Category	#	Question	Comment
General	1.1	Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?	-The need to create a remote incident response structure (For example, to make SOC research functions availble remotely) -Making various processes digital (Japan has a culture which uses name stamps) -Educating users to protect themselves from phishing frauds etc. -Expanding communication measures that users can trust (DMARC etc.) -There is a need to request communications providers to utilize trusted SMS
	1.2	To whom do you think this document should be addressed within your organization?	
	1.3	How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?	-When we create/update a BCP, we consider scenarios in which a cyber incident ocurrs. We reference NIST Cyber Security framework etc. to create a incident response procedure. -We follow the standards such as NIST, CAT, and FISC.
	1.4	Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.	-We mostly structure our cyber incident response and recovery activities along the seven components set out in the FSB toolkit based on NIST framework . -We are also strengthening our structure using a breach and attack simulation tool.
	1.5	Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	
	1.6	Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	-We set factors such as whether the issue can be handled within one department/unit, or whether the case involves damage which cannnot be covered by insurance, to determine the severity
	1.7	What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	-We would like to request authorities to share information useful for preventing similar attacks from ocurring and spreading in a feasible and timely manner.
Governance	1.1	To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	-We set roles such as the incident owner, regulatory contact, external party contact, emergency response manager, etc.
	1.2	How does your organisation promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?	-We promote a "Bad news first" culture, and place an emphasis on preventing issues from recurring
Preparation	2.1	What tools and processes does your organisation have to deploy during the first days of a cyber incident?	-We ask for external assistance regarding forensics to keep the integrity of the data. -We work with Financial services agency and law enforcement
	2.2	Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	-We enhanced a remote environment for incident response. -We conducted undisclosed scenario drills
	2.3	How does your organisation monitor, manage and mitigate risks stemming from third party service providers (supply chain)?	-We conduct periodical (at least annual) review on security of third party service providers. -We monitor security measures of critical supply chain firms using external services (BitSight).
Analysis	3.1	Could you share your organisation's cyber incident analysis taxonomy and severity framework?	
	3.2	What are the inputs that would be required to facilitate the analysis of a cyber incident?	-Information helpful for analysis would be: 1. Whether physical access is needed, whether attack tools exist externally 2. What privileges are being used in successful attacks and vulnerability information related to the start of attacks, such as the method of attacks. 3. Base Information of IT assets 4. Whether patches are available, and whether they are applied 5. Analysis of malware samples, methods to measure impact scope, eradication methods 6. IoC information
	3.3	What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?	-Drills are effective in measuring the effectiveness of regular CIRR activities. -We analyze logs of security devices to analyze the main cause of incidents. -Preparation of contingency plans, plausible scenarios. -Sharing of lessons learned from incidents.
	3.4	What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	-We participate in Financial ISAC, FS-ISAC etc. and we use that information to predict trends of cyber attacks , and collect indicator data.
Mitigation	4.1	Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?	-Communication with financial regulatory bodies and law enforcement -Share our lessons learned with others.
	4.2	What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?	(i)Monitoring of network connections (ii)Detection of fraudulent alterations (iii)EDR, AV, backup, deception, and third party assessment (i)-(iii) ・Fostering a security first culture ・Collective defense using information sharing
	4.3	What tools or practices are effective for integrating the mitigation efforts of third party service providers with the mitigation efforts of the organisation?	-Transferring data to SIEM including internal/external data -Periodical review
	4.4	What additional tools could be useful for including in the component Mitigation?	-Rapid response to address issues which caused incidents at other companies if we have the same vulnerability. -Ensure external resources for CIRR are always available with effective agreements.
	4.5	Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	-There have been cases we did both at the same time. -Temporary transaction/function restriction gives us resources for recovery and damage control.
Restoration	5.1	What tools and processes does your organisation have available for restoration?	-Conducting drills periodically
	5.2	Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	-Prioritize core banking or payment systems which have deadlines -Already known operational impact and potential impact.
	5.3	How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	-Share information with stakeholders including law enforcement (if needed), and get a mutual understanding -Prompt reporting to executive management

Improvement	6.1	What are the most effective types of exercises, drills and tests? Why are they considered effective?	-Both undisclosed scenario drills and scenario-based drills are effective. Undisclosed scenario drills are practical and scenario-based drills can help us understand steps to be taken and act quickly.
	6.2	What are the major impediments to establishing cross-sectoral and cross-border exercises?	-The prioritization, impact assessment, and reporting line depends on industry -A testing environment that connected with third parties may not exist
	6.3	Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	-Set up an incident response team, and conduct official information sharing to prevent misinformation/misunderstanding.
Coordination and communication	7.1	Does your organisation distinguish “coordination activities” from broader “communication” in general? If yes, please describe the distinct nature of each component.	
	7.2	How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	-We use a few other alternative communicaction tools such as web meeting tools (Webex) and communication tools (Teams, Skype for Business)
	7.3	Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	-Cyber incident guidelines -Sharing of examples, cases (Cases in other companies, best practices in other countries) -Feasible Information sharing including vulnerability information which are reported only to regulators.