Initiatives to Strengthen Cybersecurity of Regional Financial Institutions

Shun Miura

Coordinator and
Head of Cyber Security Planning Group
FSA

Policies to strengthen cybersecurity measures in the financial sector (Ver. 3.0)

Changes in cyber space

- **Cyber-attacks have become coordinated and sophisticated** with involvement of state actors is suspected. Such attacks as well as **ransomware attacks** by international hacking groups **occur increasingly frequently.**
- **Providers of financial service have become diverse** due to acceleration of digitalization. In addition**, financial services are increasingly provided via connected services** among different entities, such as cashless settlement.
- **Risk management in financial institutions is getting more difficult** due to expanding **outsourcing markets, including cloud services,** more complicated **supply chain, and globalization.**

Policies for new initiatives

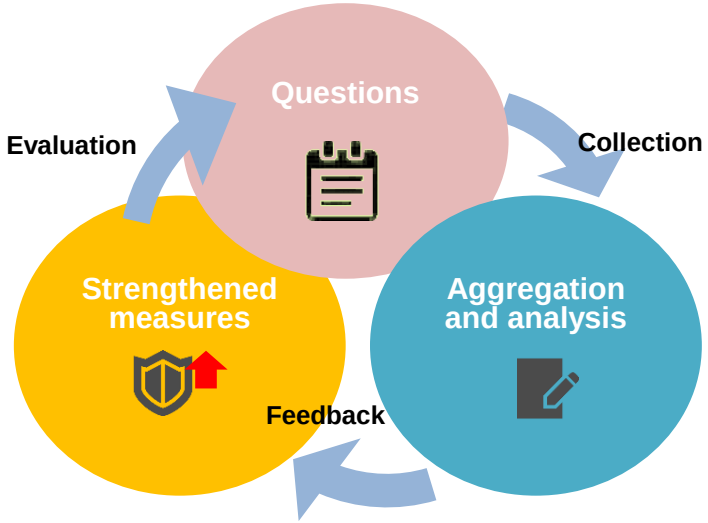
1. Enhancement of supervisory monitoring activities and exercises

FSA will conduct **inspections and other monitoring activities** on a risk-based approach taking into account the size, characteristics and cyber risk of individual financial institution to examine the cybersecurity management posture. FSA will also give feedback about common challenges and good practices to financial institutions through their industry associations to help the financial industry strengthen cybersecurity as a whole. Particularly,

- ✓FSA will monitor for the three mega banks with a focus on their response to changing threat landscape and their efforts to enhance cybersecurity with reference to advanced practices at **overseas major financial institutions**.
- ✓FSA will develop a self-assessment tool on cybersecurity for regional financial institutions and gather, analyze and share the self-assessment results to help them autonomously improve cybersecurity.
- ✓FSA will continue to enhance the cybersecurity exercises taking into account the latest **trends in cyber threat landscape and good practices in cybersecurity exercises in other countries.**

Overview of Cybersecurity Self-Assessment (CSSA)

Challenge	There was not a suitable tool for (i) regional banks, (ii) shinkin banks and (iii) credit cooperatives (regional financial institutions) to assess their cybersecurity management postures compared to peer financial institutions and to identify areas that require improvement.
Action Taken	Financial Services Agency, Bank of Japan and Center for Financial Industry Information Systems jointly developed this self-assessment tool on cybersecurity for regional financial institutions.
Objective	Regional financial institutions autonomously strengthen their cybersecurity measures by utilizing the results of the self-assessment.



Overview of the CSSA Questionnaire

Categories	No. of questions	Specific topics asked in the questions
Board/Management engagement on cybersecurity	4	Management policies and plans on cybersecurity, regular and ad-hoc reporting to management
Identifying and responding to risks related to cybersecurity	4	Information gathering on cyber threat, risk assessment
Internal audit on cybersecurity	3	Scope of audit, recipients of audit reports, and followup policy on audit findings-
Education and training on cybersecurity	1	Education and training programs on cybersecurity
Assessment of new digital technologies	2	Risk assessment for the use of new digital technologies, such as cloud
Asset Management	3	Management of hardware and software
Access Management	2	Control over access rights to critical systems, management of remote access
Data Protection	2	Data protection measures, such as encryption, and backup measures
Log Management	1	Log management policies for critical systems
Vulnerability Management	4	Status of vulnerability assessment and penetration testing, patching policies
Technical measures against cyber attacks	3	Technical measures for user PCs, perimeter defense
Detection	2	Implementation status of monitoring and analysis of threats and scope of monitoring
Incident Response and Recovery	6	Establishment of CSIRT, rules and procedures for responding to cyber incidents
Management of Third Parties	5	Risk management of third parties, security measures for cloud services
(Total)	42	

Results and Next Steps

Results

- Many regional financial institutions consider cybersecurity as an important management issue and are taking steps to improve the effectiveness of their cybersecurity measures.
- They face difficulties in securing human resources and expertise for cybersecurity and managing cyber risk related to third-party service providers.

Next Steps of CSSA

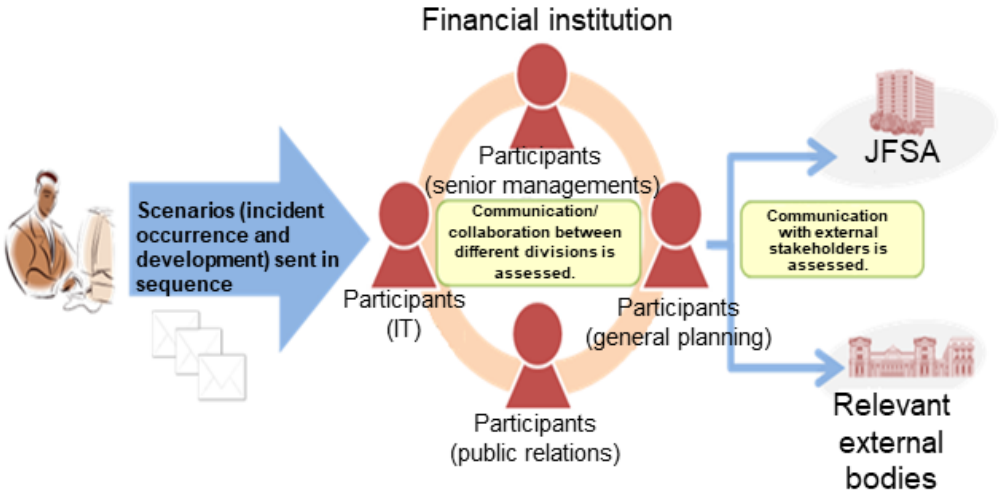
- Improvement of questions
  - Sophisticate questions and options based on the results and feedback from financial institutions
  - Add advanced questions with the aim of further strengthening the security level of financial institutions
- Cross-sector application of the CSSA
  - Apply the CSSA to the insurance and securities sectors

Financial Industry-Wide Cybersecurity Exercise (Delta Wall VII)

- In October 2022, **FSA conducted Delta Wall* VII.** 160 financial institutions and firms participated.

  * Delta Wall stands for the triad (delta) of “self-help,” “mutual assistance,” and “public assistance,” which are key elements of cybersecurity.
- Individuals at FIs can participate in their actual **teleworking environments** that may help FIs improve their response capabilities under such circumstances.
- **Participants need to submit a self-analysis report regarding items to which they could not properly respond.** This is intended to make the exercise more beneficial by clarifying lessons learned through the analysis.

Illustration of the Exercise



Examples of the scenarios

- **Banks**
  - ✓ The exercise was conducted by a blind method. (The scenario was not disclosed at all in advance.)
- **Shinkin Banks, Credit Associations and Labor Banks**
  - ✓ Customer information was leaked. Malfunctions of FI’s websites occurred.
- **Securities Companies and other financial institutions**
  - ✓ Halt of operation systems was triggered by malfunctions in network equipment.