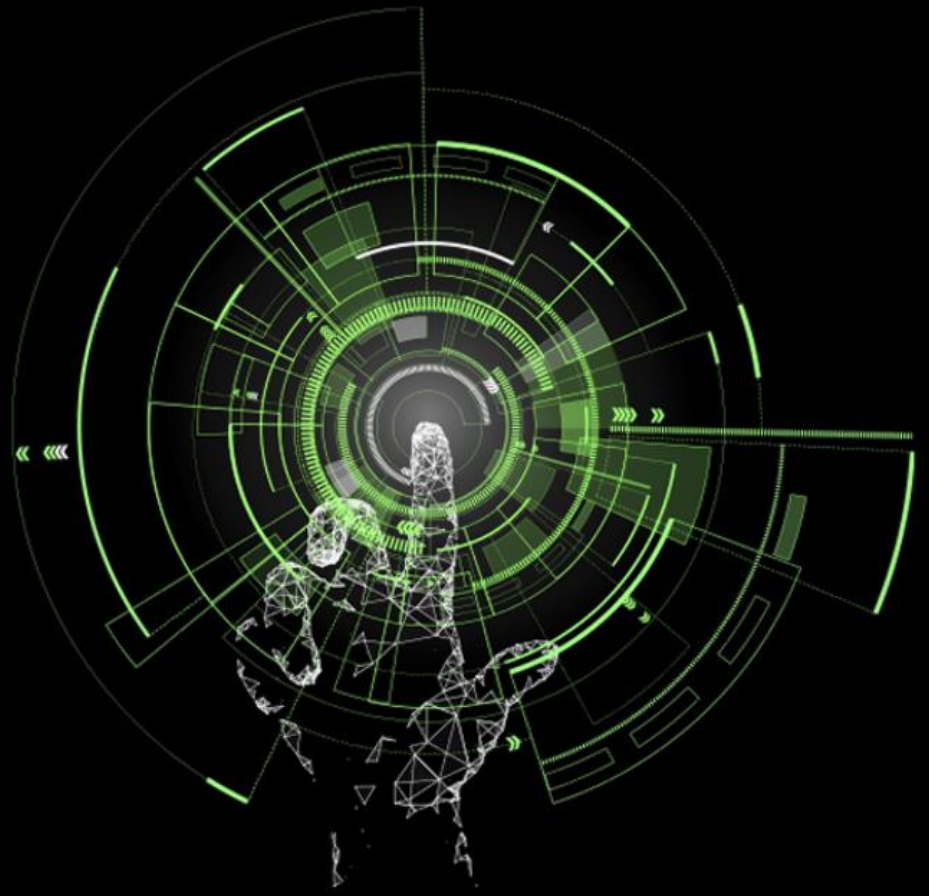
Deloitte.



Talkbook

SEOJK 29/2022 Key Requirements on Cyber Security and Resilience

PT DELOITTE KONSULTAN INDONESIA
MARCH 2023

MAKING AN IMPACT THAT MATTERS since 1845

Talkbook material

PT Deloitte Konsultan Indonesia

"On behalf of Deloitte Indonesia ("Deloitte"), we wish to thank you for this opportunity to deliver Introductory Material to you.

At Deloitte, we place our clients at the center of everything we do. We help our clients to prevent cyberattacks and protect valuable assets. We believe in being **secure, vigilant, and resilient**—not only by looking at how to prevent and respond to attacks, but at how to manage cyber risk in a way that allows our clients to **unleash new opportunities**.

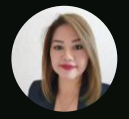
We are committed to working together with you on the near future. Partnering with us will give you access to our network of contacts, our thought leadership, and also coaching, all as part of the proposed package.

Once again, thank you for this opportunity to establish a partnership with you and look forward to be an integral part of this journey."

Contact Us

Brian Indradjaja
Risk Advisory Leader
bindradjaja@deloitte.com

Alex Siu Hang Cheung
Cybersecurity Partner
alecheung@deloitte.com



Jane Teh
Cybersecurity Director
hteh@deloitte.com

Hendro
Cybersecurity Director
hhendro@deloitte.com

Dewangga Wisnu
Associate Director
dwisnu@deloitte.com

Eryk B Pratama
Associate Director
epratama@deloitte.com

OJK Circular Letter No. 29 /seojk.03/2022

Cyber security and resilience
For the commercial bank

SEOJK 29/ 2022 on cyber security and resilience

Key requirements

Banks are required to perform periodic **cyber maturity assessments**, by using the following methods:

1. Cyber security inherent risk assessment
2. Cyber security risk management implementation assessment
3. Cyber security resilience process implementation assessment

Banks are required to perform periodic **security testing** by using the following methods:

1. Vulnerability assessment and penetration testing (VAPT)
2. Scenario based testing

Banks are required to report **cyber security incident** to OJK

Banks are required to establish **independent cyber security function**

SEOJK 29/ 2022 on cyber security and resilience

What the bank should do to determine bank's cyber security risk level?

Cyber security inherent risk assessment

Scope:
The inherent risk assessment related to cybersecurity is carried out by taking into account 4 (four) assessment factors:
1. Technology
2. bank's products
3. organizational characteristics
4. a track record of cyber incidents

Period:
Periodic (Annually)

Submission Deadline:
First submission: no later than end of June 2023

Following year: no later than 15 (fifteen) working days after the end of the reporting year

Cyber security resilience process implementation assessment

Scope:
The assessment shall include 4 (four) aspects:
1. the identification of assets, threats, and vulnerabilities
2. the implementation of asset protection capabilities
3. the implementation of cyber incident detection capabilities
4. the implementation of cyber incident response and recovery capabilities

Period:
Periodic (Annually)

Submission Deadline:
First submission: no later than end of June 2023

Following year: no later than 15 (fifteen) working days after the end of the reporting year

Cyber security risk management implementation assessment

Scope:
The assessment shall include 4 (four) aspects:
1. **cybersecurity risk governance**, includes adequacy of active oversight by the Board of Directors and Board of Commissioners, formulation of risk appetite and risk tolerance, as well as risk culture and awareness related to cybersecurity;
2. **cybersecurity risk management framework,** includes risk management strategies, adequacy of organizational tools, as well as the adequacy of policies, procedures, and setting risk limits, related to cybersecurity.
3. **cyber risk management processes,** includes the adequacy of both human resources and risk management information systems related to cybersecurity.
4. **cybersecurity risk control system,** the adequacy of the internal control system and the adequacy of reviews.

Period:
Periodic (Annually)

Submission Deadline:
First submission: no later than end of June 2023

Following year: no later than 15 (fifteen) working days after the end of the reporting year

Determining bank's Cyber maturity level

Bank's cybersecurity maturity level is determined based on the assessment results of:
- Cyber Security Resilience Process Implementation Assessment
- Cyber Security Risk Management Implementation Assessment

Determining bank's cyber security risk level

Cybersecurity risk level is determined based on the assessment results of:
- cybersecurity inherent risks and
- cybersecurity maturity level.

Bank's cyber security risk level is categorized as:
- level 1 (low),
- level 2 (low to moderate),
- level 3 (moderate),
- level 4 (moderate to high),
- level 5 (high).

SEOJK 29/ 2022 on cyber security and resilience

What else the bank should do?

Performing Cyber Security Testing

Scope:

perform cyber security testing on network, system, and data security, through:

A. Vulnerability assessment and penetration testing (VAPT)

- Objectives: identify the vulnerabilities and followed by penetration testing.
- Period: periodic based on bank's internal evaluation (the frequency can be defined based on system/ asset criticality level and if there is any changes to bank's electronic system and IT architecture which can increase the exposure to cyber risk).
- Submission deadline: no later than 15 (fifteen) working days after the end of the reporting year

B. Scenario based testing

- Objectives: to validate incident response and recovery process
- Required participants: executive officers, business functions, corporate communications functions, crisis management teams, service providers, and technical staff responsible for the cyber incident detection process, as well as the cyber incident response and recovery process.
- Some types of testing that can be performed:
  a) tabletop exercises,
  b) cyber range exercises,
  c) social engineering exercises,
  d) adversarial attack simulation exercises (red team and blue team)
- Period: periodic (annually)
- Submission deadline: no later than 10 working days after the assessment has been completed.

The Bank may conduct cybersecurity testing independently or using a third party.

Reporting Cyber Security Incidents

- **Basis:** Cyber incidents (e.g., malware, web defacement, DoS, and DDoS) occur due to disruption of cybersecurity that results in Electronic Systems not functioning properly.
- **Requirements:**
  A. Bank shall perform cyber incident monitoring and communicate to stakeholders.
  B. Bank shall submit Incident report to OJK with the following details:
    - Objectives: Bank shall submit information regarding cyber incidents to the Financial Services Authority (OJK) in the form of:
      a) cyber incident initial notifications, shall be submitted within 24 hours after the incident has been noticed by Bank.
      b) cyber incident reports, shall be submitted within 5 (five) workdays after the incident has been noticed by Bank.
    - Reporting format: Follow the format from SEOJK 29/2022 Appendix IV.a and Appendix IV.b

Independent Cyber Security Function

- Banks need to establish independent cyber security functions that are independent from IT management functions to coordinate and/or perform:
  - cyber resilience process implementation
  - cyber risk level assessment, which cover cybersecurity inherent risks and cybersecurity maturity level assessment
  - cyber security testing
  - cyber incident response

OJK Circular Letter No. 29 /SEOJK.03/2022

How Deloitte can help the bank to comply with the requirements

How Deloitte can help

Cybersecurity services

#	SEOJK 29/2022 Requirements	Required Report	How Deloitte Can Help
1	Cyber Security Risk Level Assessment: • Cyber inherent risk level • Cyber maturity level	• Cyber Security Inherent Risk Assessment Result • Cyber Security Risk Management Implementation Assessment Result • Cyber Security Resilience Process Implementation Assessment Result • Cyber Security Maturity Level Assessment Result • Cyber Risk Level Assessment Result	**Deloitte can help the Banks by providing the following services:** a) Review, design and develop cyber security governance (e.g., cyber security policy, procedures, standard). b) Review, design, and develop cyber security risk management framework. c) Perform identification of asset criticality, cybersecurity risk assessment, and develop cyber risk treatment plan. d) Design and develop cyber security key risk indicators/ key performance indicators for cyber risk monitoring. e) Design and develop cyber risk dashboard. f) Assess cyber security maturity level and develop cyber strategic roadmap (blueprint) for improvements g) Review, update, and develop bank's cyber security architecture h) Cloud security assessment and development i) Review, design, and develop data privacy and protection governance j) Information security tools/ solution implementation (e.g., identity and access management, data leak prevention, risk management tools, privacy and consent management tools)
2	Cyber Security Testing: • Vulnerability Assessment & Penetration Testing	• Vulnerability assessment and penetration test report	**Deloitte can help the Banks by providing the following services:** a) Application (web, mobile, desktop) vulnerability assessment and penetration test b) Infrastructure (wired, wireless) vulnerability assessment and penetration test c) Security configuration review (Apps, OS, DB, network) d) SAP vulnerability assessment and penetration test e) SWIFT vulnerability assessment and penetration test f) Bug bounty program (service and platform)

How Deloitte can help

Cybersecurity services

#	SEOJK 29/2022 Requirements	Required Report	How Deloitte Can Help
3	Cyber Security Testing: • Scenario-based Testing	• Security testing report, which cover: o Summary of testing o Lesson learned o Improvement plan	**Deloitte can help the Banks by providing the following services:** a) Cybersecurity tabletop exercises / cyber drill (covering executive management, business function, and technical incident response team) b) Cyber range exercises c) Social engineering exercises (phishing simulation) d) Adversarial attack simulation exercises (Red Team exercises, Compromise Assessment, Breach and Attack Simulation)
4	Reporting Cyber Security Incidents	• Notification of cyber incident • Cyber incident report	**Deloitte can help the Banks by providing the following services:** a) Review, develop and improve cyber security detection capabilities (SOC review, which cover people, process, technology, and strategy). b) Review, develop and improve cyber security incident response capabilities (people, playbook, response plan and process, and training requirements). c) Review, develop and improve business continuity management, disaster recovery management, and crisis management.
5	Independent Cyber Security Function	• Established independent cyber security function within the Bank	**Deloitte can help the Banks by providing the following services:** a) Review, design and develop cyber security structure and operating model (including 1st, 2nd, and 3rd line of defense) covering structure, roles, responsibilities, RACI matrix, interaction model, and proposed KPIs. b) Review, design and develop cyber security competencies/ skill set and training plan/roadmap. c) Review, design and develop cyber security awareness plan and material.

Deloitte.