DENTONS HPRP

Grow | Protect | Operate | Finance

Smarter Banks, Safer Systems: An Overview of OJK's Artificial Intelligence Governance Guidelines for the Banking Sector

Prepared by:

Andre Rahadian (Partner), Mika Isac Kriyasa (Partner), Josha Jehuda Ponggawa (Senior Associate) and Pritta Maharani Pribadi (Associate)

The use of artificial intelligence ("**AI**") in banking is rapidly expanding, driving greater efficiency as institutions automate functions such as fraud detection, anti-money laundering monitoring, and credit decision-making. Against this background, the Financial Services Authority of Indonesia (Otoritas Jasa Keuangan, or "**OJK**") has issued a much-anticipated set of detailed guidelines on AI governance and risk management.

On 29 April 2025, the OJK issued its **AI Governance for Indonesian Banking** guidelines (*Tata Kelola Kecerdasan Artifisial Perbankan Indonesia* or the "**Guideline**"), setting out a foundational framework to ensure the responsible development and use of AI in the banking sector.[1] The Guideline outlines key principles and expectations for banks to adopt AI in a prudent and risk-aware manner, with the aim of supporting sector stability and sound governance. It builds on and complements OJK's existing regulatory framework, including policies on banking digital transformation, as well as guidelines on digital resilience, consumer and data protection, digital banking services, IT governance, cyber resilience and security, and digital maturity assessments.

The Guideline was also developed with reference to leading international frameworks, including the European Union's AI Act, the AI Risk Management Framework by the United States National Institute of Standards and Technology, and benchmarking approaches in other jurisdictions, such as the United States, China, Singapore, and Japan. Finally, the Guideline also considers relevant local regulations, particularly Law Number 27 of 2022 on Personal Data Protection ("**PDP Law**"), to ensure alignment with Indonesia's broader legal framework for data protection.

AI Risks and Challenges

In emphasizing the need for the Guideline, OJK highlights a range of emerging risks associated with AI adoption in the banking sector. The prominent concerns including:

a. the rise of deepfakes (AI-generated synthetic media that can impersonate individuals through realistic images, videos, or audio that may be exploited for fraud, identity manipulation, or social engineering);
b. AI bias, where AI systems may produce biased outputs, caused by non-representative data, non-neutral algorithms or user factors operating the system resulting in unfair and discriminatory decisions; and
c. cybersecurity threats, where AI models are vulnerable to data poisoning, adversarial attacks, and unauthorized model extraction that can degrade system performance and compromise sensitive information.

OJK also makes reference to the vulnerabilities of AI specifically in financial services as identified by the Financial Stability Board and the European Central Bank, which include:

a. **Market correlation**: the use of similar algorithms by different financial institutions can lead to homogeneous behavior, thereby exacerbating market volatility.

[1] Otoritas Jasa Keuangan, Tata Kelola Kecerdasan Artifisial Perbankan Indonesia (2025). from https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata%20Kelola%20Kecerdasan%20Artifisial%20Perbankan%20Indonesia.pdf.

b. **Third party dependency**: excessive dependence on AI can increase systemic fragility within the operational framework.

Key Governance Principles

OJK emphasizes that governance measures should apply throughout the entire AI lifecycle, from the initiation stage to periodical evaluation and monitoring. The Guideline outlines a set of foundational principles, which is broader than the ethical principles set out in Ministry of Communication and Informatics Circular Letter Number 9 of 2023 on Artificial Intelligence Ethics, and provides a more detailed approach to mitigate risks and support responsible innovation in the banking sector:

a. **Reliability**: AI systems are required to be explainable, secure and resilient. Banks must ensure that AI-driven decisions are understandable and dependable based on clear, simple and contextual factors, while also safeguarding systems against cyber threats.
b. **Accountability**: Banks are required to have clear lines of responsibility, particularly through transparency in how AI systems operate, and through strong data governance that is aligned with the PDP Law.
c. **Human Oversight**: Banks must ensure that AI systems do not operate autonomously without the possibility of human intervention throughout the lifecycle. This can be done by establishing alternative models that can be used in emergencies (fallback mechanisms), providing an AI opt out mechanism for users, and preventing automation bias, particularly when high-stakes decisions are involved. AI use must also be inclusive and sustainable, avoiding discriminatory impacts while contributing positively to long-term development and business continuity.

Implementation of these principles must integrate across three essential domains, namely People (developing internal AI capability and ethical awareness), Process (embedding governance, risk, and compliance frameworks), and Technology (ensuring that systems are secure, transparent, and continuously monitored).

Responsible AI Governance Measures

To support responsible AI implementation in the banking sector, the Guideline introduces a set of supervisory expectations that banks are encouraged to adopt in alignment with their existing governance, risk management, and internal control frameworks as mandated under prevailing OJK regulations.

1. Policy and Risk Management

   All AI-related activities in banks must be supported by internal policies and procedures prepared in accordance with applicable laws and aligned with the bank's business processes and approval mechanisms. Parties involved in the development, deployment, and management of AI systems (AI actors) must also apply comprehensive risk management strategies across the AI lifecycle. This includes AI-specific risk controls to identify, assess, monitor, and mitigate risks associated with AI adoption. As part of AI risk management, banks should conduct AI impact assessments involving cross-functional teams, such as privacy, risk, legal, engineering, HR, products, and marketing, to ensure responsible, ethical, and secure deployment of AI technologies.

2. Board Level Supervision

   The Guideline underscores the critical role of the bank's Board of Directors and the Board of Commissioners in ensuring the responsible and ethical use of AI. This includes setting clear roles and responsibilities for AI risk management, supervising the use of high-risk AI systems, ensuring the availability of adequate expertise and resources, and understanding the bank's AI risks, strategy, ethical and legal implications, and alignment with broader business objectives.

   AI governance must be part of regular board and committee discussions, supported by appropriate escalation procedures for AI-related incidents and access to technical expertise. Banks must also ensure that board supervision complies with OJK Regulation Number 17 of 2023 on the Governance of Commercial Banks and OJK Regulation No. 11/POJK.03/2022 on Information Technology Implementation by Commercial Banks ("**OJK IT Regulation**").

3. AI Committee

   OJK recommends that a bank should form an AI Committee to supervise the use of AI within the organization. The committee may be integrated into the bank's IT Steering Committee, as stated in the OJK IT Regulation, or established as a standalone committee, particularly if AI plays a significant or complex role in the bank's operations. The AI Committee should have the following functions:

   a. Supervising the development and implementation of the bank's AI governance framework;
   b. Defining roles and responsibilities for AI supervision, design, development and use across the organization;

c. Establishing guiding principles for ethical and responsible use of AI;

d. Setting the scope of the bank’s AI governance program and ensure proper documentation;

e. Identifying and supervising policies, procedures, and training to enable responsible design, use and supervision of AI;

f. Identifying areas requiring human supervision, including inaccuracies and bias detection, as well as quality control;

g. Developing procedures to assess and escalate high-risk AI use cases;

h. Reporting regularly to the bank’s management;

i. Supporting incident management related to AI use.

4. <u>AI Audit</u>

Banks are expected to audit their use of AI as part of effective and comprehensive internal IT audits, as required under Article 53 of the OJK IT Regulation. An AI audit involves evaluating whether the AI system was trained with reliable and representative data, operates transparently, produces explainable results, and delivers outcomes that are generally predictable.

Banks may use external auditors in accordance with the relevant OJK regulations on internal auditing but remain fully responsible for outcomes. Any such arrangements must suit the bank’s size and complexity and safeguard data confidentiality.

Next Steps for Indonesian Banks

While the Guideline is framed as a guidance, it operates within the scope of binding OJK regulations. Banks deploying AI without aligning with the Guideline, particularly where existing regulatory obligations are in play, may be deemed non-compliant and subject to regulatory scrutiny or administrative sanctions such as warnings or corrective actions especially if risks materialize. Accordingly, the Guideline should be regarded as an integral part of a bank’s compliance, governance, and risk management framework.

Banks are therefore encouraged to assess existing frameworks, identify governance and risk gaps, and progressively adopt governance measures for AI implementation. Looking forward, banks can expect enhanced obligations on data governance and model transparency, and tighter alignment with the personal data protection requirements. Considering the complexity and nuance of AI utilization in the financial sector, the handling and processing of personal data will be a key consideration for successful AI implementation by banks. Thus, it is imperative that they continually review their business processes to ensure their usage of AI is compliant with the PDP Law.

Taking proactive steps now will strengthen institutional preparedness and reduce future compliance risks as regulatory expectations continue to evolve.

- o0o -

The article above was prepared by Dentons HPRP’s lawyers

This publication is not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to. Readers should take legal advice before applying the information contained in this publication to specific issues or transactions or matters. For more information, please contact us at dentons.hprp@dentons.com .