DENTONS HPRP

Grow | Protect | Operate | Finance

Commercial Banks' Obligation to Maintain Cyber Resilience and Security

Prepared by:
Mika Isac Kriyasa (Partner) and Aletheia Christy Hutabarat (Associate)

As we all know, information technology ("**IT**") is rapidly developing these days, especially in the banking industry. Banks can utilize IT to support their banking activities. The purpose of banks' utilization of IT is to gain benefits by among others increasing the efficiency and effectiveness of the bank's operations, improving services through easier cooperation with third parties, and the provision of fast and optimal services for customers.

However, due to rapid developments in the utilization of IT, banks need to pay more attention to cyber resilience and security due to the operational risks incurred. Cyber resilience and security should be the top priorities for any commercial bank. Effective security controls are essential for cyber resilience since the bank is responsible for protecting the confidentiality, integrity, and availability of assets and services.

With regard to the above matter, the Financial Services Authority (*Otoritas Jasa Keuangan* – "**OJK**") promulgated Circular Letter of OJK No. 29/SEOJK.03/2022 concerning Cyber Resilience and Security for Commercial Banks ("**SEOJK 29**") on 27 December 2022. The promulgation of SEOJK 29 was prompted by the increase of operational risks, especially the risks generated by cyber threats since the banking industry is a major target for cyber threats and banks are taking measures to protect themselves and their customers.

SEOJK 29 consists of 10 chapters, which we summarise below:

a. Inherent Risk Assessment Related to Cyber Security, which mandates:

   1. an assessment by the bank of inherent risk related to cyber security taking into account at least 4 (four) assessment factors, namely (i) technology, (ii) bank products, (iii) organizational characteristics, and (iv) cyber incident track record;
   2. an inherent risk assessment related to cyber security, which must be carried out annually; the first such assessment must be based on the position at the end of December 2022 and submitted at the end of June 2023 at the latest. The results of the inherent risk assessment related to cyber security must be submitted to the OJK as part of the report on the current condition of the bank's IT operations; and
   3. that the level of inherent risk related to cyber security will be considered as an additional parameter or indicator of the level of inherent risk for IT aspects of operational risk in assessing the soundness of the bank.

b. Implementation of Risk Management Related to Cyber Security mandates:

   1. banks' implementation of risk management related to cyber security, which includes 4 (four) aspects, namely:
      a) management of risks related to cyber security;
      b) a risk management framework related to cyber security;
      c) risk management processes, adequacy of human resources, and adequacy of the risk management information system, related to security cyber; and
      d) risk control systems related to cyber security;
   2. that the implementation of risk management related to cyber security be adjusted in accordance with the characteristics and complexity of the bank's business.

c. The Implementation of Cyber Resilience Process for Commercial Banks, in which the commercial banks carry out the following processes:
    1. identification of assets, threats and vulnerabilities;
    2. asset protection;
    3. cyber incident detection; and
    4. cyber incident response and recovery.

d. Cyber Security Maturity Level Assessment, which mandates:
    1. cyber security maturity level assessment, which includes an assessment of:
        a) quality of risk management implementation related to cyber security; and
        b) quality of implementation of cyber resilience processes;
    2. the assessment of the level of maturity of cyber security must be carried out annually; the first such assessment must be based on the position at the end of December 2022 and submitted at the end of June 2023 at the latest. The results of the assessment of the cyber security maturity level must be submitted to the OJK as part of the report on the latest condition of the bank's IT implementation; and
    3. the maturity level of cyber security is considered as a parameter or additional indicator of the quality of risk management implementation for IT aspects of operational risk in the assessment of the level of soundness of the bank.

e. Cyber Security Risk Level, which mandates:
    1. the risk level related to cyber security must be determined based on an assessment of (i) inherent risk related to cyber security and (ii) the level of maturity of cyber security. The following are the risk level categories:
        a) level 1 (low);
        b) level 2 (low to moderate);
        c) level 3 (moderate);
        d) level 4 (moderate to high); and
        e) level 5 (high).
    2. Determination of the risk level related to cyber security must be carried out annually; the first such determination must be based on the position at the end of December 2022 and submitted at the end of June 2023 at the latest. The level of risk related to cyber security must be submitted to the OJK as part of the report on the current condition of the bank's IT operations.

f. Cyber Security Testing, which mandates:
    1. Cyber Security Testing Based on Vulnerability Analysis
        a) this aims to see the weak points of the bank's system;
        b) it is carried out periodically based on the bank's internal evaluation, beginning with the identification of vulnerabilities followed by a penetration test;
        c) test results must be submitted to the OJK as part of the report on the current condition of bank IT operations.
    2. Scenario Based Cyber Security Testing
        a) this aims to validate the cyber incident response and recovery process at the bank;
        b) it must be conducted periodically, at least 1 (one) time in 1 (one) year;
        c) things that need to be considered in scenario based cyber security testing, such as testing in the form of an attack simulation, must be carried out in a controlled manner under strict supervision;
        d) test results must be submitted to the OJK no later than 10 (ten) working days after the completion of cyber security testing.
    3. Banks can carry out cyber security tests independently or use third parties while still paying attention to certain matters.

g. Units or Functions that Handle Cyber Resilience and Security, which mandates:
    1. The duties of the unit or function that handles bank cyber security and resilience, namely coordinating and/or implementing:
        a) the bank's cyber resilience processes;
        b) self-assessment of inherent risks related to cyber security and cyber security maturity level;
        c) determination of the level of risk related to cyber security; and
        d) cyber security testing;
    2. The unit or function tasked with handling cyber security and resilience must be independent from the IT management function.
    3. The unit or function that handles cyber security and resilience must coordinate the cyber incident response team, including the initiation of its formation.

4. The unit or function that handles cyber security and resilience must ensure that the cyber incident response team:
   a) has the capacity and capability related to cyber incident handling;
   b) can cooperate with related units or functions;
   c) has incident analysis resources;
   d) is able to cooperate effectively with the cyber threat intelligence function;
   e) is led by an official from a unit or function that handles cyber security and resilience; and
   f) has a contact person to support coordination in carrying out tasks.

h. Incidental Cyber Report, mandates:
   1. That cyber incidents are cyber threats in the form of attempts, activities, and/or actions that cause the electronic system to fail to work as it should.
   2. That Banks need to carry out monitoring of cyber incidents as a form of communication to stakeholders and control of the management of resilience and cyber security.
   3. Incidental Cyber Reporting
      a) early notifications of cyber incidents
         1) must contain the earliest available information regarding the cyber incident;
         2) must be submitted to OJK in writing via electronic means no later than 24 (twenty four) hours after the cyber incident becomes known to the bank;
         3) must be addressed to the supervisor of the bank concerned;
      b) cyber incident reports
         1) must contain more complete information related to the cyber incident;
         2) must be submitted online through the OJK reporting system no later than 5 (five) working days after the cyber incident becomes known.
   4. In the event that other authorities have provisions regarding the delivery of early notifications and/or cyber incident reports with a shorter timeframe, the bank must submit an early notification and/or cyber incident report to the OJK in conformity with the provisions of the other authority.

From the above explanation, it is important for the bank to conduct (i) assessment and testing; and also (ii) report to the OJK in relation to cyber resilience and security before the end of June 2023. If the Bank fails to do so, the bank will be subject to an administrative sanction in the form of a written reprimand. However, if the administrative sanction has already been imposed on the bank but it still has not fulfilled its obligation to conduct (i) assessment and testing; and also (ii) report to the OJK, then the bank will be subject to administrative sanctions in the form of: (i) prohibition on issuing new bank products; (ii) suspension of certain business activities; and/or (iii) reduction in the assessment of governance factors in the assessment of the bank's soundness.[1]

[1]Article 27 of OJK Regulation No. 11/POJK.03/2022 of 2022 concerning Implementation of Information Technology by Commercial Banks.

-o0o-