KPMG

KPMG Cyber Newsflash

Cyber security and resiliency for Indonesia banking sector

The increase in the access and connectivity of information technology (IT) could potentially increase cyber risks in banking. Currently there is no regulation regarding cyber resilience in the banking sector. Therefore, to support the digital transformation and cyber resilience of the banking sector, *Otoritas Jasa Keuangan (OJK)* has issued *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022* about *Penyelenggaraan Teknologi Informasi oleh Bank Umum* (POJK 11 - PTI). This replaces *Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016* about *Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum* (POJK 38 - MRTI).

On 27 December 2022, OJK Circular Letter *Nomor 29/SEOJK.03/2022* (SEOJK 29) about *Ketahanan dan Keamanan Siber Bagi Bank Umum* was issued to further explain the cyber security requirements set out in the POJK 11 - PTI. This SEOJK 29 consists of 10 chapters, with overview as following:

- **Chapter I – General terms**
  Explain about the understanding of cyber resilience, cyber security, cyber incident reports, and early notification of cyber incidents.

- **Chapter II – Assessment of cyber security's inherent risks**
  Cyber security's inherent risks focuses on technology, products, organizational characteristics, and cyber incident track records as the parameters. Level of inherent risk is divided into 5 categories 1-Low, 2-Low to moderate, 3-Moderate, 4-Moderate to high, and 5-High.

- **Chapter III – Implementation of cyber security risk management**
  Cyber security risk management implementation focuses on parameters such as governance, a framework for cyber security risk management, risk management processes and risk management information systems for cyber security, and internal control systems.

- **Chapter IV – Cyber resilience process implementation**
  Cyber resilience processes include the identification of assets, threats, and vulnerabilities, protection of assets, detection, as well as handling and recovery.

- **Chapter V – Assessment of a bank's cyber security maturity level**
  Based on the assessment of the quality of risk management implementation for cyber security and cyber resilience processes. The determination of the quality of risk management implementation related to cyber security is divided into 5 categories: 1-Strong, 2-Satisfactory, 3-Fair, 4-Marginal, and 5-Unsatisfactory. In addition, there are 5 levels of cyber security maturity which are Level 1-5.

- **Chapter VI – Risk level for cyber security**
  A bank's cyber security risk level is based on the assessment of a bank's inherent risk and cyber security maturity level.

- **Chapter VII – Cyber security testing**
  Consist of vulnerability analysis-based testing & scenario-based testing. Bank can perform cyber security testing independently or engaging the third party.

- **Chapter VIII – The unit/function which handles cyber security & resilience**
  Banks should establish a dedicated unit/function that is independent from operational IT. It will be responsible for handling cyber security and resilience including coordination of cyber security incident response team. Furthermore**, it should conduct a bank's cyber resilience processes, self-assessment of a bank's cyber security inherent risk and maturity level, determination of cyber security risks level and cyber security testing.**

  The unit/function responsible for handling cyber security and resilience should ensure the following:
  - Competency, capacity, and capability.
  - Coordination and collaboration.
  - Resources and access.
  - Leadership.

- **Chapter IX – Cyber incident report**
  Cyber incidents are critical events which include misuse and/or criminal activities relating to activities in electronic systems. The monitoring of cyber incidents should be performed to maintain cyber security and resilience. Cyber incidents need to be reported to OJK.

- **Chapter X – Closing terms**
  The provisions in this circular letter on cyber security and resilience in commercial banks (SEOJK Cyber) come into effect on 27 December 2022.

Cyber security related reports

This SEOJK 29 states 5 types of report to be prepared and submitted to OJK, such as:

Cyber incident reports	Cyber security inherent risk level	Cyber security maturity level	Cyber security risk level	Cyber security test results
• Early incident notification: no later than **1x24 hours**, via electronic communication (e.g. email). • A cyber incident report: submitted no later than 5 working days from the event and covers: – ***Information about the reporter and general information.*** – ***An impact assessment*** – ***Chronology of incidents*** – ***Root cause analysis*** – ***Final assessment***	• **Annually:** end of December. • Submission to OJK: at the latest **15 working days after** year end reporting. • First reporting **FY22**: submitted to OJK at the latest end of **June 2023**. • Considered as an **additional parameter of IT inherent risk level on operational risk**	• **Annually:** end of December. • Submission to OJK: at the latest **15 working days after** year end reporting. • First reporting **FY22**: submitted to OJK at the latest end of **June 2023**. • Includes an assessment of the quality of: - Risk management implementation for cyber security; and - Cyber resilience process implementation.	• Based on an assessment of **cyber security inherent risk and cyber security maturity level** • First reporting **FY22**: submitted to OJK at the latest end of **June 2023.**	• **Based on a vulnerability analysis** (e.g. penetration testing). Submission to OJK: at the latest **15 working days after** year end reporting. • **Scenario-based** (e.g. table-top exercises, cyber range exercises, social engineering exercises, adversarial attack simulation exercises, and/or other testing methods). The test result should be reported to OJK at the latest **10 (ten) working days after** testing is done.

The perspective of SEOJK from three lines model:

Governing body	First line	Second line	Third line
The governing body has an accountability to stakeholders to monitor the organisation. Some of the responsibilities include: • Active supervision and full responsibility • Availability and sufficiency of resources • Culture and awareness • Formalisation, implementation, communication, updating strategy, framework, policies, procedures, risk limits • Periodic evaluation, monitoring, and review • Direction on implementation and improvement actions • Assignment of roles and responsibilities	The first line is the process owner who is directly responsible for operational processes. Some of the responsibilities include: • Implementation of internal controls and cyber resilience processes • Assessment and reporting of the cyber security maturity level • Periodic cyber security testing • Risk monitoring and reporting	The second line is a dedicated function that assists in designing and monitoring the strategy for risk management. Some of the responsibilities include: • Cyber security risk management policies and strategy • Monitoring: policies vs implementation • Cyber resilience assessment • Review the impact to risk exposure. • Cyber risk management processes. • Periodic review and evaluation of the implementation of cyber security risk management.	The third line is an independent party that ensures risk management procedures have been performed in accordance with the relevant rules and regulations. This line model usually serves an internal audit function. Some of the responsibilities include: • Periodic review and evaluation of cyber security risk management. • Monitoring of remediation items and follow up actions. • Reporting remediation and outstanding audit findings to BoC and/or BoD.

SEOJK 29 is the first cyber security regulation for banking sector that specifically discuss about a good cyber security internal control in bank, for both conventional banks and syariah banks. The self-assessment method allows banks to start the cyber security internal control implementation based on risks. Considering that, SEOJK 29 is relevant with Indonesia current banking sector since each bank has a unique environment. Therefore, the cyber security risk faces will be different one to others so each bank cyber security internal control should be tailored.

Contact us

KPMG Siddharta Advisory
35th Floor, Wisma GKBI
28, Jl. Jend. Sudirman
Jakarta 10210, Indonesia
T: +62 (0) 21 574 0877
F: +62 (0) 21 574 0313

Irwan Djaja
Head of Advisory Services
Irwan.Djaja@kpmg.co.id

Freddie Mulyadi
Partner, IT Assurance & Cyber Security
Freddie.Mulyadi@kpmg.co.id

Eric Junatra
Senior Manager, Cyber Security
Eric.Junatra@kpmg.co.id

home.kpmg/id

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.