Digital Trust NewsFlash

PwC Digital Services / April 2025 / No. 8

PADG No. 24/2024 on Information System Security and Cyber Resilience

In response to increasing digitalisation and the need for robust cybersecurity in the financial sector, Bank Indonesia has issued the Regulation of The Member of Board of Governors, *Peraturan Anggota Dewan Gubernur* (PADG) No. 24/2024 regarding Information System Security and Cyber Resilience/ *Keamanan Sistem Informasi dan Ketahanan Siber* (KKS) (hereinafter referred to as "PADG KKS"). The PADG KKS, which became effective on 31 December 2024, serves as an implementing regulation that will further govern operational matters supporting Bank Indonesia Regulation Number 2 Year 2024, previously issued on 22 April 2024.

The provisions of PADG KKS apply to payment system operators, money market and foreign exchange market participants, as well as other parties regulated and supervised by Bank Indonesia (hereinafter referred to as "Operators").

KKS ensures that the Operators' information and systems are protected from cyber attacks, keeping business operations running smoothly through proactive and adaptive measures. It also involves the ability to quickly respond to and recover from cyber incidents.

The following is a brief summary of the key points in PADG KKS:

1. Governance that strengthen KKS requires Operators to establish a KKS Strategy and Policy to implement a KKS culture:
   a. KKS Strategy and Policy must consists of:
      - Developing a KKS strategic plan by considering the Operators' risk appetite, regulatory requirements, technology trends, and cyber threats.
      - Developing and evaluate KKS policies, standards, and procedures that cover people, process, and technology aspects.
      - Establishing organisational functions of KKS that consists KKS management for strategic planning, cyber risk management, and an annual KKS audit by an independent auditor at least once a year.
   b. Implement a KKS culture for internal parities, external parties, and consumers through awareness, training, and education programmes.

2. Prevention involves implementing proactive measures to protect the Operators' information assets, systems, and networks from potential security breaches. It consists of three steps: Identification, Protection, and Detection.

Identification	Protection	Detection
Identifying and assessing cyber risks from the perspectives of people, processes, and technology, as well as understanding their potential impact on the business.	Establishing a robust and secure defence system is crucial, alongside safeguarding and protecting data and information.	Conduct monitoring, analyse the results, investigate cyber attacks and malicious code, and carry out maintenance and testing of detection systems.

3. Handling involves a structured approach to responding to and recovering from cyber incidents, minimising their impact on business operations.

Response	Recovery
a. Establishing a Cyber Incident Handling and Recovery Plan b. Executing Cyber Incident Simulations and Trials c. Handling Cyber Incidents d. Establishing Communication Methods and Strategies e. Cyber Incident Response Team	a. Restoring Services to Normal Conditions b. Continuous Improvement c. Communication

4. Submission of data and information

Operators must provide data and information to Bank Indonesia about KKS governance, prevention, and handling. This data should be submitted online using Bank Indonesia's reporting system. If the system isn't available, reports can be submitted offline.

Type of report	Annual	Incidental	
		Cyber Incident Initial Notification	Cyber Incident Report
Minimum Information	• KKS Maturity Level Report • The identification of vital information infrastructure • Supporting documents: - KKS Audit report - Penetration Test report	• The reporter's contact information • General information about the cyber incident • Initial assessment of the cyber incident impact	• The reporter's contact information • General information about the cyber incident • A comprehensive analysis of the cyber incident's impact • Cyber incident forensics • Conclusions and follow-up corrective actions.
Latest Submission	No later than 31 January for the previous annual reporting period	No later than 1 hour after a cyber incident is detected	No later than 3 calendar days after a cyber incident is detected
First Report	No later than 31 January 2026 for reporting period 2025	-	-

5. Sanction

Operators who violate the provisions will be subject to administrative sanctions in the form of:

a. A written warning issued through an official letter;
b. An obligation to pay a maximum of IDR 5,000,000 (five million rupiah) per report;
c. A temporary suspension of part or all activities, including the execution of cooperation agreements, through the revocation of licences and/or approvals, issued via an official revocation letter; and/or
d. The revocation of licences and/or approvals already granted, issued via an official revocation letter.

Key takeways

In accordance with PADG KKS, Operators should develop a comprehensive understanding of their risk profile by implementing robust cyber governance and risk management strategies like Cybersecurity Maturity Assessment. This involves undertaking thorough risk assessments to identify vulnerabilities and threats, aligning people, processes, and technology to enhance cyber resilience. Operators are expected to establish proactive measures like regular Vulnerability Assessment and Penetration Testing (VAPT) to safeguard information assets. These measures focus on identification, protection, and detection, ensuring a strong security posture. Operators must have a structured approach to swiftly respond and recover from cyber incidents, minimising their impact on business operations and maintaining resilience against cyber threats. Additionally, Operators should refer to best practice standards (e.g., NIST, ISO 27001) and adhere to relevant laws and regulations, such as the Personal Data Protection Law (UU PDP), PBI No. 23/6/PBI/2021, and PBI No. 23/7/PBI/2021.

PwC Indonesia contacts

Subianto
Broader Assurance Services Leader
Chief Digital & Technology Officer
subianto.subianto@pwc.com

Daniel Septianto
Cybersecurity Senior Manager
daniel.s.septianto@pwc.com

Yudhi Ariyanto
Cybersecurity & Privacy Manager
yudhi.ariyanto@pwc.com

Ivan Kirsten
Cybersecurity & Privacy Manager
ivan.k.kirsten@pwc.com

Andrew Tirtadjaja
Cybersecurity & Privacy Director
andrew.tirtadjaja@pwc.com

Mila Ichwanto
IT Governance Senior Manager
mila.ichwanto@pwc.com

Dimas Kusuma
Cybersecurity Manager
dimas.kusuma@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia