

Ref No.: S - 27 /PB.1/2020

July 10th , 2020

**Financial Stability Board
Centralbahnplatz 2 CH-4002
Basel Switzerland**

Re.: Consultation Document on The Effective Practices For Cyber Incident Response and Recovery (CIRR)

We welcome the opportunity to respond to the Financial Stability Board (FSB) consultation report on the Effective Practice For Cyber Incident Response and Recovery (CIRR). We have consistently called for holistic study of the development of banking regulatory reforms, including the FSB financial regulatory reform, which has accordingly been adopted to best fit the Indonesian banking conditions. As the Deputy Commissioner I Banking Supervision of the Indonesian Financial Service Authority in charge of the Department of Banking Research and Regulation, I present our view on the consultation report on CIRR.

In summary, we are strongly supportive and commend the consultation report on CIRR. The current Covid-19 pandemic has taught us the importance to have a robust CIRR framework. It has created an abrupt need for banks to move out their corporate facilities into virtual environment. Moreover, the digital era has encouraged banks to transform their business into digital. The shift of this magnitude poses risk arising from major cyber incidents that could seriously disrupt financial systems. Thus, effective CIRR is very important to address the risk.

The consultation report notes that FSB would publish a final report on CIRR. It lists 46 effective practices that are structured into seven components. It underlines that the effective practices serve as toolkits of options rather than one-size-fits all manner. We strongly agree with this principle-based approach.

While the effective practices in the consultation report are already comprehensive, there are several areas requiring further explanation or clarification as follows:

1. The toolkits have yet discussed the role of the board to set out risk appetite, to determine and approve strategic plan and written policies and procedures, to conduct periodic monitoring and evaluation and to take prompt action to respond to and recover from cyber incidents.
2. The level of management acting as Scribe/Independent Observers should be clarified in order to provide a clear guideline.
3. The detection process of cyber incident has not clearly stated in the toolkit. Accurate detecting and assessing possible incident is very important in order to resolve the incident and mitigate the impact.
4. The investigation of the cyber incident has yet clearly stated in the toolkits. Specifically, the toolkits do not provide effective practices for evidence gathering and/or handling and investigation or identifying the attacking hosts. The evidence gathering and handling is imperative to resolve the cyber incident.

We offer the following comments in response to select questions posed by the FSB's consultation report:

General

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?*

During the current COVID-19 pandemic, we learnt that remote working and emergency working protocols are important. The sudden change of working condition make the supervisory measures for banks regarding cyber incident become more challenging, especially in analysis/investigation and recovery process. Both supervisors and Bank's employees are working in isolation; therefore incident reporting and prompt action are not conducted immediately.

2. *To whom do you think this document should be addressed within your organisation?*

- Deputy Commissioner I Banking Supervision (in charge of the Department of Banking Research and Regulation)
- Deputy Commissioner III Banking Supervision and Deputy Commissioner IV Banking Supervision (in charge of the Department of Banking Supervision)

3. *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.*

OJK has issued regulations that included the cyber incident response and recovery with components quite similar to the FSB toolkit. Specifically, OJK has issued the Regulation No. 38/POJK.03/2016 regarding Implementation of Risk Management of Information and Technology by Banks as amended by OJK Regulation No. 13/POJK.03/2020 and OJK Circular Letter No. 21/SEOJK.03/2017. These regulations set out cyber incident response and recovery as a part of the banks' IT framework. However, these regulations outline several other components, such as:

- a. IT risks assessment, measurement, and monitoring. Some risks that correlated to IT are including operational risk, compliance risk, legal risk, reputational risk, and strategic risk.
- b. Procurement standards and procedure for vendor/third party that carried out cyber services providers, including subcontract activities conducted by vendor.
- c. Incident response procedure (helpdesk and power user management).
- d. Database management policy.
- e. Exchange of information policy.

In addition, OJK has issued Regulation No. 39/POJK.03/2019 regarding Implementation of Anti-Fraud Strategy, which included cyber utilization as a type of fraud. Based on the regulation, Banks are required to establish a special Anti-Fraud unit and Anti Fraud strategy that consists of:

- a. Prevention (anti fraud awareness and culture, vulnerability identification, and know your employee).
- b. Detection (whistleblowing system, surprised audit, and supervisory system).
- c. Investigation, reporting, and detention.
- d. Monitoring, evaluation, and follow up.

4. *What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?*

As mentioned above, OJK as financial service authority has issued regulations to provide guideline for banks to establish a safe, standardized, and integrated cyber incident reporting system to escalate industries' report in case of cyber incident occurred. Furthermore, OJK assesses the banks' information technology, including cyber incidents as part of the operational risk assessment periodically.

Governance

5. *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?*

OJK set out the Bank's management role and responsibility as follows:

- a. The responsibility of the boards (it is worth mentioning that the Indonesian corporation law adopted two-tier board system comprising the Board of Commissioners and the Board of Directors)
 - The board of director has responsibilities to set IT risks appetite of the organization, to set IT strategic plan, effectively implementing risk management of IT, set written policies and procedures including conducting socialization effectively, conduct periodic monitoring and evaluation, and conduct prompt action if necessary to respond and recover from cyber incident.
 - The board of commissioners has responsibilities to evaluate and monitor the cyber incident response and recovery, and evaluate Directors' responsibility regarding cyber incident response and recovery.
- b. The IT Steering Committee has responsibility to assess and provide recommendations to the board of directors on the implementation of IT risk management, including cyber incident response and recovery.

Preparation

6. *How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?*

The OJK regulations required banks that use third party service providers to:

- a. Take full responsibility of the IT risk management, including cyber incidents response and recovery
- b. Conduct due diligence to asses third-party service providers candidate's reputation, technical capacity, operational capacity, financial resources, development plan, and innovation ability with evolving market.

- c. Oversee and evaluate the performance of third-party service providers periodically.
- d. Ensure that the third-party service providers grant access to intern and extern auditor and also authorities (OJK), to audit or supervise and provide data or information if necessary.
- e. Ensure that the third-party service providers are chosen by cost and benefit analysis, have a sufficient human resources and experts, implementing the information technology control proven by the result of independent auditor, keep Bank's confidentiality, reporting any critical incident to Bank, and providing a sufficient Disaster Recovery Plan.
- f. Ensure that the third-party services providers' responsibility are set forth in the written agreement.

Analysis

7. *What are the inputs that would be required to facilitate the analysis of a cyber incident?*

Based on best practices, to make cyber incident analysis more effective, organization must build an incident response team, comprising highly experienced and proficient members, to analyze the precursors and indicators effectively and efficiently and to take prompt corrective actions. The incident response team should promptly work to analyze and validate each incident, following a pre-defined process and documenting each step taken. When the team finds that an incident has occurred, the team should perform an initial analysis to determine the incident's scope, including affected networks, systems, or applications; origination of the incident; and root-caused of the incident.

Mitigation

8. *Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?*

Protecting confidential information and data, company's reputation, and maintaining report to the management and authorities in a timely manner.

9. *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) Tools to mitigate the impact of data breaches include:
 - a. Identifying type of data breach incident.
 - b. Mandatory reporting for every data breach indication.
 - c. Establishing the Data Security Incident Response team or task force if necessary.
 - d. Reviewing and monitoring the effectiveness of policy, standard, and procedure of data security.
 - e. Monitoring the method or technical issues that threatening Bank's data security system as preventive measure.

- (ii) Tools to mitigate the impact from loss of data integrity include:
 - a. Implementing method and procedure to reduce external threat such as virus and malicious transaction that can affect data integrity.
 - b. Creating audit trail as key to learn about data throughout the different stages.

10. What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?

Insurance to cover the potential loss caused by cyber incident. Bank must assess the scope of insurance, cost, and the coverage provided by the insurance.

Restoration

11. What additional tools could be useful for including in the component Mitigation?

Restoration tools and processes for cyber incidents are as follows:

- a. Policies of Disaster Recovery Plan coordinated by Disaster Recovery Plan task force that based on sufficient business impact analysis and risk assessment.
- b. Procedures of Disaster Recovery Plan including emergency response – immediate steps, system restoration procedures, data synchronization procedures, disaster recovery center, and data backup adequacy.
- c. Disaster Recovery Plan tests periodically.
- d. Disaster Recovery Plan maintenance and internal audit.

12. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?

OJK required Banks to implement restoration activities as a part of their operational risk management framework. The restoration scenario is determined based on critical activities, functions, or services of the Banks.

13. What are the major impediments to establishing cross-sectoral and cross-border exercises?

The major impediment has been different regulations or standards among countries, particularly on data protection and cyber security.

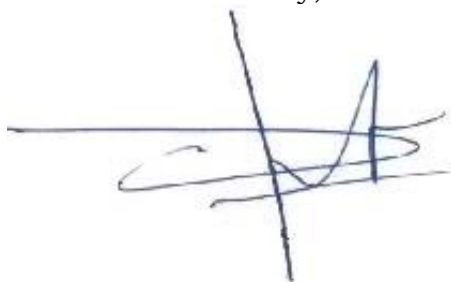
14. How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?

To address the possibility the unavailability of traditional communication during cyber incident, OJK required banks to conduct risk control and monitoring of communication line. Bank must assess the possible risks that may occur, such as loss of data or information, loss of data integrity, flaw of transmitted data, loss of confidential data, communication line unavailability, and loss or damage of communication line. Therefore, Bank must set action plan to control and mitigate the risks mentioned above by doing assessment on capacity planning of communication line; media of communication line; backup, alternative routing, and alternative provider; logical and physical security; and audit trail availability.

In conclusion, we appreciate the opportunity to respond to the consultation report on CIRR. This is important subject in the current Covid-19 pandemic and digital era. We appreciate your attention toward understanding how international best practices may affect our policy and regulation. We look forward to engaging with you on this topic and on future areas of regulatory reform.

For further information, kindly contact Tony (tony@ojk.go.id), Diar Lasrumondang (diar.lasrumondang@ojk.go.id), and Aninda Nusratina (aninda.nusratina@ojk.go.id).

Yours sincerely,



Teguh Supangkat

Deputy Commissioner I Banking Supervision
Indonesian Financial Service Authority