Deloitte.

Together makes progress

Building trustworthy AI in Indonesian banking:

A strategic response to OJK AI governance framework

July 2025

Executive summary

Artificial Intelligence (AI) has moved beyond the experimental stage and is now a critical engine of transformation in financial services. In Indonesia's banking industry, AI is already redefining credit scoring, fraud detection, customer personaliation, and operational efficiency. As banks accelerate their AI adoption to stay competitive, new questions emerge:

- **Can these systems be trusted?**
- **Are they ethical and explainable?**
- **Who is accountable when AI fails?**

These concerns are no longer theoretical. Globally – and increasingly in Indonesia – regulators are stepping in to ensure AI innovation is accompanied by accountability. In this context, the Otoritas Jasa Keuangan (OJK), has introduced the Artificial Intelligence Governance for Indonesian Banking, a foundational guide that outlines how banks should build and govern AI systems to ensure they are **safe, fair, transparent, and aligned with societal values.**

This publication explores how banks can respond strategically to OJK's guidance by leveraging the **Deloitte Trustworthy AI Framework**. Widely adopted by leading financial institutions globally, the framework offers a **structured, practical, and ethically grounded approach** to operationalising AI governance across the model lifecycle – from design to deployment and ongoing monitoring.

In the following chapter, we provide a narrative alignment between OJK regulatory pillars and Deloitte governance model. We demonstrate how banks can not only meet compliance standards, but also embed trust into every layer of their AI ecosystem. **For forward-looking institutions, this is more than a response it is a competitive differentiator.**

By institutionalising trustworthy AI practices today, Indonesian banks have the opportunity to lead with integrity, build enduring customer trust, and future-proof their digital strategies in a fast-evolving risk and regulatory environment.

Interpreting OJK AI governance guidance for Indonesian banking

OJK released the Tata Kelola Kecerdasan Artifisial Perbankan Indonesia to establish a foundational governance framework for the responsible use of Artificial Intelligence (AI) in the banking sector. As AI becomes increasingly embedded in core banking operations ranging from credit scoring and fraud detection to customer engagement, the OJK emphasises the need for structured oversight to safeguard fairness, transparency, accountability, and financial stability.

The OJK guidance is not prescriptive, but principle-based, allowing banks flexibility in how they apply governance aligned with their size, digital maturity, and AI use cases. Key expectations include:

- **Adopt responsible AI practices**
  Banks are expected to build AI systems that are fair, explainable, safe, and secure—minimising unintended harm and ensuring outcomes remain aligned with institutional values.
- **Embed governance across the AI lifecycle**
  From data acquisition and model development to deployment and retirement, every stage must be governed with appropriate oversight, documentation, and controls.
- **Establish ethical foundations**
  AI must reflect principles such as human oversight, transparency, accountability, and privacy, particularly in customer-facing or high-impact applications.
- **Align with global best practices**
  While tailored to the national context, the framework encourages banks to adopt globally coherent standards, preparing institutions to operate in an interconnected digital ecosystem.

In essence, the guidance provides a strategic foundation for banks to mature their AI capabilities with trust at the center.

While the guidance offers a clear vision, many banks face a gap in turning these expectations into action. This is where a structured approach becomes essential. To meet these expectations, institutions require a governance model that is not only technically robust but also ethically grounded and adaptable across use cases.

The **Deloitte Trustworthy AI Framework** offers a methodology to operationalise the OJK guidance. Built around seven dimensions: **fairness, transparency, accountability, privacy, security, reliability, and responsibility** the framework helps banks implement AI governance that is both scalable and sustainable.
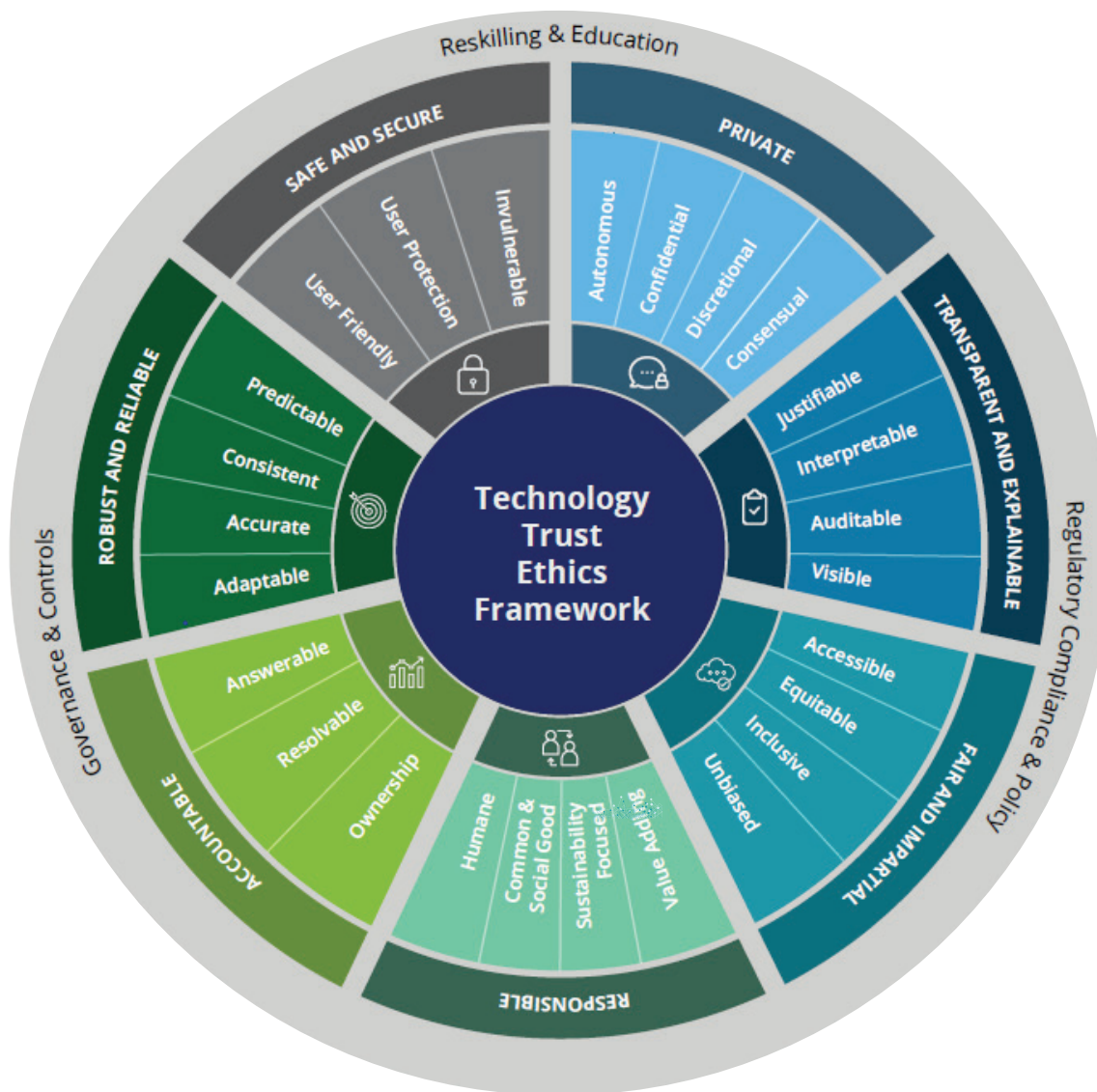
By aligning strategic goals with AI oversight, banks can move beyond risk mitigation to create trusted AI ecosystems capable of delivering long-term value while meeting the expectations of customers, boards, and society at large.

Deloitte Trustworthy AI Framework
High level overview

Deloitte Trustworthy AI Framework provides a practical and strategic foundation for banks to implement AI governance in alignment with the principles outlined in OJK's guidance. By embedding **trust across each stage of the AI lifecycle**, Trustworthy AI helps institutions navigate the expectations of the **Tata Kelola Kecerdasan Artifisial Perbankan Indonesia** and implement a governance model that is **robust, explainable, and value driven**. Deloitte Trustworthy AI is built on **seven foundational dimensions**, each addressing core aspects of AI risk and responsibility:
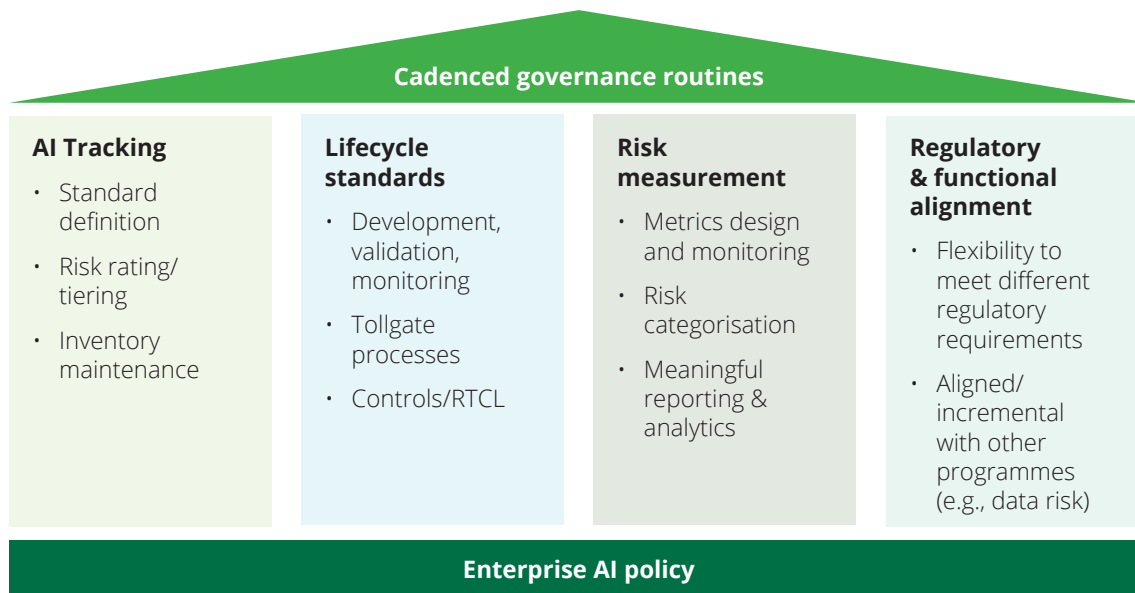
Dimension	Description	Alignment with OJK AI governance principles
Private	Privacy and confidentiality are respected in accordance with contractual and regulatory obligations, and data is not used beyond its intended and stated purpose.	Reflects OJK requirement to uphold privacy, data protection, and responsible data use. Trustworthy AI embeds data governance principles such as minimisation, consent management, and anonymisation across model development and deployment.
Transparent / Explainable	Participants can understand how their data is being used and how AI systems make decisions; algorithms, attributes, and correlations are open to inspection.	Aligns with OJK emphasis on explainability and traceability by enabling organisations to make AI decisions auditable, understandable, and communicable to internal and external stakeholders. This is especially critical in regulated processes such as credit scoring and fraud detection.
Fair / Impartial	AI applications include internal and external checks to help ensure equitable application across participants.	Responds to OJK call for fairness and non-discrimination by ensuring AI systems are designed and tested to minimise bias. Trustworthy AI supports organisations in identifying risk factors related to data imbalance or algorithmic bias early in the development process.
Responsible	The technology is created and operated in a socially responsible manner.	Captures the broader ethical vision laid out in the OJK framework. This dimension encourages institutions to assess the societal and customer impact of AI use cases ensuring technology serves human interests and supports long-term trust.
Accountable	Policies are in place to determine who is responsible for the decisions made or derived with the use of technology.	Reinforces the governance expectations in the OJK framework by defining clear responsibilities across the AI value chain from model developers to risk stewards and executive oversight. This ensures decisions made by or with AI can be traced back to responsible human actors.
Robust / Reliable	AI systems can learn from humans and other systems, where acceptable, and produce consistent and reliable outputs.	Supports lifecycle oversight by embedding performance validation, scenario testing, and monitoring practices into AI operations. This enables banks to meet OJK expectation of maintaining consistent and reliable outputs over time, especially in mission-critical applications.
Safe / Secure	AI systems can be protected from risks (including Cyber) that may cause physical and/or digital harm.	Addresses OJK concerns on model stability and digital resilience. Trustworthy AI incorporates cybersecurity and operational safeguards to ensure that AI systems are protected from manipulation, breaches, and misuse particularly when handling sensitive customer data.

Each of the dimension is supported by lifecycle governance and enterprise-wide risk management capabilities that make the framework scalable across AI use cases and organisational complexity.

Establishing trustworthy AI governance

Deloitte translates the above principles into a practical AI governance model that supports both compliance and innovation. Key building blocks include:

Cadenced governance routines

AI Tracking	Lifecycle standards	Risk measurement	Regulatory & functional alignment
• Standard definition • Risk rating/ tiering • Inventory maintenance	• Development, validation, monitoring • Tollgate processes • Controls/RTCL	• Metrics design and monitoring • Risk categorisation • Meaningful reporting & analytics	• Flexibility to meet different regulatory requirements • Aligned/ incremental with other programmes (e.g., data risk)

Enterprise AI policy

1. **Enterprise AI policy**
   - Aligns with broader Global Risk Management Framework.
   - Defines roles & responsibilities and key life-cycle requirements.
   - Drives consistency across the enterprise in AI Risk Management activities.

2. **AI tracking**
   - Definition is unambiguous and aligned / reconciles with existing model definition.
   - Up-to-date inventory includes necessary attributes for Risk Management programme.

3. **Lifecycle standards**
   - Well-defined processes, procedures, controls, templates, and technology requirements that facilitate the AI policy through each stage of an AI object's lifecycle.
   - Flexible to be adjusted by lines of businesses/functional areas based on the idiosyncrasies of respective AI-use environments (e.g., 3rd party AI, Generative AI).

4. **Risk measurement**
   - Quantitative and qualitative approaches to measuring and monitoring AI risk.
   - Practical to assemble on an ongoing basis (e.g., automatable/repeatable).

5. **Regulatory & functional alignment**
   - Flexibility to align to different regulatory jurisdiction requirements.
   - Where appropriate, incremental to existing Risk Management programmes, such as Model Risk Management (MRM), data risk, cyber risk, legal risk, technology risk, etc..

6. **Cadenced governance routines**
   - Inclusion of the right stakeholders (e.g., key risk stewards, senior management).
   - Focus is risk-based and action-oriented.

The six-step model transforms governance from a static requirement into a dynamic enterprise capability, enabling Indonesian banks to meet OJK guidance with confidence and consistency.

Building an AI-fueled bank – Components of organisational readiness

Deloitte translates the above principles into a practical AI governance model that supports both compliance and innovation. Key building blocks include:

Talent
Hiring and developing talent to support the next generation of ways of working.

Operating model
Maturing from a decentralised model to a scalable and nimble hub-and-spoke structure, such as a Center of Excellence (CoE).

Risk management
Managing AI risk by ensuring there is a robust and responsible AI framework to create a sustainable, safe, and responsible AI-use environment.

Data
Implementing modern data platforms that enable AI use cases.

Technology
Developing an infrastructure that has the compute capacity to support AI programmes, is scalable, safe, and secure, and leverages AI within its own stack.

AI governance is only as strong as the organisation behind it. Building these five components ensures that banks do not just control AI, they empower it responsibly.

How organisations can get started

The Deloitte Trustworthy AI Governance Framework brings structure to AI implementation through six interdependent components designed to help banks responsibly develop, deploy, and manage AI systems. This six-part model aligns with the OJK's lifecycle-driven governance expectation (Bab 6.1), where AI systems must be governed from planning to post-deployment. Each component embeds trust, accountability, and control, ensuring that Indonesian banks meet OJK's principles while supporting safe innovation.
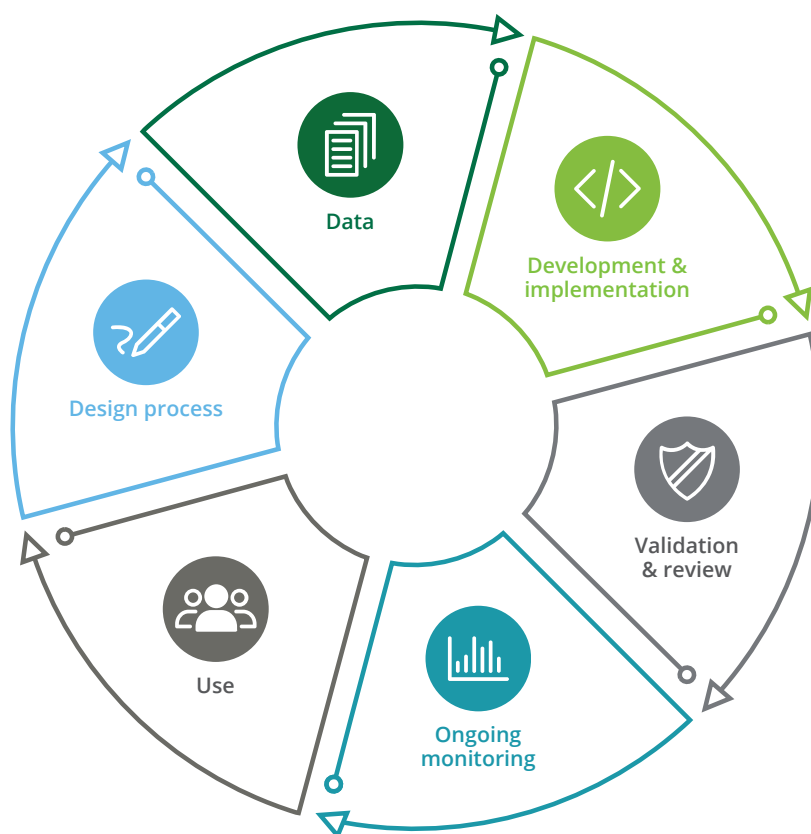
1. **Design process**

   This first phase focuses on shaping the AI solution in line with organisational strategy, stakeholder needs, and regulatory expectations. Key actions:

   - **AI Ethics training** programmes for AI developers.
   - **Consult a diverse group of stakeholders** and gather a variety of use-case scenarios.
   - Conceptualise and **document** the system's intended use, objectives and risks.
   - Hold sessions with stakeholders to **identify potential sources of adverse** outcomes and risks.
   - Understand latest **regulatory and legal requirements**.
   - Potential sources of risks (e.g., bias) are identified and **plans for mitigation** are put into place.

   In alignment with OJK's guidance, this phase ensures AI systems are responsibly initiated starting with proper intent, stakeholder clarity, and risk awareness.

2. Data

Data is the fuel of AI. This phase focuses on ensuring quality, fairness, and integrity across the AI data pipeline. Key actions:

- Data sources are **reputable and well-documented**.
- **Representative data sets** are utilised for AI training purposes.
- Utilise least number of data features that meet **performance goals**.
- Perform assessment of data elements/features (including post-transformations) for **potential bias**.
- **Data quality metrics** identified and monitored.

OJK emphasises the importance of data fairness and explainability. Deloitte ensures these expectations are met through proactive data governance embedded from the start.

3. Development & implementation

Once data and design foundations are in place, the AI model is built and implemented. Key actions:

- **A clear statement of purpose** to ensure that the model is developed in line with its intended use.
- A model selection process driven by **objective criteria** and a structured assessment of the model suitability.
- A variety of **development tests** used to evaluate the model type assumptions, the model stability, bias, impact of potential limitations, and model behaviour over a range of input values (sensitivity and boundary testing).
- **Back-testing (in-sample and out-of-sample)** and cross validation results.
- **Strong documentation** that discusses approach, assumptions, limitations, risks and related mitigation controls.

This phase supports OJK's guidance for transparent, documented, and risk-calibrated development. It also reflects the requirement for human-centric design principles.

4. Validation & review

Before release, AI models must undergo rigorous independent validation to assess accuracy, ethics, and compliance. Key actions:

- A second line of defense for review and AI oversight.
- AI oversight with authority to challenge AI design and development.
- Review conceptual design of model including data elements.
- Review developmental tests and perform additional tests where needed.

OJK requires structured review mechanisms and stakeholder oversight prior to launch. Deloitte integrates this through internal tollgates and stakeholder reviews to ensure auditability and model confidence.

5. Ongoing monitoring
Post-deployment, AI systems must be continuously supervised to ensure they perform as expected. Key actions:

- Regularly evaluate model performance using relevant metrics looking for changes or degradation.
- Compare performance to relevant baselines or expected performance indicators.
- Use visualisations for easier identification of patterns/trends.
- Monitor distribution of input data.
- Evaluate the model performance on subsets of data (e.g., edge cases and demographic groups).

These practices are in direct response to OJK guidance, which highlights continuous supervision, anomaly detection, and real-time intervention as critical pillars of AI oversight.

6. Use
This final component governs the active use of AI systems by internal teams and external stakeholders. Focus areas:

- Use a human-centric approach for decision-making to identify and report bias.
- End-user training that includes considerations for ethics and potential harm.

OJK calls for responsible usage and adaptive governance and Deloitte's framework ensures that once AI is live, it continues to operate ethically and remains aligned with institutional and public interest.

The **six components** described above are not isolated technical steps – they form an **integrated governance system** that ensures AI systems remain **accountable, explainable, and continuously safe over time**. This structure responds directly to OJK's guidance, which require:

- **Lifecycle-based AI risk management**
- **Clear governance roles across all phases**
- **Data integrity and fairness**
- **Explainability, accountability, and adaptability over time**

By adopting this implementation framework, banks can fulfill the regulatory spirit and technical expectations of OJK while building internal capabilities to responsibly scale AI. Deloitte methodology ensures governance is embedded at every layer of AI activity allowing banks to innovate confidently while safeguarding trust, compliance, and long-term resilience.

Conclusion and how Deloitte can help

OJK's guidance signals a pivotal shift for Indonesian banks, **AI must be developed and deployed with integrity, accountability, and oversight**. Achieving this goes beyond setting policies it requires embedding **responsible AI practices into decision-making, risk controls, and everyday operations**.

The Deloitte Trustworthy AI Framework offers a practical pathway to achieve these outcomes. Grounded in **global best practices and tailored to local needs**, our method enables effective implementation across two key focus areas:

1. **Build governance and risk foundations**
    We support institutions in establishing robust structures and controls by:
    • Clarifying roles across business, risk, compliance, and technology.
    • Defining policies and ethical principles tailored to your AI strategy.
    • Assessing AI risks based on system complexity, criticality, and exposure.
    • Embedding controls throughout the AI lifecycle from design to deployment.

2. **Operationalise oversight and compliance**
    To ensure accountability and adaptability, we help:
    • Implement real-time monitoring and bias detection tools.
    • Strengthen model documentation and explainability for all stakeholders.
    • Create audit trails, response protocols, and internal control libraries that align with OJK expectations.

With this structured support, banks can align with OJK principles while turning AI into a secure, transparent, and trustworthy engine of innovation. Partnering with Deloitte gives you access to multidisciplinary expertise combining regulatory insight, technical capability, and deep banking experience to help you lead confidently in the era of AI.

Contact Us

Robertus Indrakrishna
Regulatory & Financial Risk
Partner
Deloitte Indonesia
rindrakrishna@deloitte.com

David Christian Hidayat
Regulatory & Financial Risk
Director
Deloitte Indonesia
dhidayat@deloitte.com

Erwin Junatra
Regulatory & Financial Risk
Manager
Deloitte Indonesia
ejunatra@deloitte.com

R Dimas Bagas Herlambang
Regulatory & Financial Risk
Manager
Deloitte Indonesia
rherlambang@deloitte.com

Deloitte.