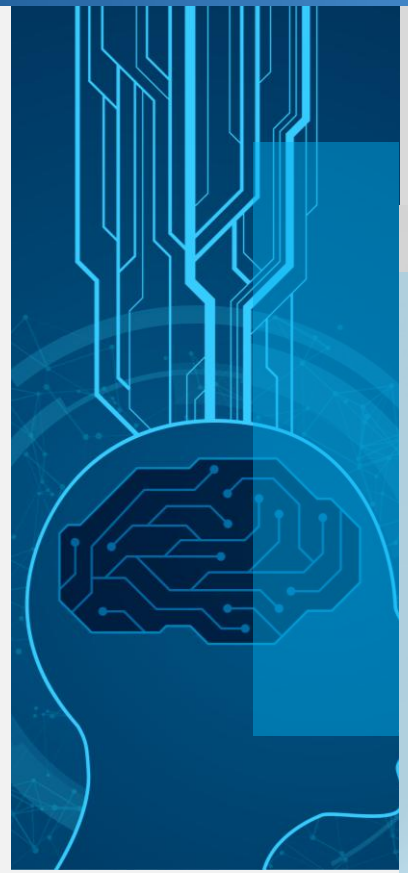
Artificial Intelligence in the Malaysian Financial Sector

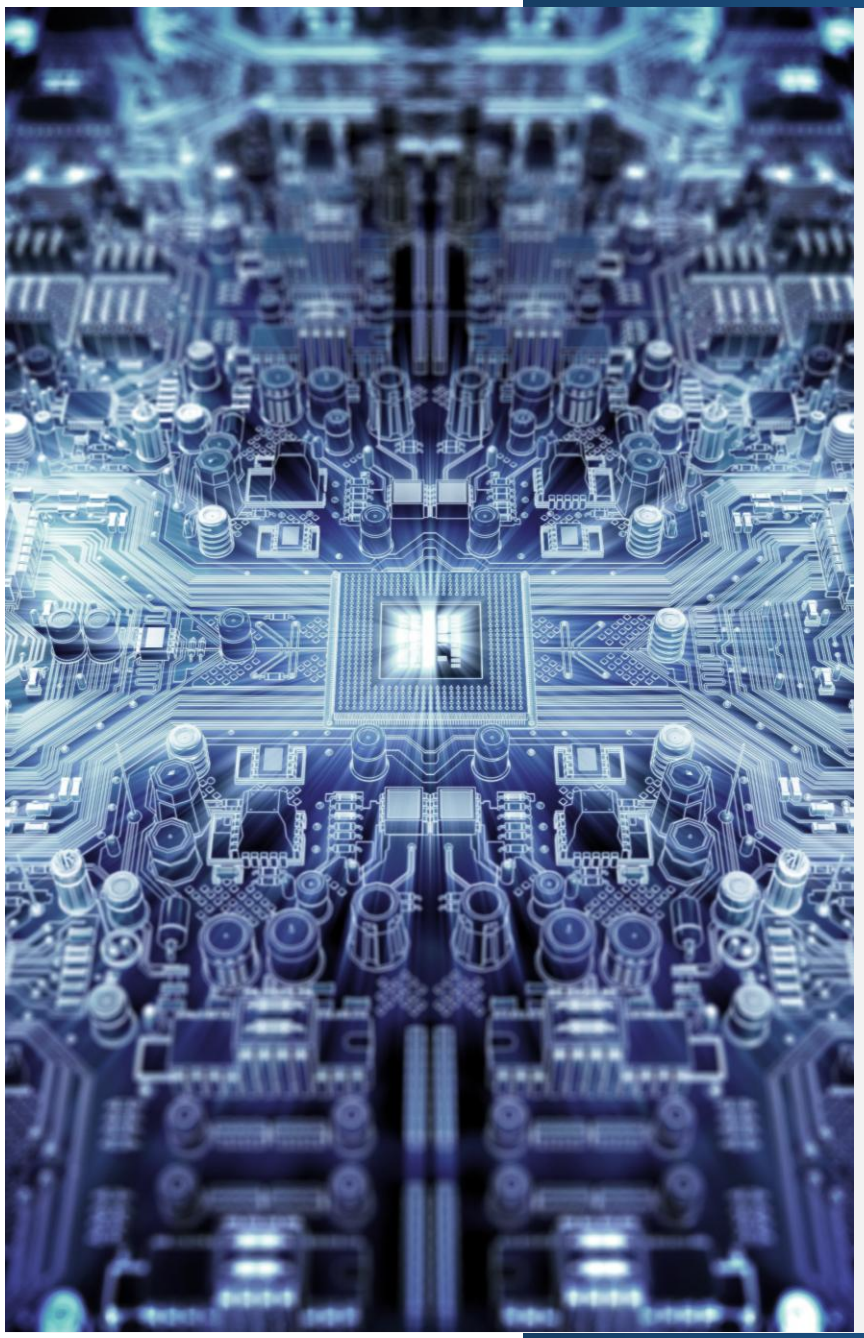
Feedback Statement

November 2026





BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA



Contents

Executive Summary 3

Discussion Paper Findings 4

Development Approach 9

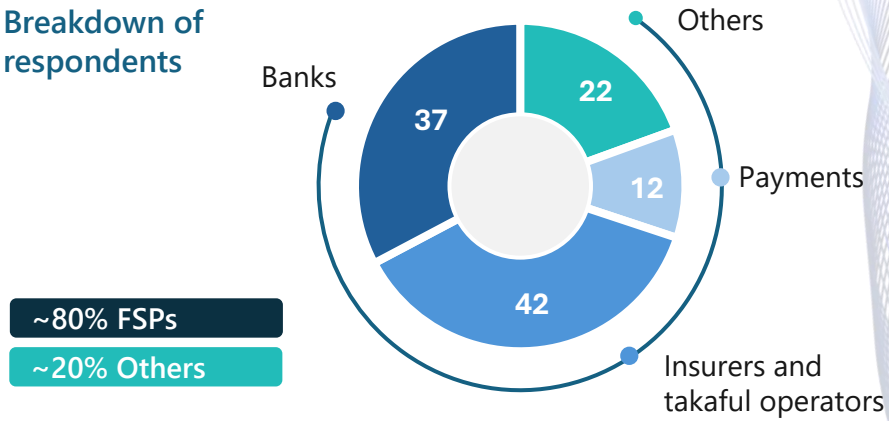
Regulatory Approach 14

Emerging Best Practices 19

Executive Summary

The **Discussion Paper on Artificial Intelligence in the Malaysian Financial Sector (AIDP)** was issued in August 2025 to gather views on the opportunities, risks and governance considerations associated with AI adoption in the financial sector. Bank Negara Malaysia (BNM) received feedback from 113 respondents, including financial service providers (FSPs) and a broad range of ecosystem stakeholders, reflecting strong interest in the role of AI in shaping the future of financial services.

Breakdown of respondents



Overall, respondents expressed strong support for the responsible adoption of AI and for BNM's technology-neutral and proportionate approach. The feedback suggests that AI adoption is already underway across the sector, particularly in areas such as operational efficiency, customer service and fraud management, and is increasingly being viewed as a strategic capability that can support broader business, consumer and policy outcomes.

Respondents also highlighted the rapid evolution of AI technologies, including generative AI, agentic AI and synthetic data, which are expected to further transform financial services. At the same time, stakeholders noted challenges relating to data access, governance, talent, third-party dependencies, concentration risks and the application of existing regulatory expectations to emerging AI use cases.

Key insights

- Strong support for responsible AI adoption across the financial sector
- Existing regulatory expectations remain broadly applicable
- Continued collaboration, practical guidance and capability building are priorities for industry
- AI should advance innovation while strengthening trust, resilience and consumer outcomes

The feedback points to a clear path towards enabling AI innovation while strengthening governance, consumer protection and risk management. Together with the industry, BNM aims to expand opportunities for shared learning, safe experimentation and practical testing, helping institutions build capability and translate emerging practices into responsible adoption. Moreover, BNM is not introducing AI-specific regulation at this stage and instead will progressively provide greater regulatory clarity as AI use cases and risks evolve.

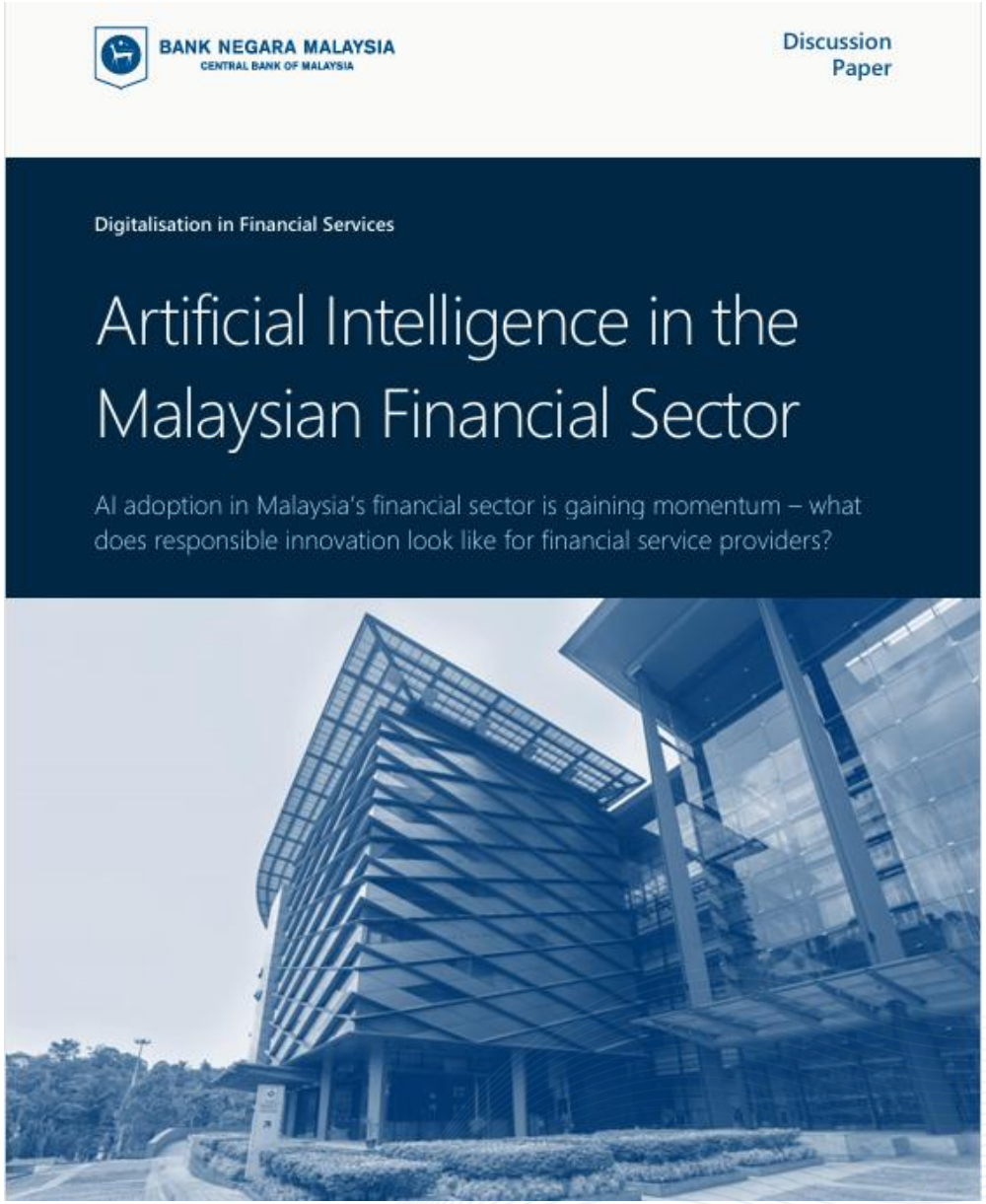
Looking ahead, we hope these insights will catalyse greater knowledge sharing and more meaningful testing across the industry. They provide a starting point for FSPs to assess and strengthen their own practices, while enabling BNM to deepen its understanding of emerging practices, opportunities and risks, helping us calibrate future interventions to where they can have the greatest impact.

Discussion Paper Findings

In August 2025, BNM issued the AIDP and received feedback from 113 respondents, including financial service providers (FSPs) and a broad range of ecosystem stakeholders. The strong response underscores growing momentum behind AI adoption across the financial sector.

Respondents broadly supported BNM's technology-neutral and proportionate approach, recognising AI as an increasingly important capability for driving innovation, strengthening resilience and improving consumer outcomes.

Feedback also highlighted that realising AI's full potential will require strong governance, trusted data, skilled talent and continued collaboration across the ecosystem. As adoption accelerates, trust, transparency and accountability will remain critical to ensuring AI is deployed responsibly and delivers sustainable benefits for consumers and the financial sector.



Use Cases

Respondents highlighted a growing breadth of AI adoption use cases across the financial sector. While many institutions are focused on **improving productivity and customer experience**, AI is also being applied to **strengthen fraud detection, compliance, risk assessment and financial inclusion**. The findings indicate that AI is increasingly being used not only to improve productivity, but also to advance broader policy and consumer outcomes.

Top areas across the sector*

64%	Operational Efficiency/ Process Automation
61%	Customer Service/ Personalisation
52%	Fraud/ Anti-Money Laundering (AML)
48%	Compliance
43%	Financial Inclusion
32%	Risk Assessment

Notable use cases mentioned by institution type

Banks	Development Financial Institutions	Insurers and Takaful Operators	Payment Service Providers
Customer Service/ Personalisation	Credit Risk	Operational Efficiency/ Process Automation	Operational Efficiency/ Process Automation
Financial Inclusion	Compliance	Customer Service/ Personalisation	Customer Service/ Personalisation
Credit Risk	Financial Inclusion	ESG & Social Impact	Fraud and AML

Examples of AI use cases by institution type:

- Test case generation and code development
- GenAI assistant to boost staff productivity
- AI-assisted straight-through processing
- Data management automation
- AML solutions for transaction reviews
- Automated regulatory reporting
- Customer service chatbot
- AI-powered electronic Know-Your-Customer

** Percentages reflect the share of respondents that identified each use case as deployed, piloted, or being explored within their organisation*

AI Risk Considerations

Respondents recognised that **AI may introduce new risks and amplify existing ones** through its scale, autonomy and complexity. This reinforces the **importance of robust governance, effective risk management and appropriate oversight** to support safe and responsible AI adoption. The following are the risks most frequently cited by respondents.

Data Governance

Privacy: Unauthorised use of sensitive data

Data leakage: Unintended disclosure through prompts

Data quality: Biased or inaccurate data

Adversarial Attacks on AI Systems

Prompt injection: Manipulation of prompts to bypass safeguards

Fake identities: Synthetic identities used to bypass e-KYC controls

Model Risk and Governance

Accountability: Unclear ownership of AI decisions

Validation: Difficulty testing and explaining models

Bias: Unfair outcomes arising from biased data or model design

AI-enabled Fraud and Scams

Deepfakes: AI-generated impersonations enabling fraud

AI phishing: More sophisticated, personalised and scalable attacks

Third-Party Dependency and Concentration Risks

Third-party dependency: Limited visibility over vendor practices and embedded AI

Concentration risk: Reliance on a small number of foundation model providers

Workforce Impact

Overreliance: Erosion of staff judgement and critical thinking abilities

Workforce transition: Reskilling and redeployment of staff whose roles may be affected by AI

The findings align with the AI-related risks highlighted in BNM's **Emerging Operational Risk Survey (EORS) 2026/2027**, including data leakage, weak AI governance, cyber attacks, fraud, model risk and vendor concentration. These findings highlight the importance of FSPs **understanding their AI exposures, establishing appropriate accountability and assessing whether relevant safeguards remain effective**, consistent with applicable existing requirements.

Collaborative Enablers

Respondents generally **preferred practical and collaborative approaches** over prescriptive requirements to support the responsible adoption of AI. Respondents recommended **continued knowledge sharing, opportunities for safe experimentation, and greater regulatory clarity**. Collectively, these recommendations reflect a shared view that advancing AI adoption will require coordinated efforts across industry and regulators.

Roundtables, dialogues and community of practice

Respondents sought regular roundtables, dialogues and community of practice as mechanisms for knowledge sharing, capability building and reducing duplicated efforts across the sector.

Areas of interest

- Technical clinics and case studies to address AI implementation challenges
- Joint pilots on AI-enabled compliance tools and privacy
- Collaboration on AI use cases that deliver benefits for industry, consumers and the wider ecosystem

Testing and enablement support

Respondents identified safe experimentation and collaborative testing as practical enablers for validating control measures and strengthening AI risk management practices.

Areas of interest

- Dedicated AI Sandbox to test and refine emerging or higher-risk AI use cases
- Data-sharing or synthetic data initiatives to support responsible experimentation
- Red-teaming (simulated attacks and stress-testing) of AI systems

Regulatory clarity and guidance

Respondents viewed industry-developed guidelines complemented by regulatory clarity from BNM as a sound basis for orderly and proportionate adoption of AI.

Areas of interest

- Over 80% of respondents support an industry-wide AI adoption survey
- Co-development of practical AI governance guidelines
- Guidance to support consistent application of regulatory expectations for the use of AI

Advancing responsible AI adoption will require coordinated efforts across industry, technology providers, associations, academia and regulators. **BNM encourages industry participants to pursue these opportunities through collaboration with the wider ecosystem to strengthen collective capability and enable responsible innovation.**

From Insights to Action:

The feedback provides a clearer picture of how AI is evolving across the financial sector, including the opportunities institutions are pursuing, the challenges they face and the safeguards needed to support responsible adoption.

The next step is to translate these insights into action. BNM's way forward will be anchored in two complementary approaches:

- **Development:** Creating stronger avenues for knowledge sharing, practical testing and collective learning to help the industry build capabilities and adopt AI responsibly.

- **Regulatory:** Supporting a clearer understanding of how existing expectations apply to AI, while continuing to monitor emerging practices and risks to inform proportionate interventions as the landscape evolves.

Together, these approaches seek to enable responsible innovation while ensuring that safeguards and regulatory responses evolve alongside AI adoption.



Development Approach

BNM facilitates responsible innovation through four interconnected approaches:

Co-create and Engage

We collaborate with industry to identify emerging issues early, test high-value use cases and collectively shape the future of financial innovation



Adapt Regulation for Innovation

We strive to provide regulatory clarity to facilitate innovation while safeguarding stability, trust and financial integrity



Facilitate Safe Experimentation

We provide structured pathways where new ideas can be tested responsibly, enabling innovation within clear safeguards



Enable Shared Infrastructure

We support shared building blocks that allow innovations to interoperate, scale, and deliver system-wide value



As AI adoption evolves, new opportunities and considerations are emerging across a wide range of areas. BNM's development approach provides an adaptive framework to support responsible innovation, address implementation challenges and explore issues important to the financial sector, including consumer protection, Shariah compliance as well as agentic AI and other emerging use cases.

Advancing responsible AI adoption through coordinated action

Responsible innovation requires **a balanced pathway** that enables institutions to **pursue meaningful AI opportunities while strengthening governance, risk management and implementation capabilities**. BNM will work with industry to support adoption that is purposeful, proportionate and anchored in positive outcomes for the financial sector and consumers.

BNM seeks to advance an adoption trajectory that balances innovation with sound governance



Feedback received indicated that AI adoption across the financial sector is gaining momentum, with institutions increasingly viewing AI as a strategic capability to enhance efficiency, resilience and customer outcomes.

As AI capabilities continue to advance, there is also a growing opportunity to harness AI in addressing real industry challenges and supporting broader financial sector objectives. Together, these developments underscore the need for coordinated efforts to support responsible innovation and ensure AI adoption remains aligned with sound governance and positive outcomes for consumers and the financial sector.

> *"Innovation without trust is not progress. Innovation is not just adoption of technology, but also about leadership and governance to ensure that the financial system we build remains trusted and firmly anchored in the needs of society."*
>
> Governor, Bank Negara Malaysia

Focusing AI innovation on meaningful outcomes

FSPs are encouraged to prioritise "**win-win-win**" use cases that benefit consumers and FSPs, while advancing broader policy objectives. The areas below highlight opportunities for **near-term exploration and ecosystem-wide collaboration** to tackle shared challenges and unlock greater value from AI. We look forward to seeing further innovation across these areas and beyond, particularly where **AI can deliver meaningful outcomes for the financial sector**.

	Strengthen protection against fraud, scams and cyber threats	Expand fair and responsible access to financing	Address insurance and takaful protection gaps	Build confidence in AI-enabled financial services
Outcomes sought	Earlier detection, faster intervention and stronger protection as threats become more sophisticated and coordinated	Financing decisions that better reflect the circumstances and potential of underserved consumers and businesses	More accessible, relevant and responsive protection for households and businesses facing financial shocks	Consumers who can use AI-enabled services with greater clarity, agency and confidence
Direction of innovation	**Detect** synthetic identities and coordinated suspicious behaviour across channels **Anticipate** emerging scams and cyber security threats **Prioritise** alerts, automate appropriate responses, and support intelligence-sharing	**Anticipate** financing needs and emerging financial pressures **Expand** credit assessment using alternative data and cash-flow insights **Match** consumers and businesses to suitable financing based on their needs and circumstances	**Identify** changing protection needs across life and business events **Personalise** coverage and support according to changing circumstances **Improve** risk assessment, servicing and claims experience	**Guide** consumers through personalised and accessible financial support **Explain** product features, risks and trade-offs **Protect** consumers by identifying scams and supporting safer decisions

BNM stewardship can catalyse coordinated industry action, but progress will ultimately depend on collective industry effort

The following areas have been identified as potential avenues to address common implementation challenges, support responsible innovation and unlock opportunities for the financial sector. Insights generated through these engagements will help inform future supervisory, policy and development priorities. From 2027 onwards, BNM will work with industry to explore the following avenues for co-creation:

Co-creation initiatives for the financial sector

AI Responsible Innovation Forum (ARIF)

- **Mobilise industry stakeholders** to build shared understanding of AI governance, emerging risks and win-win-win use cases through structured peer learning and collaboration
- **Surface implementation insights and common challenges** to inform future Sandbox priorities and supervisory focus

Insights generated from ARIF, such as emerging use cases, tools and practices, may help identify areas for further exploration and testing

Testing Pathway for AI Solutions

- **Enable safe experimentation** of advanced AI use cases to validate controls, understand challenges and support responsible deployment
- **Generate evidence-based learning** to inform future policy and supervisory priorities

Insights from testing may help identify potential data access initiatives for further consideration

Improved Data Access

- **Explore pathways to enable better access to cross-institution and cross-sector data** and the use of "**synthetic data**" for win-win-win use cases
- **Develop appropriate safeguards** to balance innovation objectives with privacy, security and governance considerations

Introducing the AI Responsible Innovation Forum (ARIF)

Industry feedback calls for **practical collaboration, implementation insights and safe experimentation**. From 2027 onwards, BNM will work with the industry to **explore ARIF as a structured forum** for shared learning on AI governance and emerging risks, and to identify use cases for wider co-creation initiatives.

How ARIF will work

A collaborative platform

ARIF is expected to convene FSPs, fintechs, technology providers, researchers and public-sector partners around shared challenges and opportunities.

By bringing together industry experience, technical capabilities and policy perspectives, ARIF can build a stronger shared understanding of emerging issues and identify areas where collective action can make a difference.

Thematic, challenge-led engagements

Engagements will be structured around thematic chapters, each anchored in a clearly defined sector challenge and practical questions for the industry to work through together.

Chapters will combine technical clinics, knowledge sharing and peer exchange to surface practical approaches and areas for further exploration.

Turning learning into action

Each chapter will help surface shared insights, potential solutions and areas where further exploration, evidence or testing may be valuable.

Where appropriate, these learnings can support stronger industry practices and future testing pathways, while informing BNM's broader development and supervisory approach.

Priority area

Strengthening cyber resilience

Why this matters

AI can increase the speed, scale and sophistication of cyber threats, including phishing, deepfakes and synthetic identity fraud. As individual institutions may see only part of an evolving threat landscape, sector-wide collaboration can help build a fuller picture and strengthen collective resilience.

Potential areas for collaboration

Build a shared view of emerging threats and vulnerabilities, identify cross-institution exposures, and explore where joint red-teaming, common safeguards or controlled testing could add value.

Regulatory Approach

Three principles guide how BNM aims to unlock the upside of innovation, creating a conducive environment that promotes responsible innovation and a level playing field across the sector:

Parity
Activities that carry the same type of risk should be subject to the same regulations

Proportionality
Rigour of regulation calibrated to the level of institution-specific and systemic risk

Neutrality
Regulations are agnostic to different technologies, systems and approaches



BNM's role is to enable innovation that delivers meaningful benefits to consumers and the financial sector, while ensuring that associated risks are appropriately understood, governed and managed through proportionate safeguards, effective oversight and clear accountability.

Supporting responsible AI adoption through proportionate steps

As BNM's regulatory frameworks are largely **technology-neutral, proportionate and outcomes-based**, AI-related risks may be addressed through existing regulatory frameworks. **BNM is not introducing AI-specific regulation at this stage** and will continue to support responsible AI adoption through **existing regulatory expectations**, **proportionate supervision** and **ongoing engagement**.

Focus areas for FSPs:

Existing regulatory expectations continue to apply

- AI-enabled activities presenting risks similar to those posed by conventional activities remain subject to the same applicable regulatory requirements.
- Existing requirements, including those on governance, risk management, consumer protection and Shariah compliance, continue to apply to AI-enabled activities.
- Consider industry guidance, such as the AI Governance Framework and the upcoming AI Model Risk Management Framework.

Expected outcome:

Existing accountability requirements continue to apply where AI is used in regulated activities and decision making

Proportionate and risk-based application of requirements

- Apply existing requirements proportionately to the nature, scale and significance of the AI-enabled activities, taking into account the associated risks and potential impacts on business operations and customers.
- Implement stronger safeguards to higher-risk AI use cases, including proportionate testing, monitoring and human oversight, supported by a documented rationale and periodic reassessment as the use and risk profile evolve.

Safeguards calibrated to the risks and impact of AI

In the near term, BNM will deepen its **understanding of AI adoption**, **governance practices** and **key third-party dependencies** across the sector, while **strengthening multidisciplinary capability within existing supervisory structures.** These **insights may inform further supervisory engagements where warranted**, potentially including thematic reviews, guided by evidence and risk materiality. Industry engagement and shared learning through ARIF will complement these efforts by **surfacing implementation challenges** and **deepening understanding of AI governance and emerging risks.**

Existing regulatory expectations continue to apply

FSPs are encouraged to **translate applicable requirements into effective controls** for each AI use case, by assigning clear ownership, addressing identified gaps and maintaining ongoing oversight to ensure controls remain effective. The policy documents below provide a starting point for identifying relevant requirements, with **FSPs responsible for considering the full range of applicable requirements** based on the nature, risk and impact of each use case.

Key policy documents with expectations that remain applicable to AI use include (non-exhaustive):

Risk Management in Technology (RMiT)	**Corporate Governance**	**Risk Governance**	**Responsibility Mapping**	**Fair Treatment of Financial Consumers (FTFC)**
Outsourcing	**Capital Adequacy Framework**	**Management of Customer Information and Permitted Disclosures (MCIPD)**	**Guidelines on Data Management and Management Information System (MIS) Framework**	**Complaints Handling**

FSPs remain responsible for complying with applicable laws relating to personal data protection and intellectual property (IP) rights. FSPs **are also encouraged to consider internationally recognised standards, frameworks and guidance**, including but not limited to:

National Institute of Standards and Technology (NIST) AI Risk Management Framework	**Basel Committee on Banking Supervision (BCBS) Principles for Effective Risk Data Aggregation and Risk Reporting**

Building on existing regulatory expectations, industry-led frameworks can help FSPs strengthen AI governance and model risk management

To support responsible AI adoption, the Chief Risk Officers' (CRO) Forum of the Asian Institute of Chartered Bankers (AICB) issued the AI Governance Framework in 2025, endorsed by the Association of Banks in Malaysia (ABM). Building on this, the CRO Forum will issue the AI Model Risk Management Framework soon.

2025

AI Governance Framework (AIGF)

Provides industry-led guidance on institutional governance, accountability and responsible AI practices.

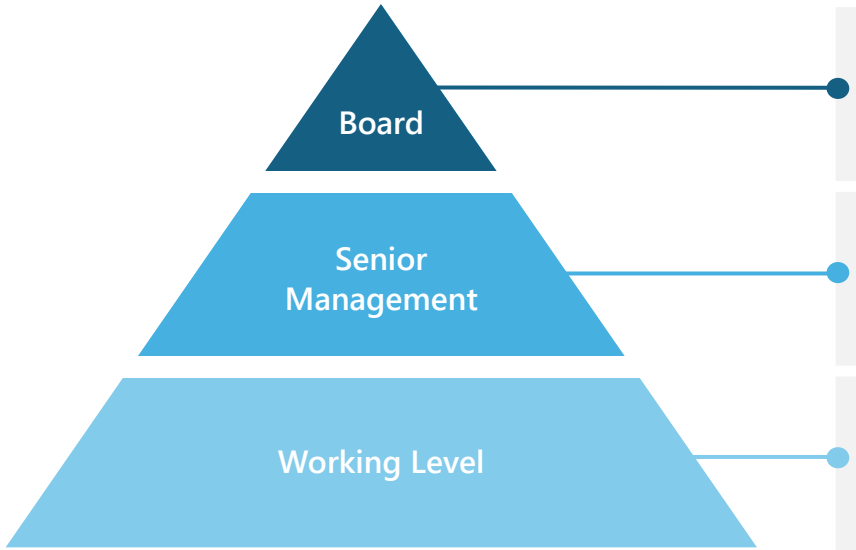
FSPs may **consider the seven AIGF principles** *(Fairness, Ethical Use, Accountability, Transparency, Explainability, Reliability and Security)* and address any gaps.

Coming soon

AI Model Risk Management (MRM) Framework

Provides more specific guidance on managing model risks across the AI lifecycle. Existing expectations continue to apply in the meantime.

Once issued, FSPs may consider **assessing current practices against the guidance's recommendations** on model validation, monitoring, data governance and human oversight.



AIGF Layers	Accountability focus	What FSPs should put into practice
Board	**Set direction and oversee outcomes**	Align AI strategy with risk appetite and capacity Challenge material AI uses and hold management accountable for governance and outcomes
Senior Management	**Build institutional readiness**	Translate frameworks into applicable policies and processes, with clear ownership, adequate expertise, proportionate approvals, independent challenge and escalation arrangements
Working Level	**Demonstrate effective controls**	Assess risks before deployment; test and validate models, protect data and maintain human oversight Monitor outcomes, reassess material changes and escalate concerns

Proportionate and risk-based application of requirements

Not all AI use cases carry the same risks, and safeguards should reflect this. **Governance expectations, risk controls and supervisory attention should be proportionate to the materiality, complexity and potential impact of each use case.** For example, AI that could materially influence customer outcomes, financial decisions or regulatory obligations may require stronger safeguards than applications focused on internal process efficiency.

The table below illustrates how proportionality can be applied in practice across validation, approval and security requirements:

	Where the assessed risks warrant simpler controls	Where the assessed risks warrant stronger controls
Governance and approvals	Department-level approval may suffice for internal productivity tools, such as meeting summarisation applications.	More senior-level oversight or approval may be appropriate, depending on the materiality and potential impact of the use case, such as credit decisioning applications.
Testing and validation	Simplified validation where employees review AI outputs before use.	More comprehensive testing and independent validation for models that materially influence customer outcomes or financial decisions, such as credit underwriting.
Security and adversarial testing	Security checks proportionate to the application's intended use and risk exposure.	More extensive cybersecurity and adversarial testing may be considered, where relevant, based on the nature of the use cases and associated risk exposures, particularly for external-facing applications.

These examples are illustrative only and do not introduce new requirements, thresholds or approval arrangements. FSPs remain responsible for determining appropriate controls based on applicable regulatory requirements and the circumstances and risks of each use case.

Emerging Best Practices for Responsible AI Adoption

AIDP feedback suggests that the financial sector is moving from exploration towards broader implementation of AI. As adoption scales, FSPs will need to apply appropriate judgement in adapting governance, oversight and risk management practices alongside AI deployment. This section highlights emerging considerations and illustrative practices to support responsible AI adoption, with a focus on strengthening consumer outcomes, managing emerging risks from increasingly autonomous AI systems and ensuring alignment with Shariah principles.



Responsible AI Strengthens Trust and Consumer Outcomes

AI adoption should be guided by fairness, accountability and strong data governance to protect consumers and build public trust.

Agentic AI Requires Stronger Guardrails and Oversight

As AI systems become more autonomous, robust safeguards are needed to ensure outcomes remain fair, transparent and aligned with institutional objectives.

AI Adoption Should Remain Anchored in Shariah Principles for Islamic Financial Institutions

AI-enabled solutions should uphold Shariah objectives through appropriate governance, human oversight and transparency.

Responsible AI adoption strengthens consumer outcomes

As AI adoption evolves, financial institutions remain accountable for ensuring AI is governed responsibly, uses data appropriately, and delivers fair and trusted outcomes for consumers. Consumer trust is built when AI is fair, accountable and supported by strong data governance. The following are emerging best practices that FSPs are encouraged to adopt to ensure AI use strengthens consumer outcomes.

Institutions remain accountable for AI-driven decisions and outcomes*

- Boards and senior management set expectations for the responsible use of AI that aligns with the institution's standards of conduct and considers potential impacts on customers.
- FSPs maintain sufficient understanding and oversight to explain, challenge and correct AI-driven decisions, proportionate to their potential impact on customers.

** Aligned with Principle 1 of the Fair Treatment of Financial Consumers Policy Document*

AI should be deployed in a manner that promotes fair treatment and positive consumer outcomes

- Identify, mitigate and monitor risks of bias, unfair outcomes and consumer harm, and take timely corrective action where adverse outcomes are identified.
- Validate AI-enabled products, services and recommendations appropriately before deployment and monitor on an ongoing basis to ensure they remain aligned with consumers' needs and circumstances, including those of vulnerable consumers.
- Establish clear boundaries for AI use, including prohibiting use cases where material risks of discrimination, unfair treatment or consumer harm cannot be adequately mitigated.

Robust data governance is fundamental to safe, reliable and trusted AI adoption

- Maintain strong safeguards and consent practices governing the collection, use, sharing, storage and protection of customer information used for AI-enabled products, services or recommendations.
- Adopt effective data governance practices to support reliable, accurate and fair AI outcomes, including consistent data definitions, formats and classifications. In addition, maintain clear records of where data comes from and how it is transformed and used, and enable consistent and controlled use of data across systems.

Agentic AI could unlock new value, but requires stronger safeguards

Agentic AI marks a shift from AI that primarily supports decisions to systems capable of undertaking increasingly autonomous, multi-step actions. As FSPs explore greater autonomy, safeguards should be proportionate to the potential impact, with clear authority boundaries, robust execution controls and effective human intervention. Continued testing will be important to strengthen and refine good practices as capabilities and use cases mature. The following emerging practices are intended to guide FSPs' exploration of agentic AI and support continued industry learning.

Clear accountability and boundaries for autonomous actions

- Clearly map the decisions and actions that each agent is permitted to undertake across connected systems, with clear institutional accountability for resulting outcomes.
- Define and calibrate permitted activities, access rights and transaction limits based on the FSP's risk tolerance.
- Implement clear thresholds or circumstances for human approval and escalation arrangements where actions exceed defined limits or could materially affect customers.

Continuous oversight and adaptive safeguards

- Adapt and strengthen existing controls, including access management, logging and monitoring, to address risks arising from autonomous and multi-step operations.
- Monitor agentic AI systems on an ongoing basis to identify unintended outcomes, privilege escalation and autonomy drift as agent behaviour and underlying processes evolve.
- Establish clear avenues for customer review and redress where agentic AI-enabled decisions materially affect customers.

Controlled exploration focused on beneficial outcomes

- Prioritise agentic AI use cases that deliver shared benefits for customers and institutions, such as identifying emerging threats and proposing detection rules that strengthen fraud prevention and reduce potential customer harm.
- Adopt a controlled experimentation approach for agentic AI to build understanding of its capabilities and risks before progressively expanding the scope or autonomy of activities.
- Build customer protection into the testing and use of agentic AI for financing decisions, including safeguards to ensure fair and transparent outcomes and assess suitability and affordability.

AI adoption should be anchored in Shariah values and governance

AI offers significant opportunities for Islamic finance, but its adoption by Islamic financial institutions (IFIs) should remain guided by Shariah objectives and supported by robust governance, oversight and accountability arrangements. The following are emerging best practices that IFIs are encouraged to adopt to ensure that AI adoption aligns with Shariah values and principles.

AI adoption supports realisation of the objectives of Shariah *(Maqasid al-Shariah)*

- Ensure AI adoption supports outcomes consistent with Shariah principles and objectives, including fairness, prevention of harm, preservation of rights and Shariah compliance.
- Provide clear and comprehensible disclosures for AI-enabled offerings, enabling customers to understand key features, risks and contractual implications without material uncertainty (*gharar*).
- Ensure AI systems and AI-supported decisions are sufficiently explainable and traceable to enable appropriate Shariah review, validation and assurance to support effective Shariah governance.

Accountability for Shariah decisions remains with the Shariah Committee

- AI should support, rather than replace, human Shariah decision-making, including by providing analysis and recommendations to inform consideration.
- Final Shariah decisions remain subject to appropriate human review and judgement, with IFIs remaining accountable for AI-enabled outcomes, while the Shariah Committee is accountable for decisions that fall within its remit.

The next phase of AI adoption should be defined not simply by how widely AI is deployed, but by how effectively and responsibly it delivers value. This means creating the conditions for AI to scale with confidence, while safeguarding the resilience, accountability and trust that underpin the financial system.

BNM will continue to work alongside industry, supporting shared learning, safe experimentation, and proportionate regulation and supervision as technologies, use cases and risks evolve.

The opportunity now is to move from insight to implementation, translating these foundations into stronger practices, greater confidence and responsible AI adoption at scale.

Key considerations highlighted in this Feedback Statement:

- Clear accountability for AI-enabled decisions and outcomes
- Strong governance and oversight arrangements before scaling deployment
- Robust data governance and data quality foundations
- Preparedness to address AI-enabled fraud, scams and cyber threats
- Effective management of third-party and concentration risks
- Appropriate human oversight for material AI-enabled decisions



Prepared by
Harizal Alias, Farhana Hassan Naziri, Atiqah Zaki, Asha Baskaran, Ong See Qi, Lydia Awarudin
Financial Development and Innovation Department | November 2026 | aipolicy@bnm.gov.my

To learn more about BNM's innovation agenda and related initiatives, visit bnm.gov.my/innovation.

© 2026 Bank Negara Malaysia. All rights reserved. No part of this presentation may be reproduced, distributed, published or transmitted in any form or by any means without the prior written consent of Bank Negara Malaysia.

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA