Many of these incidents can be said to be cases of taking advantage of third-party vulnerabilities, such as the misconfiguration of access authority to cloud services or the attacks on outsources.

89. Based on its incident reporting regime, the FSA gathers incident information from its supervised entities and conducts a detailed analysis of the incidents. The analysis is then fed back to the industry.

90. The Japanese ecosystem for threat intelligence is strong, with a range of different public and private bodies providing threat information to the financial authorities. The FSA and BOJ have a broad range of sources to collect cyber threat intelligence, and in conjunction with information from incidents in the sector, provide a good basis for the authorities to understand the threat landscape for the Japanese financial system. However, both authorities could improve their overall analysis of the threat landscape by combining the different sources and developing a Generic Threat Landscape (GTL) Report. The GTL Report could elaborate on the specific threat landscape of the Japanese financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report could consider key financial market participants and their critical functions, including (wholesale and retail) banks, broker-dealers, financial market infrastructures, financial market utilities, and other critical third parties, the different threat actors (including their tactics, techniques, and procedures) targeting these entities, and the common vulnerabilities. By better understanding the threat landscape, the authorities would be well placed to foresee attack patterns and work with the financial entities to better prepare for potential attacks through scenario development, building playbooks and exercising. The GTL could also be used by smaller financial entities, assisting in further broadening access to TLPT in the Japanese financial system, thereby reducing the overall costs of the test.

91. The BOJ should make progress on red team testing (i.e., TLPT) on its ICT environment. Red team tests mimic the tactics, techniques, and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. A red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e., its people, processes, and technologies). It helps an entity to assess its protection, detection, and response capabilities. The BOJ could benefit from a full-scope red team test on the central bank's infrastructure, to test the full range of its protection, detection, and response controls.

B. Response and Recovery

Business Continuity Planning and Cyber Incident Response and Recovery

92. The FSA has a mechanism to escalate computer system failures including cyber incidents, based on the significance of incidents of any financial institutions and FMIs. In the

event of a large-scale cyber-attack, the supervisor of the entity will promptly escalate the incident to senior FSA officials and the Prime Minister's Office and will report the incident to the NISC. To this end, the FSA maintains a contact list with relevant individuals.

93. In addition, if the incident affects not only a single financial entity but also the entire financial sector, the FSA will issue alerts to some or all sub-sectors. At the same time, depending on the content of the information that should be alerted, the FSA will convene a Liaison Council meeting and share information at the meeting. Furthermore, in the event of a cyber incident with international impact, the FSA will share necessary information through the G7 financial authorities.

94. Under the FSA's Business Continuity Plan (BCP), the FSA maintains a list of action and manuals. They include: (1) actions to be taken in the event of an emergency that causes particularly serious damage to the FSA for some reasons; (2) a manual for FSA staff to assemble in the event of a disaster; and (3) a BCP manual to assess the extent of damage to financial entities, monitor the business continuity of priority operations in financial entities, and monitor the appropriate handling of customers by financial entities.

95. In the past, the FSA has issued statements to the public and financial markets in a flexible and timely manner at various times, including at the time of the financial crisis in Japan, September 11 attacks in the U.S., the Great East Japan Earthquake in Japan, and during the COVID-19.

96. In the event of a large-scale cyber incident, the FSA takes prompt actions based on the principles of the BCP. Under this policy, the FSA shares information on cyber incidents with related parties, determines the severity of the incident, and takes specific actions on a case-by-case basis. In doing so, the FSA also coordinates internationally, particularly when incidents have global ramifications.

97. However, it should be noted that the FSA's BCP is heavily focused on earthquakes and does not currently address cyber incidents sufficiently. The BCP states: *"Constant efforts are required to strengthen the business continuity system in the event of an earthquake, etc. Going forward, the FSA will continue to make further efforts to strengthen its business continuity system and request financial institutions to verify its business continuity system, with the aim of building a business continuity system that is resilient to risks such as earthquakes throughout the financial system while continuing to work closely with related organizations"*.

98. The BOJ has a BCP, the basic framework of which was published in 2003. The BOJ's disaster management consists of (1) minimizing the impact of a disaster on its business operations by implementing measures to prevent damage, and (2) ensuring, to the greatest extent possible, continuity of its critical business operations to fulfill the responsibilities it is expected to exercise even in times of disaster.

99. The BOJ faces various potential threats to business continuity. They include: (1) natural disasters including earthquakes and typhoons, (2) man-made disasters including terrorist attacks and cyber-attacks, and (3) technical disasters including power outages and system failures. In this

context, the BOJ has identified three scenarios. The first scenario assumes a case where the Head Office in Tokyo (hereafter the Tokyo Head Office) remains functional, but the main computer center in the vicinity of Tokyo (hereafter the main computer center) is unable to continue its operations. The second scenario assumes that the main computer center remains functional, but the headquarters function at the Tokyo Head Office is affected by the disaster. In the third scenario, it is assumed that the Tokyo Head Office is affected, and the main computer center is unable to operate.

100. Specific action plans differ for each scenario, and in each case, careful consideration is given to how BOJ-NET will continue to operate. In this regard, the operators of BOJ-NET have business continuity arrangements which are regularly tested. To prepare for disruptions related to BOJ-NET and any loss of the computer system, the BOJ carries out system-wide testing of switch-over to the backup center on an annual basis. The test aims to verify the plan's effectiveness, familiarize staff with relevant procedures, and determine areas requiring further improvement. The BOJ-NET operator confirmed that work is ongoing to include a range of extreme but plausible different cyber scenarios in its BCP starting from 2024.

101. In recent years, the BOJ has also developed a Cyber Incident Response (CIR) framework. The CIR framework sets out the governance arrangements for domestic and international cyber incidents, classifying incidents in five categories: (1) domestic incident (i.e. major domestic incident); (2) international incident in Japanese bank (i.e. incident affecting Japanese banks operating internationally); (3) overseas incident affecting Japanese banks (incident that occurs overseas and involves Japanese banks); (4) overseas incident (an incident that occurred overseas and had little impact on Japanese banks); and (5) cross border incident (i.e. incident that has domestic and international impact). For each of these scenarios, the CIR framework sets out the internal governance arrangements to manage the incident.

102. Efficient and effective response to and recovery from a cyber incident by organizations in the financial ecosystem are essential to limit any related financial stability risks. Such risks could arise, for example, from interconnected IT systems between multiple financial entities or between financial entities and third-party service providers, from loss of confidence in a major financial entity or group of financial entities, or from impacts on capital arising from losses due to the incident. Consequently, enhancing cyber incident response and recovery (CIRR) is an important focus for national authorities and such authorities have an important role to play in responding to cyber incidents that present potential risks to financial stability.

103. Given the unique characteristics of cyber incidents, it is essential that the FSA and BOJ keep upgrading, as necessary, a range of extreme but plausible cyber scenarios along with their BCP and CIR framework (i.e., BCP or CIRR for the FSA; and CIR framework and BOJ-NET BCP for the BOJ). It will facilitate them to respond and recovery from cyber incidents that could have sector-wide implications and trigger financial instability. Typically, organizations' plans and playbooks include extreme but plausible cyber scenarios that are based on high-impact, low-probability events and scenarios led by cyber threat intelligence that may result in service failure. Organizations regularly use threat intelligence to update the scenarios so that they remain current

and relevant. These scenarios tests are regularly assessed in business continuity tests and cyber incident response and recovery exercises.

Cyber Exercising

104. The FSA has been running an annual financial industry-wide cybersecurity exercise (Delta Wall) with the aim of further improving the industry's incident response capabilities since 2016. One of the aims of the Delta Wall exercise is to check how financial entities would investigate a cyber-attack, how they would respond, including technical responses, responses from the perspective of customer relations, efforts to continue services and responses for restoration. The participants join the Delta Wall exercise from their workplace, which encourages participation not only from IT division, but also from other relevant divisions, such as public relations, various business lines, and senior management.

105. The 2023 exercise (Delta Wall VIII) included four scenarios for (i) banks, (ii) Shinkin banks / credit unions, (iii) securities companies, and (iv) insurance companies / funds transfer service providers / prepaid payment instrument issuers / crypto-asset exchange service providers. 165 financial institutions participated in the exercise.

106. The findings of the 2022 exercise (Delta Wall VII) were very insightful. The FSA provided the detailed feedback to strengthen the cybersecurity posture to financial entities including non-participating ones, and will do the same for the 2023 exercise.

107. Overall, the Delta Wall exercise is a very well-run exercise, with a range of different scenarios for a broad range of financial entities. The preparation, scenario-building and execution of the exercise is very well done, and the exercise provides deep insight on the capabilities of the industry. The Delta Wall exercise emphasizes ex-post evaluation of actions taken and decisions made by participants during the exercise. Following the exercise, the FSA analyses the exercise findings and provides feedback to the industry, recommends action points to improve its incident response capabilities and shares best practices observed in the exercise.

108. In addition, in 2021, the FSA hosted a desktop exercise at the Liaison Council for Cybersecurity Stakeholders. It was attended by CEPTOARs, JPX, the BOJ, and Financials ISAC Japan to strengthen cross-sector coordination.

109. Furthermore, there are government-led crisis response exercises such as cross-sector exercises (using large-scale scenarios) hosted by the NISC that include participants from outside the financial sector. In 2022, the number of financial sector institutions participating in the NISC's cross-sector exercise was 434, including banks, securities firms, insurance companies, funds transfer service providers, and FMIs.

110. In its role as operator of BOJ-NET and overseer of FMIs, the BOJ is in a unique position to conduct cyber simulations and desktop exercises with BOJ-NET, BOJ-NET participants and other FMIs that have links or connections to BOJ-NET. The goal of the industry-wide cyber crisis

simulation exercise is to rehearse the collective response of the financial sector to major operational disruption. The attack scenarios can vary, but the focus is on collective response capacity. These exercises aim to: (i) test the effectiveness of decision-making and crisis communication arrangements; (ii) validate collective contingencies; (iii) enable participants to practice their response protocols; and (iv) to improve the sector-level response coordination between the public and private, and with other jurisdictions. Such exercises can identify gaps in operational resilience of entities and of financial systems, helping to identify priorities that strengthen response and recovery capabilities. In conducting such exercises, the BOJ would strengthen the responses to potential cyber incidents that could have a material impact on broader payment and settlements systems.

C. Recommendations

111. The FSA and BOJ should consider developing a Generic Threat Landscape (GTL) Report. The report could set out the specific threat landscape of the Japanese financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report could also consider key financial entities and their critical functions, the different threat actors (including their tactics, techniques, and procedures) targeting these entities, and the common vulnerabilities.

112. The BOJ should make progress on red team testing on its ICT environment.

113. The FSA should update its BCP or develop a standalone Cyber Incident Response and Recovery (CIRR) plan, with a playbook of different cyber scenarios, which are regularly tested. The BCP or CIRR plan should set out the governance arrangements and thresholds for cyber incidents that could potentially trigger systemic risk.

114. The BOJ should continue to upgrade its BOJ-NET BCP with a range of extreme but plausible cyber-specific scenarios that are regularly tested, taking into consideration the feasibility of meeting the two-hour recovery time objective (RTO).

115. The BOJ's CIR framework should be regularly tested.

116. The BOJ, as overseer of FMIs and operator of BOJ-NET, should consider conducting cyber exercises and simulations (e.g., table-top exercises) for BOJ-NET with relevant parties (e.g., BOJ-NET participants and other FMIs having link/connection with BOJ-NET) to strengthen the responses to potential cyber incidents that could have material impacts on broader payment and settlements systems.[6]

INFORMATION SHARING AND INCIDENT REPORTING

A. Information and Intelligence Sharing

117. The information and intelligence sharing ecosystem in Japan is mature. There are several external stakeholders that provide the financial sector with threat information and intelligence:

[6] From an FMI perspective, such exercises allow authorities to assess FMI capabilities in meeting the two-hour recovery time objective and end of day settlements following a market-wide cyber crisis simulation.

- The NISC shares vulnerability and threat information with the FSA, who disseminates this information to all financial entities depending on the Traffic Light Protocol;
- The NPA and the Public Security Intelligence Agency share information on trends of cybercrime with the FSA, who in turn sends warnings and useful countermeasures to the financial sector;
- The FSA and BOJ gather information from cyber incident reports from financial entities, which they analyze and feed back to the financial sector;
- Private entities in the financial sector share information with each other through the Financials ISAC Japan, in which 436 financial entities participate; and
- As a framework for sharing cybersecurity-related information across the public and private sectors in the financial sector, the FSA has established the Liaison Council for Cybersecurity Stakeholders, of which the FSA serves as the Secretariat and which includes the Secretariats of the respective financial CEPTOARs, the BOJ, the Financials ISAC Japan, the FISC, and the JPX as members.

B. Incident Reporting

118. The FSA and BOJ have comprehensive cyber incident reporting regimes in place. Both authorities have clear definitions for cyber incidents, severity ratings, templates for reporting and clear procedures for reporting. Their approach places them ahead of other jurisdictions, where developing and operationalizing an incident reporting regime remains a key challenge. Financial entities must report cyber incidents to their respective financial authorities.

119. The incident reporting regime is mature, and the FSA receives incident notifications daily. The IT Cyber Monitoring Team reviews the notifications on a daily basis and is able to judge the severity of each incident. The FSA reviews the incidents annually and produces aggregated analysis of the incidents.

120. The FSA is actively participating in the FSB's Cyber Incident Reporting working group which is developing a standard for incident reporting to achieve global convergence. It would be advisable for the FSA and BOJ to review their existing incident reporting regime and update it in line with the FSB's framework, if appropriate.

C. Recommendations

121. The FSA and BOJ should review whether their existing incident reporting regime is appropriate in light of trends in international CIR discussions, such as those at the FSB.

Appendix I. Comprehensive Supervisory Guidelines: Cybersecurity

1. *Governance*
2. *Identification of Assets*
3. *Technology and Cyber Risk Management*

- Project Management Framework
- System Acquisition
- System Development Life Cycle and Security-by-Design
- System Requirements Analysis
- System Design and Implementation
- System Testing and Acceptance
- Secure Coding, Source Code Review, and Application Security Testing
- DevSecOps (Development, Security, and Operation) Management
- Application Programming Interfaces (API)

4. *IT Services Management*

- IT Service Management Framework
- Documentation
- Physical Controls
- Software Management
- Configuration Management
- Technology Refresh Management
- Patch Management
- Change Management
- Incident Management
- Post-incident Review and Lessons Learned
- Identity and Access Management
- Network Management
- Virtualization Security Management
- Data Security and Privacy
- "Bring Your Own Device" Security Management
- Secured Disposal Management

5. Cyber Security Operations

- Cyber Threat Intelligence and Information Sharing
- Cyber Event Monitoring and Detection
- Cyber Incident Response, Management, and Reporting
- Incident Reporting

6. Response and Recovery

- System Availability
- Business Continuity Management and Disaster Recovery
- Testing of Disaster Recovery Plan
- Backup and Recovery
- Data Center

7. Scanning, Testing, Exercising, and Remediation

- Vulnerability Scanning
- Penetration Testing
- Incident Response Exercises
- Remediation Management

8. Independent Assurance

- Technology Risk Audits

9. Outsourcing and Technology Service Provider Management

- Governance
- Risk Assessment
- Vendor Contracts
- Regulatory Oversight
- Vendor Competency
- Cloud Computing