Digital Trust NewsFlash

June 2025 / No. 9

Page 1
Artificial Intelligence (AI) Governance for Indonesian Banking Industry

Artificial Intelligence (AI) Governance for Indonesian Banking Industry

On 29 April 2025, the Financial Services Authority (*Otoritas Jasa Keuangan*) has introduced the Artificial Intelligence Governance for Indonesian Banking as a guideline aimed at ensuring that Indonesian banks develop and implement AI technologies (including advanced AI systems) responsibly. The guideline covers various aspects, such as risks and challenges, guiding principles, risk management and governance, implementation guidelines, supervision and audit processes associated with AI implementation. It also encompasses AI governance frameworks, AI guidelines, and AI regulation developments in other countries such as The European Union's AI Act (EU AI Act), G7 Hiroshima Principles, etc. as well as in Indonesia such as, OJK AI guideline and MOCI circular letter.

What's in the Artificial Intelligence Governance for Indonesian Banking?

The main objective of the guideline is to maximise the benefits of AI while effectively managing the associated risks—such as customer protection, banking system resilience, and broader financial system stability.

Definition of AI

AI is a transformative force which includes a range of capabilities that mimic human intelligence in machines and software. Today, AI has grown into several main areas, each with its own special uses, like Machine Learning (ML), Deep Learning (DL), Predictive AI, Generative AI, and the newest type, Agentic AI. Due to the use case variation, AI is often compared to automation, but the main difference is that automation follows set of rules, while AI can learn on its own.

Risks and challenges of AI implementation

As there is a growing capability of AI, more diverse risks and challenges. Risks and challenges to AI implementation are often cross-cutting and intersectional between financial, cybersecurity, and legal risks and challenges. Various risks and challenges that emerged including:

1. **Risk of misinformation and decrease in public trust**
   - **Deepfakes**: Artificially generated media created by GenAI could lead to the spread of misinformation and decrease public trust.
   - **GenAI specific risks**: confabulation (where content appears to be true), harmful biases may contribute to misinformation and reduced reliability of outputs.
2. **Transparency and fairness challenges**
   - **Black box**: lack of explainability in complex AI systems leads to trust, accountability, and governance concerns. Additionally, absence of explainability creates a challenging situation to determine accountability of such decision-making.
   - **AI bias**: Arises from non-representative data, non-neutral algorithms, or user factors could result in discriminatory outcomes and unfair decision-making.
3. **Privacy and intellectual property concerns**
   - Unauthorised access to sensitive personal data like financial information that may be collected and processed without proper basis for processing or without adequate protection measures.
   - Infringement of intellectual property protection, in case developers uses training data protected with intellectual property rights without proper permission.
4. **Cybersecurity and technical vulnerabilities**
   - Threats such as data breach & data privacy attacks, adversarial inputs, model extraction and training data poisoning could lead to producing incorrect or harmful outputs.
   - AI systems can be attractive targets for cyberattacks, significantly impacting security and manipulation by hackers.
5. **Human-related challenges**
   - Leadership skill gaps, job displacement, talent shortages, and overreliance on AI could lead to human-related issues and challenges.
6. **Risk of financial stability**
   - Dependency on third-parties, algorithmic herding behaviour (similar algorithm leads to similar responses) could increase systemic risks and threaten financial stability.

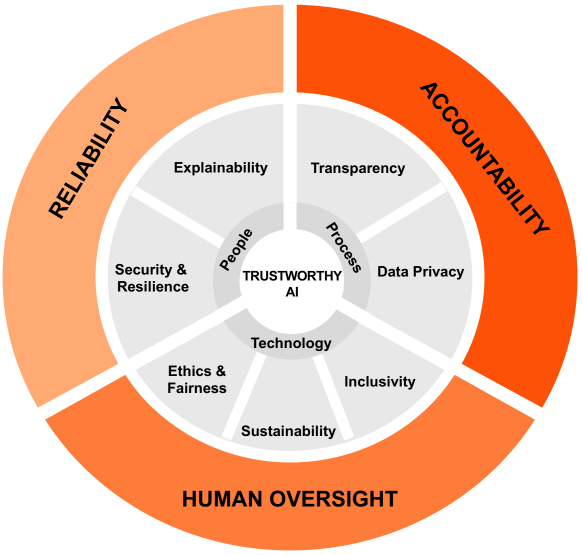
Suggested measures

Understanding core values to achieve responsible and trustworthy AI

As various risks and challenges emerge in the implementation of AI, core values are essential in promoting responsible and trustworthy AI. The guideline outlines three fundamental principles essential for realising responsible and trustworthy AI (see **Figure 1**):

1. **Reliability**
   A reliable AI model produces explainable, secure, and resilient outcomes. It is essential to ensure that decisions made using AI are trustworthy and consistent with the strategies implemented by banks.
2. **Accountability**
   AI systems should be accountable to ensure that banks, as organisers, can be held responsible for the proper functioning of the developed and operated AI systems. The entire process must be transparent for audit and accountability purposes, and a robust data management mechanism, including data privacy, should be in place.
3. **Human oversight**
   Human oversight is considered one of the most crucial values. Without human intervention, potential biases and inconsistent outputs that do not align with values of fairness or objectives may occur. Therefore, human oversight is necessary to ensure AI systems adhere to principles of ethics, fairness, sustainability, and inclusivity.

Figure 1. Basic principles of responsible and trustworthy artificial intelligence



Source: Artificial Intelligence Governance for Indonesian Banking Guideline, 2025

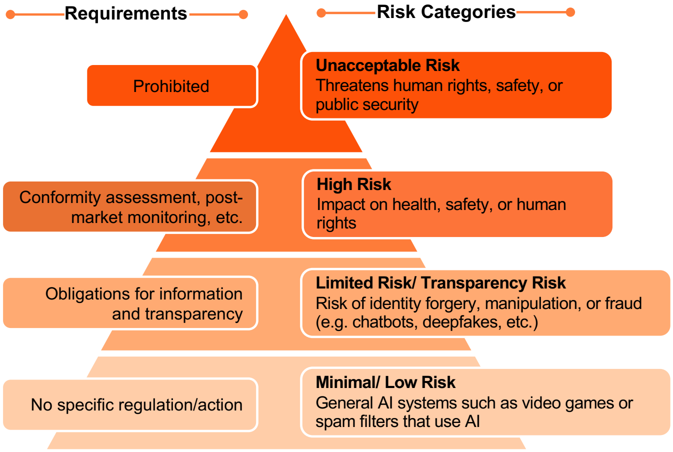
Integrating trustworthiness into the AI lifecycle through risk management and governance

According to the National Institute of Standards and Technology (NIST) AI Risk Management Framework, there are four functions that enhance the Bank's ability to manage risks associated with AI implementation:

1. **Govern**: Establish a risk management culture during the design, development, and evaluation of AI systems.
2. **Map**: Identify AI risks and their contributing factors.
3. **Measure**: Monitor AI risks and their impacts.
4. **Manage**: Allocate resources to regularly map and measure risks.

In terms of the application of AI risk management, the EU AI Act provided a risk-based approach, classifying AI systems based on the risk levels (see Figure 2)

Figure 2. AI system risk classification


Requirements
Risk Categories
Prohibited
Unacceptable Risk
Threatens human rights, safety, or public security
Conformity assessment, post-market monitoring, etc.
High Risk
Impact on health, safety, or human rights
Obligations for information and transparency
Limited Risk/ Transparency Risk
Risk of identity forgery, manipulation, or fraud (e.g. chatbots, deepfakes, etc.)
No specific regulation/action
Minimal/ Low Risk
General AI systems such as video games or spam filters that use AI

Source: Artificial Intelligence Governance for Indonesian Banking Guideline, 2025

Overseeing AI governance

The Board of Directors (BoD) and Board of Commissioners (BoC) play pivotal role in ensuring the responsible and trustworthy implementation of AI within the Indonesian banking sector. Their responsibilities must align with applicable laws, regulations, and governance practices, particularly:

1. OJK Regulation No. 17 of 2023 on Governance Implementation for Commercial Banks; and
2. OJK Regulation No. 11/POJK.03/2022 regarding Information Technology Implementation by Commercial Banks.

OJK regulations and other provisions concerning the duties, responsibilities, and authorities of the BoD and BoC, as well as the execution of functions from the three lines of defence—namely, the business management line, the risk management and compliance line, and the internal audit line—remain applicable.

To support the BoD and BoC in overseeing AI initiatives, the establishment of an AI Committee is recommended. This committee may include representatives from key functional areas such as:

- Legal
- Compliance
- Risk Management
- Product Development
- Procurement
- Data Science
- Cybersecurity
- Marketing
- Customer Service

The roles of the AI Committee may encompass:

Supervising the design and launch of the company's AI governance framework	Defining key roles and responsibilities related to the oversight, design, development, and use of AI across the business	Creating guiding principles for AI
Defining and documenting the scope of the AI governance program	Identifying and overseeing policies, processes, and training to enable responsible design, use, and oversight of AI	Identifying areas that require human review or oversight
Developing processes to assess and escalate high-risk AI use cases	Reporting to company management (the board and senior management)	Assisting in managing incidents related to the use of AI

It is recommended that the AI Committee either be integrated into the IT Steering Committee, as outlined in OJK Regulation No. 11/POJK.03/2022, or established as a dedicated committee focused solely on AI governance. The appropriate structure should be determined based on the complexity and scale of AI adoption within the bank.

In addition to the roles of BoD, BoC and the AI Committee, several other factors contribute to effective oversight of AI governance in banking:

1. Organisational readiness, including the necessary strategic alignment, leadership commitment, and operational capacity to support AI adoption.
2. Human resources with sufficient knowledge, skills, and diverse experience in developing and implementing AI systems, as well as an openness to new ideas, an understanding of how AI will impact their tasks and responsibilities, etc.
3. Robust AI infrastructure, comprising hardware and software to support AI systems and machine learning workloads. Unlike traditional IT infrastructure, AI infrastructure is optimised for high computational demands and large-scale data processing required by AI algorithms.
4. Supports from all AI actors (internal and external) throughout the AI lifecycle.

Leveraging existing AI guidelines and/or regulations

This new guideline provide a foundational reference for banks to follow when implementing AI systems. These guidelines emphasize the importance of upholding integrity, ethical values, and strong governance while ensuring compliance with applicable regulations. These include OJK's regulations related to IT governance, digital services in banks and other relevant regulations that will continue to serve as guidelines.

Banks are encouraged to refer to a range of existing standards and regulatory frameworks, including:

1. Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (UU P2SK);
2. Law No. 27 of 2022 on Personal Data Protection (UU PDP); and
3. Other relevant OJK guidelines/regulations including blueprint for digital transformation in banking, digital resilience guideline, OJK provisions regarding:
   - Provision of Information Technology by Commercial Banks.
   - Digital Services by Commercial Bank.
   - Digital Maturity Level of Commercial Banks (DMAB).
   - Cyber Resilience and Security for Commercial Banks.
   - Implementation of Risk Management in the Use of Information Technology by Commercial Banks.
   - Implementation of Governance for Commercial Banks, and Implementation of Sharia Governance for Sharia Commercial Banks and Sharia Business Units.
   - Consumer Protection.

Auditing AI implementation

To regulate the implementation of AI audits, OJK has issued several key provisions and guidelines that can be referred to, including:

1. POJK No. 1/POJK.03/2019 concerning the Implementation of Internal Audit Functions in Commercial Banks;
2. POJK No. 11/POJK.03/2022 concerning Information Technology Implementation by Commercial Banks;
3. POJK No. 17 of 2023 concerning Governance Implementation for Commercial Banks; and
4. SEOJK No. 21/SEOJK.03/2017 concerning Risk Management Implementation in the Use of Information Technology by Commercial Banks.

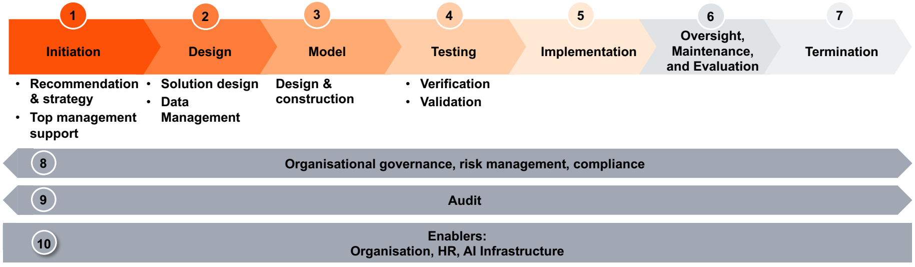
The primary objective of an AI audit is to ensure that the AI systems used by banks are trained on representative and credible data, operate through transparent processes, and generate explainable outputs.

Additionally, auditors are encouraged to evaluate the governance processes, risk management practices, and the integration of AI systems within the bank's broader operational framework.

To effectively conduct AI audits in banks, auditors can align the audit process with the stages of the information technology system lifecycle. This approach ensures that AI systems are evaluated comprehensively—from development and deployment to monitoring and decommissioning.

1. Life Cycle Framework for Auditing AI Algorithms (Luliana Sandu, Menno Wiersma, Daphne Manichand).
2. Value, Criteria, Indicators, and Observable (VCIO) issued by the AI Ethics Impact Group (AIEI).
3. ISACA AI Audit Toolkit.
4. The Institute of Internal Auditors (IIA) framework.

Figure 3. Implementation guideline for the AI lifecycle



Source: Artificial Intelligence Governance for Indonesian Banking Guideline, 2025

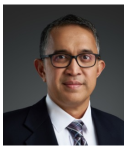
Key takeaways

AI governance in the Indonesian banking sector serves as a foundational guideline to ensure that AI technologies are developed and implemented in a responsible, ethical, and trustworthy manner. To support this objective, several key practices are recommended for fostering responsible AI adoption:

1. **Establishing an AI governance framework**
   Banks should ensure that AI implementation aligns with OJK's core principles of trustworthy AI. This involves fully internalising all relevant values—such as fairness, transparency, accountability, and security—rather than selectively applying them.
2. **Forming an AI committee**
   An AI Committee should be established to support the roles of the BoD and BoC. Depending on the complexity of AI adoption, banks may either form a dedicated AI Committee or integrate its responsibilities into the existing IT Steering Committee.
3. **Aligning AI implementation with regulatory framework**
   Banks must consistently refer to applicable regulations—including those issued by OJK and other relevant authorities—to ensure that AI deployment delivers benefits while effectively managing associated risks.
4. **Supervising and auditing AI implementation**
   Regular supervision and audit activities should be conducted in accordance with established guidelines. These audits help identify emerging risks and ensure that AI systems remain compliant with regulatory and ethical standards.

For more information, contact your PwC contact below:

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

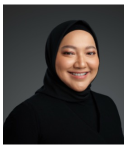


Indra Allen
Legal Partner
indra.allen@pwc.com

Richard Ticoalu
Data, AI and Risk Partner
richard.ticoalu@pwc.com

Hengky Antony
Data & Analytics Director
hengky.antony@pwc.com

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



Roro Astuti
Legal Senior Manager
roro.astuti@pwc.com

Kevin Gian
Data Analytics Senior Manager
kevin.gian@pwc.com

Marcello Dwianto
Data Analytics Manager
marcello.dwianto@pwc.com

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

www.pwc.com/id

in PwC Indonesia

𝕏 @PwC_Indonesia

If you wish to unsubscribe, please reply with UNSUBSCRIBE in the subject line, or send an email to id_contactus@pwc.com.

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC Indonesia, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

The documents, or information obtained from PwC, must not be made available or copied, in whole or in part, to any other persons/parties without our prior written permission which we may, at our discretion, grant, withhold or grant subject to conditions (including conditions as to legal responsibility or absence thereof).

PwC Indonesia is comprised of KAP Rintis, Jumadi, Rianto & Rekan, PwC Tax Indonesia, PwC Legal Indonesia, PT Prima Wahana Caraka, PT PricewaterhouseCoopers Indonesia Advisory, and PT PricewaterhouseCoopers Consulting Indonesia, each of which is a separate legal entity and all of which together constitute the Indonesian member firms of the PwC global network, which is collectively referred to as PwC Indonesia.