28 February 2022

To:
Otoritas Jasa Keuangan (OJK)
Department of Banking Research and Regulation
For the attention of: Rizki Yuniarini ; Aninda Nusratina

Submitted by email to: Rizki.Yuniarini@ojk.go.id; aninda.nusratina@ojk.go.id; humas@ojk.go.id

ASIFMA response to OJK Consultative Paper on Commercial Bank Cybersecurity Risk Management

Dear,

ASIFMA[1] and its members welcome the opportunity to respond to the Otoritas Jasa Keuangan (OJK) Consultative Paper on Commercial Bank Cybersecurity Risk Management (Manajemen Risiko Keamanan Siber Bank Umum).

We respectfully submit that any new cybersecurity guidance should be consistent with existing global best practices, be principles- and risk-based, and focused on firms' ability to demonstrate security capabilities and outcomes in proportion to their size, complexity, and risk appetite. The Consultative Paper references some examples of existing global best practices include NIST Cybersecurity Framework, and ISO/IEC 27001 Information Security Management among others.

We encourage OJK to align with more international standards and best practices related to cybersecurity, in particular, the Financial Services Cyber Profile (also called Financial Sector Profile or "FSP" or the "Profile"). The Profile is based on the NIST Cybersecurity Framework, and tailors controls specifically to the financial sector by synthesizing the best cyber practices from industry, as well as regulators in different jurisdictions. The Profile is increasingly used and recognized around the world by regulators, international standards setting bodies and industry bodies. In April 2021, Royal Bank of New Zealand referenced the Profile as

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.

"recommended frameworks for entities to refer to" alongside NIST Cybersecurity Framework and others in its Guidance on Cyber Resilience[2] .

The financial industry seeks coordinated cybersecurity regulation across the globe that would enable financial market participants and countries to align cybersecurity efforts to mitigate cyber risk impacting financial stability. The Profile represents financial industry's policy harmonization effort as disparate requirements consume precious resources and weaken industry's security posture. Additionally, prescriptive and conflicting regulatory requirements can result in misalignment of organizations' cybersecurity investments.

In this spirit, we would like to provide more detailed comments, including but not limited to the need for Banks to be able to leverage global frameworks, the frequency and approaches to cyber incident reporting, cybersecurity maturity level assessment and cybersecurity awareness training.

Article	**Comments and Suggestions**
Article 8	We seek clarification on the relationship between the consultation and the existing OJK regulations covering cybersecurity and technology controls, namely 13/POJK.03/2020 and 21/SEOJK.03/2017 and 12/POJK.03/2018. We recommend OJK to articulate how the existing controls in 13/POJK.03/2020, 21/SEOJK.03/2017 and 12/POJK.03/2018 align with this guideline, ensure requirements are consistent and specify which one will take precedence if any divergence.
Article 11	In addition to the applicable laws and regulations related to cyber security, OJK should ensure that the provisions are aligned with other OJK regulations on Information Technology Risk Management and Commercial Bank Risk Management, including the implementation provisions specifically related to Banks Soundness, in particular, how to align the assessment with the banks' risk profile.
Article 16	We hope OJK will align the sources of cyber security risk with those in the working paper on the assessment of the bank soundness of commercial banks, especially regarding operational risk and clarify whether a separate assessment on cyber security and operational risk is required given that it contains many of the same component coverage i.e. human resources, systems, process, and external factors.
Article 23	We recommend OJK to provide an Inherent Risk Assessment Template similar to other regulatory initiatives such as the Hong Kong Monetary Authority's Cyber Resilience Assessment Framework 2.0 (HKMA CRAF 2.0) and Bank of Thailand Cyber Resilience Assessment Framework (BOT CRAF) to provide more measurable metrics and avoid any ambiguity in identifying the risk levels for Inherent Risk Assessment.
Article 25	We seek clarification that banks can leverage existing Board or Board delegated committee to fulfill this requirement and we propose allowing a bank to leverage its

[2] https://www.rbnz.govt.nz/news/2021/04/reserve-bank-publishes-cyber-resilience-guidance

	current governance/ organizational structure in accordance with the bank's business model.
Article 28 ,29, 36, 37, 39, 58, 91, 133 and Section B.1.4	We would like to clarify the role of "Board of Directors" and "Board of Commissioners" referenced in the consultation. Under the dual board structure in Indonesia, we seek confirmation that "Board of Directors" here is equivalent to "Senior Management" in other jurisdictions who are undertaking day-to-day managerial responsibilities and that "Board of Commissioners" is equivalent to "Board of Directors" in other jurisdictions who are responsible for oversight. We recommend alignment with firms' existing governance structure where operating level functions are managed by senior management equivalent in Indonesia and oversight is performed by Board equivalent in Indonesia. For global banks operating in multiple jurisdictions, it is key for them to be able to implement a scalable and consistent global framework and leverage firmwide support from Global and Regional functions/Committee on the Governance, control and others. Therefore, we recommend that the Guideline recognize global framework and existing governance structure and allow global banks to adopt global frameworks that have been instituted at Group level to fulfil requirements in the guideline. 29(a) - A foreign bank branch will be subject to the provisions of the Group. We suggest the OJK confirms that the written strategic policy and cyber security risk management framework including cyber security risk limit can follow and leverage the applicable Group's provisions. 29(h) - For most international firms it is market practise that cyber security risk sits under the management of the Regional Information Security Office. As such we hope the OJK can confirm that firms can leverage such existing regional group teams depending on the firms' business model and setup. 29(j) – For a foreign bank branch, the requirement to report to the Board of Commissioners will follow the applicable bank's governance process. We ask OJK to provide separate stipulation for foreign banks.
Article 29 (a)	See our response above, we believe global banks should be allowed to leverage group level cybersecurity risk management policies, strategies and frameworks. We ask OJK to confirm that the written strategic policy and cyber security risk management framework including cyber security risk limit can follow the applicable Group's frameworks.
Article 33	As stated above, we ask OJK to consider allowing a foreign bank to use its current bank policies including risk level and cybersecurity risk tolerance.
Article 36	Article 36 states "the organizational structure must be designed to ensure that the work unit that performs the internal control function on cyber security risk management is independent of the business work unit."

	We would like to seek confirmation that the OJK requirement is consistent with the industry general practice that risk management function sits in the 2nd line as part of the 3-line of defense model.
Article 38	We believe a bank should be able to leverage the current party who is handling cyber security risk management.
Article 40 (f), 130 and 133	The term "Cyber resilience testing" has very broad meaning and could cover a wide range of cybersecurity assessment and exercise such as table-top exercise and others. Based on article 130, the "cyber resilience testing" refers to penetration testing and we recommend that the guideline clearly and consistently define the term throughout the document. We also suggest OJK clarify whether cyber resilience testing of the bank's overall risk profile indicate that cyber security risk will also be integrated into the bank's risk profile report or whether it becomes a separate risk assessment although the cyber security risk elements are the same as for operational risk i.e. human resources, processes, systems and external factors.
Article 47	We recognise the importance of cybersecurity related education and training. Banks periodically conduct cybersecurity awareness training and activities such as phishing test to enhance employee's cybersecurity awareness. In view of the extensive coverage of cybersecurity training activities performed, we suggest the guideline to focus on outcome and allow banks the flexibility to define frequency of the education and training related to cybersecurity. We also ask OJK to consider firms' internal standards and if there is no significant difference between the standards of OJK and those of the bank, the bank should not be obliged to participate in the human resource capacity building program issued by the cyber security agency.
Article 59	We would like to seek clarification that the term "Limit Setting" here refers to Risk Appetite/Threshold?
Article 79	We recommend that further clarity on 'hard copy' could be provided. The key IT policies and operating procedure are available online with recovery capabilities.
Article 64	Foreign bank branches typically adopt the data protection policy issued by their head office. We ask that a foreign bank branch can refer to the group policy without being required to adopt a new data protection policy at the branch level.
Article 80 (l,m)	Referring to several events in the past, related to the provisions in this article, we see the importance of exceptions, especially regarding the dependence on update support from existing applications, with applications provided by regulators/SROs in Indonesia where these applications still use software components which no longer

	received support from the principal, or the version has not been updated to the recommended version. This is to maintain the bank's business continuity process where the bank avoids any issue in the implementation of the application whose software has not been updated by the principal.
Article 80 (n)	We suggest OJK allows Indonesian branches of foreign banks to follow its standard control procedures and assessment frequency of configuration management that have been determined by the head office/group according to the group' needs.
Article 82 (e)	We noted the guideline requires banks to use "authorized cloud storage" and would like to seek clarification on the requirement. We recommend that the guidelines allow banks to choose cloud service providers (CSPs) that best suit their business needs while properly managing risks of using CSPs.
Article 86 (d)	We would like to seek clarification on the expectation of independent testing and recommend that the guideline recognize firm-wide independent testing conducted globally.
Article 87 (d)	Article 87 (d) requires banks to prioritize events (events) in log by severity/impact, and safety category while monitoring suspicious activity. We seek confirmation that banks could define its own categories for prioritizing events.
Article 92	We ask OJK to consider allowing Indonesian branches of foreign firms to leverage the existing incident team who will actually cover all incidents in the bank including cyber incidents.
Article 101	Financial sector adopts three lines of defense as the common best practice. We would like to seek clarification if the Risk Management Unit described in this article referring to 1st line cyber risk management function or 2nd line of defense.
Article 102	We suggest OJK issues more detailed guidance regarding reporting standards from the bank to OJK.
Article 107 and 108	We would like to seek clarification on Internal Control System, in particular whether the system refer to a Control Framework rather than a Technology Application/system.
Article 111	The Bank is required to perform periodical review and evaluation regarding the implementation of cyber security risk management carried out by the cyber risk management function and the internal audit work unit. 111(1) - Regarding the cyber risk management function, we suggest the OJK clarifies whether foreign bank branches in Indonesia are required to establish a new function or may leverage the existing functions in accordance with the bank's business model. We suggest the latter.

	111(2) - Currently, the bank has conducted its periodical review and evaluation on system security which also required by OJK regulations regarding IT Risk Management and Bank Indonesia regulations, especially the payment system where banks are required to review at least 1 (one) time in 3 (three) years. We ask OJK to harmonize the review requirement and if it contains equal elements, we believe OJK should consider allowing the bank to use the same review to ensure efficiency from a resource perspective.
Article 111	Article 111 states that "Banks must periodically review and evaluate the implementation of cyber security risk management. Review and evaluate it carried out by the work unit that handles the cyber security risk management function and the internal audit work unit. The review and evaluation are carried out at least once every year." We would like to seek clarification that the work unit that handles cybersecurity risk management function refers to 2nd line of defense. Annual IT audit requirement is mandated by existing IT Risk Management by Commercial Banks regulations (POJK Number 38/POJK.03/2016 as amended by POJK Number 13/POJK.03/2020 and SEOJK Number 21/SEOJK.03/2017). We would like to seek clarification whether OJK expects an annual cybersecurity audit to be performed following the existing regulations. We recommend OJK to harmonize the Internal Audit's annual audit requirements across these regulations and avoid duplicated requirements.
Article 113 and 114 and 117	We suggest to include language for Internal Audit coverage over cyber security risk management on risk-based approach which commensurate with the criticality and the risk. We propose that the review and evaluation carried out by the internal audit can be based on a risk-based approach to systems/applications with high risk with a period that is aligned with other provisions as stated in the entry of article 111 above.
Article 119 Article 120 Article 122 Appendix B Article 126 Article 135 Article 137	We would like to clarify if Banks are expected to perform all 3 self-assessments, i.e. Inherent Risk Assessment, Assessment of the Implementation of Cyber Risk Management and Maturity Assessment twice a year. Considering the assessments are resource intensive and the results may not be meaningful if the identified remediation has not be largely completed and the overall control environment is not varied that much in a short time frame, we suggest to change the frequency for the self-assessment to once a year or varied according to the result of inherent risk assessment, to allow banks to allocate resources on actual controls and protect themselves. FI's should have the flexibility to leverage existing routines (Global / Regional) as well as decide the intervals at which those need to be conducted. FI's should be allowed to follow their own internal categorisation using risk-based

	principles. To allow banks to properly assess risks, we recommend the guidelines to provide 12 months' time for banks to complete the first assessment. The guideline does not provide detailed clarity on how the 3 assessment will come together taking a risk-based approach. We recommend OJK to provide acomprehensive risk matrix (Inherent risk rating, Control maturity and overall implementation status) for the 3 assessments and also detailed list of control objectives for the 3 assessments. As outlined in the general comments section, we recommend OJK can consider leveraging FSP as an international best practice and harmonize requirements for banks. In "Appendix C", the characteristics defined in the 'Definition of Rank' column are fixed and standardized according to the rating. We seek clarification on a possible scenario that certain characteristics are strong, certain are normal and some may be weak. As the definition is too general and banks may demonstrate strong on some and normal on others, it would present challenge to accurately decide on rating based on the definition.
Article 130, 131	Regarding the penetration test, we suggest the OJK to consider that firms may use the bank's methodology and frequency in-line with the bank's head office. We believe there is no need for separate testing other than what the bank has done by referring to the group provisions as long as the scope and methodology set by the head office are in accordance with or in line with the provisions OJK.
Article 132	In conducting the periodical scenario-based cybersecurity testing, it is expected that the bank may use its existing test result by referring to head office's provisions and by ensuring that the scope and methodology of testing are in accordance with OJK regulations.
Article 133, 134 and 137	We seek clarification on "cybersecurity resilience test" and 'cybersecurity defense test results report', specifically on the kind of test it refers to (e.g. attack simulation or red-team report, blue-team report, cyber resilience drill report, penetration testing report etc.). If cybersecurity resilience test refers to penetration testing (pen-testing), it is important to recognize that pen-testing test results are sensitive and disclosure to any party outside of Banks would pose cybersecurity risks to Banks. We recommend the guidelines take into consideration of sensitivity of testing results and risks of sharing the sensitive results. Additionally, we recommend that the guideline recognize firm-wide independent testing conducted globally or in other jurisdictions. The mutual recognition mechanism is also reflected in HKMA's CRAF 2.0 where HKMA allows more flexibility for banks to leverage the results of similar cyber resilience assessments performed by their banking groups or headquarters. There are several reports that must be submitted by the bank. As mentioned above, a bank is required to submit their self-assessment of risk management maturity level,

	cyber incident report and cyber resiliency test results reports. We suggest the OJK provides detail requirement regarding the cyber resiliency test report to support the explanation in art 137 above.
Article 134	We recommend more clarity on 'regular basis'.
Article 135	Referring to article 119 above, in line with globally accepted principles, FI's should have the flexibility to leverage existing routines (Global / Regional) as well as decide the internals at which those need to be conducted. FI's should be allowed to follow their own internal criteria using risk-based principles. Alternatively, we hope the OJK can consider an annual self-assessment report (instead of semi-annual in June and September).
Article 136	**Notification trigger**: The initial incident notification time frame of 24 hours is administratively difficult to comply with given the broad range of information required as per Appendix A. We would instead propose for an open-ended time frame of "as soon as possible after an incident that could materially disrupt, degrade and impair Banks, its clients or financial stability is known by the senior management of Banks's cybersecurity, privacy or technology organization". This would allow for Banks to make a more definitive determination on the event and prevent the notification of false positives. **Incident requiring notification**: We would suggest to make clear that only *actual* incidents need to be reported, so as to exclude attempts at a breach of Banks' environment which may create white noise and notice fatigue. The same comment is applied for Article 136(b) and Chapter VI where relevant. For the monthly incident report, we recommend that banks are not required to submit monthly cyber incident report there is no incident. It would create administrative burden to both Banks and OJK without added value if monthly report is required even if there's no incident. **Continuing notifications.** We would suggest for the obligation to provide updates on the change in conditions to be replaced with an obligation to provide updates where requested by the supervisor, as is the position adopted by other regulators in the region such as MAS and HKMA. We suggest changing the language as follows: "Initial incident notification needs to be submitted by the Bank as soon as possible to the supervisor ~~no later than 1x24 hours~~ after ~~the~~ an actual incident that materially impacts Banks, its clients or financial stability is ~~known~~ notified to senior management within cybersecurity, privacy or technology organization through e-mail or other means of communication. The scope of incident notification includes brief incident details and initial impact assessment. After the initial incident notification, the Bank may be requested by the supervisor to provide further updates on the relevant incident. ~~In the event of a change in conditions or at the request of the supervisor, the Bank may submit updated information on the incident notification~~." 8

	We also submit that in case there are no cyber incidents, banks should not be required to submit monthly reports to OJK. If there is a mechanism for disclosure of information to cyber security agencies, we suggest this should be supported by a non-disclosure agreement considering that customer consent is only limited to information disclosure to bank's groups and its affiliates as well as third parties who provide services to the bank.

We are grateful for the opportunity to share our feedback on the Consultative. We hope our suggestions will be reflected in the final framework and are more than willing to discuss our response in more detail during a meeting during which we can invite representatives of the Cyber Risk Institute as well. We remain at your disposal for any questions you might have in relation to the above response.

Best regards

Laurence Van der Loo

Executive Director Technology and Operations

ASIFMA