Digital Trust NewsFlash

PwC Digital Services / January 2023 / No. 6

OJK Circular Letter No.29/SEOJK.03/2022 on Cyber Security and Resilience for Commercial Banks

In response to increasing cyber security risks due to the advancement and innovative use of IT in the banking industry to provide financial services, the Indonesian Financial Service Authority or *Otoritas Jasa Keuangan* (OJK) released circular letter No. 29/SEOJK.03/2022 regarding Cyber Security and Resilience for Commercial Banks (Ketahanan dan Keamanan Siber bagi Bank Umum, referred to herein as "SEOJK Siber") on 27 December 2022. It will come into effect immediately for **all commercial banks, including conventional and shariah banks**. This circular letter is a subset of POJK PTI No. 11/POJK.03/2022 that has been effective since 7 October 2022.

The SEOJK Siber aims to provide minimum requirements regarding cyber security and resilience that need to be fulfilled by banks**,** and aims to increase overall cyber security and resilience by enforcing and incorporating effective **cyber security risk management** and end-to-end implementation of **cyber resilience processes** (identify, protect, detect, respond, and recover) that supports the banks' business objectives.

What's new in SEOJK Siber

Cyber Security Risk Assessment

SEOJK Siber mainly consists of several key components to define **overall cyber security risk rating** as follows:

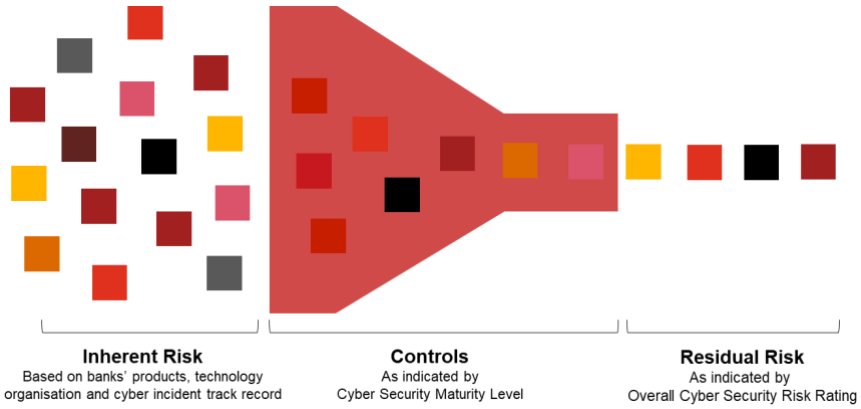
Banks are required to perform **cyber security risk assessments** to determine overall cyber security risk rating, which is assessed based on the results of:

a. **Cyber security inherent risk assessment,** to measure given risks arising from a bank's business, complexity, and technology adoption**.**
    1) This is assessed with regard to four aspects: technology, the bank's product, organisational characteristics, and cyber incident track record;
    2) Inherent risk rating is categorised as level: 1 (low), level 2 (low to moderate), level 3 (moderate), level 4 (moderate to high), and level 5 (high).

b. **Cyber security maturity assessment**, to measure the level of cyber security maturity in a manner which reflects the current cyber security conditions. Cyber security maturity is assessed based on implementation quality of:
    1) **Cyber security risk management,** consisting of 56 controls divided into 4 domains and 11 subdomains, covering:
        a) Cyber security risk governance, which includes active oversight of BoD and BoC, cyber security risk appetite, risk tolerance, culture and awareness;
        b) The cyber security risk framework, which includes cyber security risk management strategies, adequacy of organisation, adequacy of policies, procedures, and risk limits;
        c) Cyber security risk processes, resources, and information systems;
        d) The cyber security risk control system, which includes internal control system and review adequacy.
    2) **Cyber resilience process implementation**, consisting of 24 controls divided into 4 domains, covering:
        a) Asset, threat, and vulnerability identification
            i) Inventory and valuation of assets and their configuration;
            ii) Perform a vulnerability assessment and monitor emerging threats;
            iii) Perform cyber security testing (VAPT or scenario-based testing) regularly.
        b) Asset protection
            i) Implement, manage, maintain and continuously improve comprehensive security controls over IT assets;
            ii) Implement risk-based information and data security management;
            iii) Implement protections towards computer networks, hardware, and software;
            iv) Implement access control management, security patch management, protection on third party services, and secure coding during system development.
        c) Cyber incident detection
            i) Establish baseline performance and cyber detection processes;
            ii) Perform monitoring and detection on anomalous activity continuously;
            iii) Test and continuously improve cyber detection processes;
            iv) Perform analysis of threats and vulnerabilities of cyber incidents.
        d) Cyber incident response and recovery.
            i) Establish and perform a cyber incident response and recovery plan, including an escalation path and communication plan;
            ii) Define the roles and responsibilities of cyber incident response team;
            iii) Perform containment, eradication, and recovery procedures;
            iv) Perform post-incident analysis to identify lessons learned and improvement opportunities.

(Ref: Section III - V)

The relationship between **cyber security inherent risk assessment**, **cyber security maturity assessment**, and **cyber security risk assessment** indicates the current condition of a bank's overall cyber security control implementation as illustrated below:



By the end of the risk assessment process, banks will be able to determine an overall cyber security risk rating to indicate residual risk that should be tracked and monitored against banks' expected and risk appetite and tolerance. Risk rating is categorised as level 1: (low), level 2 (low to moderate), level 3 (moderate), level 4 (moderate to high), and level 5 (high).
(Ref: Section VI)

Cyber Security Testing

As part of asset, threat, and vulnerability identification processes in cyber resilience process implementation, Banks must perform cyber security testing through:

a. **Vulnerability Assessment and Penetration Testing (VAPT)**
   1) Must be performed regularly based on the Bank's internal evaluation and needs. For instance, based on system criticality level and changes to a Bank's system and/or IT architecture;
   2) Reported to OJK as part of the report of the current condition of the bank's IT operation.

b. **Scenario-based testing** (e.g., table-top exercise, cyber-range exercise, social engineering exercise, red teaming, and adversarial attack simulation exercise)
   1) Must be performed at least once a year;
   2) Reported to OJK no more than 10 working days after the assessment has been completed; and
   3) The scope of work should include, at minimum: objective, scope, and scenarios; testing execution; test evaluation; and assessment of the effectiveness of cyber incidents' mitigation, response, and recovery processes.

(Ref: Section VII)

Cyber Incident Report

A cyber incident (e.g. malware, web defacement, DoS, and DDoS) is an effort, activity, and/or action that could cause an electronic system failure. In the occurrence of a cyber incident, Banks need to:

a. Perform cyber incident monitoring and communicate this to stakeholders
b. Report to OJK in the form of:
   1) Initial Notification
      - Must be reported no later than 24 hours after a cyber incident detected;
      - Reported using a defined format, which must contain general incident information including: incident timeline, incident type, affected system, and initial response and analysis of the cyber incident.

2) Cyber Incident Report
   - Must be reported no later than 5 working days after the cyber incident is detected;
   - Reported using a defined format, which must contain general incident information, an impact assessment, chronological analysis, root cause analysis, conclusion and remediation efforts.

(Ref: Section IX)

Cyber Security Organisation

Banks need to establish **independent cyber security functions** that are independent from IT management functions to coordinate and/or perform:

a. Cyber resilience processes implementation;
b. Cyber risk assessment, inherent cyber risk assessment and cyber maturity assessment;
c. Cyber security testing;
d. Cyber incident response team.

(Ref: Section VIII)

Sanctions

There is no section explicitly explaining about sanctions in SEOJK Siber. However, since SEOJK Siber provides guidelines to implement cyber risk management and cyber resilience as required in Article 15 and Article 21 on OJK Regulation No. 11/POJK.03/2022 or POJK PTI, failing to comply with this circular letter may result in failing to comply with POJK PTI, which may result in administrative sanctions, including written warnings, fines, temporary suspension of activities and a decreased score for governance factors in assessments of soundness level.

Key Takeaways

SEOJK Siber sets a new baseline and expectation for the cyber security landscape in the banking industry. Many banks will have to revisit their cyber security practices and may need to establish or adjust current cyber security practices in order to manage compliance with the SEOJK Siber. Importantly, SEOJK Siber will help the Indonesian banking industry to improve overall cyber security maturity and enable banks and their key stakeholders to review their cyber security state.

a. Banks need to establish independent cyber security and resilience functions that are independent from IT management functions.
b. Banks need to implement cyber security risk management and cyber resilience processes, including cyber security incident management and reporting to OJK whenever a cyber security incident occurs.
c. Expected deliverables from this SEOJK Siber are:

	Cyber security inherent risk level assessment	Cyber security maturity level assessment	Cyber security risk assessment	Cyber security testing		Cyber incident	
				Vulnerability Assessment & Penetration Testing (VAPT)	Scenario-based testing	Initial Notification	Cyber incident report
Type	Regular	Regular	Regular	Regular	Regular	Ad-hoc	Ad-hoc
Frequency	Annual	Annual	Annual	Annual	Annual	-	-
Latest Submission	No later than 15 working days after the reporting year	No later than 15 working days after the reporting year	No later than 15 working days after the reporting year	No later than 15 working days after the reporting year	No later than 10 working days after testing is done	No later than 1x24 hours after cyber incident detected	No later than 5 working days after cyber incident detected
First Report	No later than the end of June 2023	No later than the end of June 2023	No later than the end of June 2023	As part of the report of the current condition of the 2022 bank's IT operation	Immediately after scenario-based testing performed in 2023	-	-

Your PwC Indonesia Contacts:

Subianto
Broader Assurance Services Leader
subianto.subianto@pwc.com

Andrew Tirtadjaja
Risk Assurance Director
andrew.tirtadjaja@pwc.com

Melissa Gunarto
Risk Assurance Director
melissa.g.gunarto@pwc.com

Benny Setyadi
Risk Assurance Senior Manager
benny.setyadi@pwc.com

Salman Alfarisy
Risk Assurance Senior Manager
salman.alfarisy@pwc.com

Beatrix Ariane
Risk Assurance Senior Manager
beatrix.b.ariane@pwc.com

Ade Triangga
Risk Assurance Manager
ade.triangga@pwc.com

Ledwin Ewaldo
Risk Assurance Manager
ledwin.ewaldo@pwc.com

Yudhi Ariyanto
Risk Assurance Manager
yudhi.ariyanto@pwc.com

Mila Ichwanto
Risk Assurance Manager
mila.ichwanto@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

pwc