BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Discussion Paper

Digitalisation in Financial Services

Artificial Intelligence in the Malaysian Financial Sector

AI adoption in Malaysia's financial sector is gaining momentum – what does responsible innovation look like for financial service providers?

August 2025

This discussion paper outlines Bank Negara Malaysia (BNM)'s proposed approach and views relating to the development and adoption of artificial intelligence (AI) in the Malaysian financial sector. This discussion paper is a non-binding publication and may not result in an exposure draft or policy document under the same title.

BNM invites all relevant stakeholders, including financial service providers, government agencies, industry associations, technology service providers, consumer groups, non-governmental organisations, and other interested parties to review this discussion paper and provide written feedback on the issues discussed.

BNM highly encourages feedback to be supported by appropriate justification, rationale and evidence. We kindly request respondents to specify the applicable paragraphs and provide sufficient examples or illustrations.

By submitting feedback, comments, or proposals in response to this discussion paper, respondents acknowledge and agree that BNM may reproduce, publish, or otherwise use the content of such submissions, in whole or in part, in any form and for any purpose it deems appropriate. BNM is not obligated to seek permission from, or provide attribution to, the respondents. BNM will not publish or disclose the names or identifiable details of respondents unless explicit consent is provided or disclosure is required by law.

All feedback for the discussion paper is to be submitted electronically and emailed to aipolicy@bnm.gov.my latest by 17 October 2025. The email must be titled "*AI in the Malaysian Financial Sector: Feedback from [name of institution/individual]*".

Any queries relating to this discussion paper can be directed to aipolicy@bnm.gov.my.

Contents

Part A: Introduction

Part B: BNM's Approach to Artificial Intelligence Adoption in the Financial Sector

Part A: Introduction

1 BNM's Posture on Artificial Intelligence

1.1 Artificial intelligence (AI) represents a transformative advancement in technology, with the potential to fundamentally reshape the delivery of financial services. This transformation has been accelerated by the advent of accessible Generative AI (GenAI) in recent years. When properly trained, AI systems can deliver significantly enhanced operational efficiency and improved customer experiences. As interactions increasingly shift from physical to digital channels, customers now expect more seamless, intelligent, and personalised financial services.

1.2 With 97% of Malaysian households having internet access and 98% having access to smartphones[1], the Malaysian financial sector is well-positioned to adopt and benefit from AI technologies.

1.3 While there is no single universally accepted definition of AI[2], there is broad consensus that AI refers to machine-based systems designed to perform tasks that typically require human intelligence. With the advent of GenAI, some standard setting bodies have updated their definitions of AI to encompass the ability for such systems to generate content, in addition to making predictions to support decision making.

1.4 For the purposes of this discussion paper, AI is defined as "*the use of advanced computer systems capable of processing and analysing large volumes of data and performing tasks that traditionally require human intelligence, including generating content or making predictions to aid in decision making processes*"[3]. This definition is intended to provide clarity within the scope of this discussion paper and does not represent a formal or regulatory definition of AI.

1.5 BNM is committed to ensuring that the financial system remains resilient and continues to play its role in supporting economic activity. Amidst increasing digitalisation of financial services, we will continue to provide a facilitative environment for responsible innovation in the financial sector and strive to promote a regulatory environment that is responsive to technological advancements. We are also committed to ensuring that our regulatory approach for AI aligns with the principles of parity, proportionality, and neutrality for regulating innovation[4].

[1] DOSM (2025).

[2] BIS (2024d). OECD (2024b).

[3] AI is a broad field, of which "machine learning" (ML) is a sub-category.

[4] For further information on our approach to regulating innovation, see pg. 77 of the Financial Sector Blueprint (2022 – 2026). BNM (2022).

1.6 In the context of AI, BNM aims to facilitate and encourage responsible adoption and use of AI across the financial sector in a manner that will advance better consumer outcomes and our broader policy objectives. This means that while new innovations, such as AI, are given the opportunity to flourish, associated risks that may negatively impact system-wide stability, consumer outcomes, and confidence in the financial sector will need to be managed effectively.

1.7 BNM closely monitors[5] technological developments and innovation in the financial sector to shape our future regulatory and supervisory approach on AI. This discussion paper seeks to share and obtain feedback on the following:

i) BNM's posture on responsible AI innovation in the financial sector;

ii) The proposed regulatory approach for AI, as well as industry guidelines on responsible use; and

iii) General development approach, including priority areas for greater innovation and industry-led collaboration.

For feedback

1. BNM welcomes industry feedback on whether a formal sector-specific regulatory definition of AI would be beneficial, including:
   - How would such a definition support greater clarity, consistency, or compliance in the financial sector?
   - What should be the appropriate definition of AI for the Malaysian financial sector?

[5] In 2023, BNM published a box article in the Financial Stability Report 2H 2022 on the state of early adoption and potential risks arising from the use of AI in the financial sector. The article noted a growing use of predictive AI in the financial sector. BNM (2023).

2 Artificial Intelligence Adoption Trends in the Malaysian Financial Sector

2.1 To gain deeper insights into recent advancements on AI within the Malaysian financial sector, BNM interviewed select local financial industry players throughout 2024 and issued an updated industry-wide survey (BNM AI Survey 2024)[6]. The AI Survey 2024 received responses from 120[7] financial service providers (FSPs)[8,9]. This section will discuss the findings from the interviews and the BNM AI Survey 2024.

2.2 Overall, FSPs in Malaysia are increasingly adopting AI. Notably, in 2024, 71% of banking institutions and DFIs had implemented at least one AI application, an increase from 56% in the previous year. Similarly, 77% of ITOs had adopted at least one AI application, compared to 58% in the previous year.

2.3 This trend looks set to continue in the coming years as over half of the respondents agreed that AI has the potential to generate significant new value for both their organisations and consumers. As illustrated in *Exhibit 1*, this insight has translated into growing prioritisation for AI adoption across different segments of the financial sector. Looking ahead, more than 60% of banking institutions and ITOs view AI as a strategic priority at their institutions in the next 1-3 years.

[6] The first industry-wide BNM AI Survey was issued in 2023.

[7] Including combined responses from group institutions.

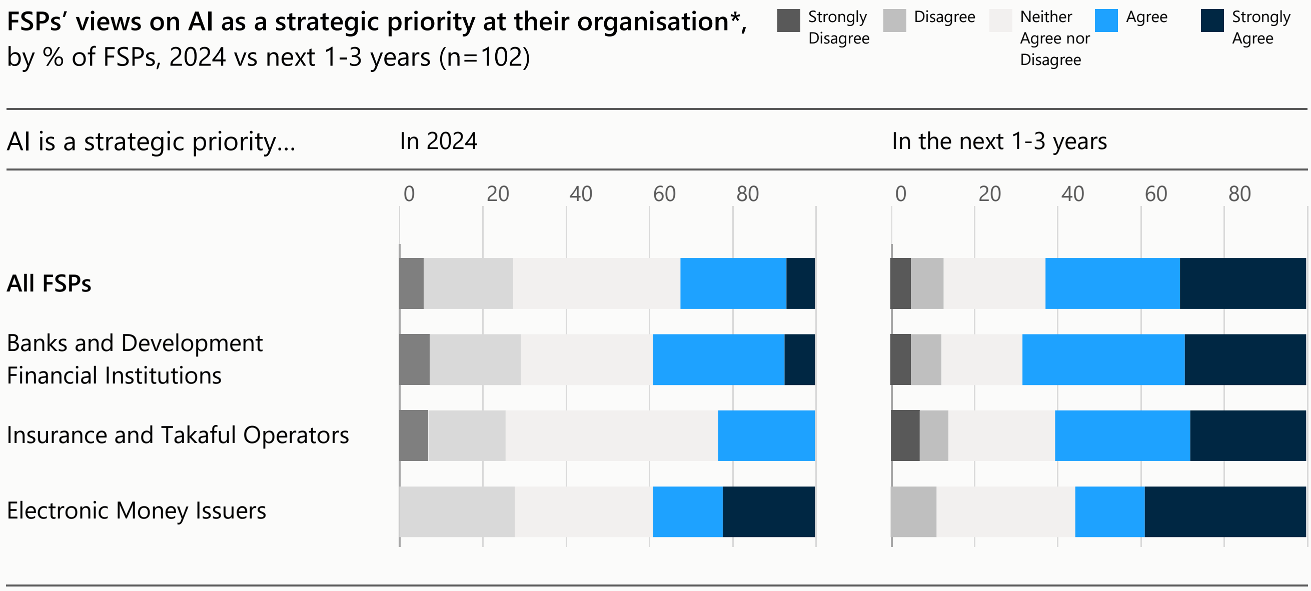
[8] "Financial service providers" (FSPs) include licensed banks, Islamic banks, and investment banks (banks), insurance and takaful operators (ITOs), development finance institutions (DFIs), and electronic money issuers (EMIs).

[9] Where applicable, "financial institutions" in this discussion paper refer to banks, ITOs and prescribed DFIs.

Exhibit 1

Financial service providers in Malaysia are increasingly prioritising AI adoption

FSPs' views on AI as a strategic priority at their organisation*, by % of FSPs, 2024 vs next 1-3 years (n=102)



* Respondents include banks, development financial institutions, insurance and takaful operators, and electronic money issuers, irrespective of whether they have tested/ deployed AI projects or otherwise.

Source: BNM AI Survey 2024

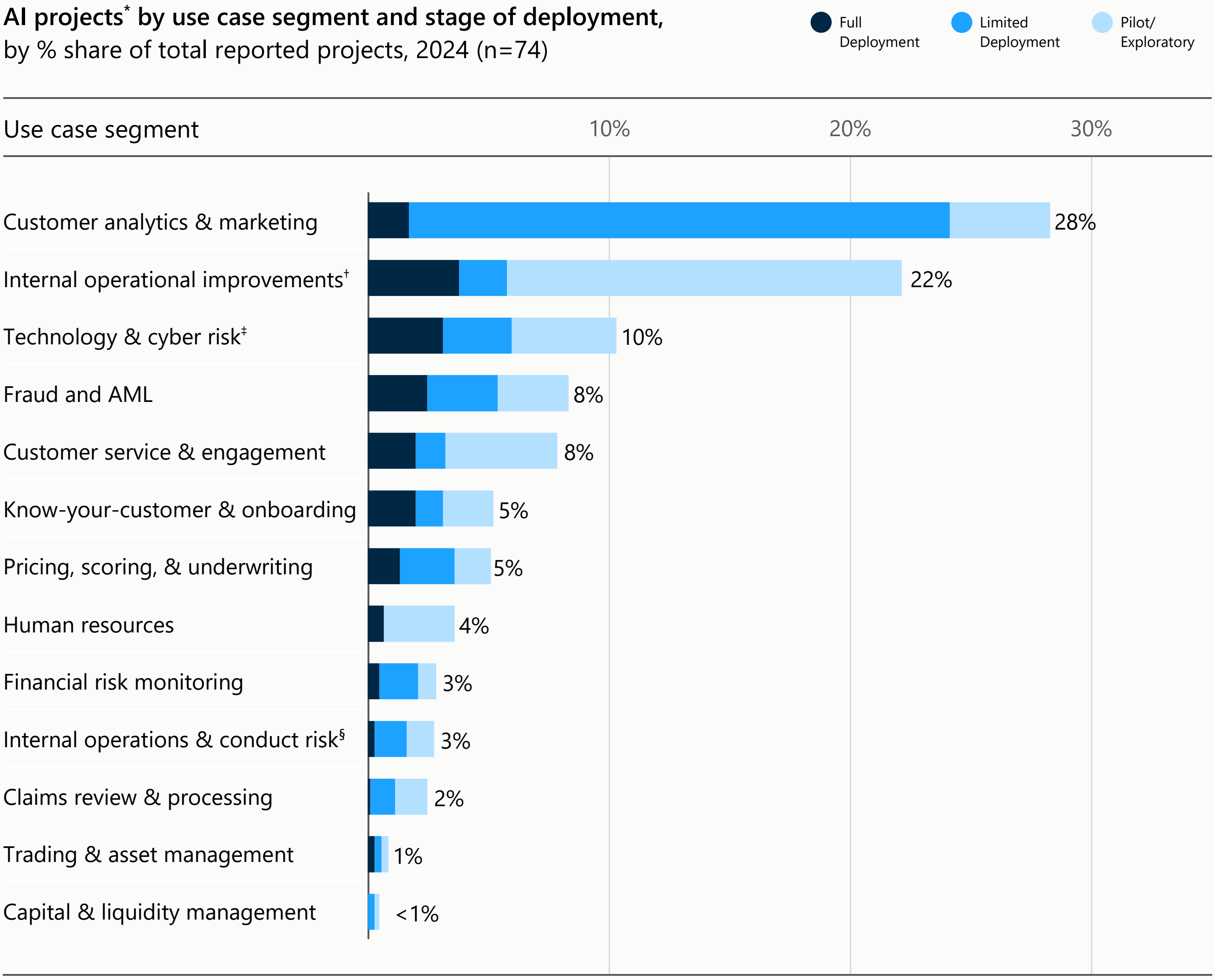
2.4 Most FSPs deemed 2024 to be a pivotal year for AI exploration for the financial sector. Overall, FSPs deployed over eight times more pilot or exploratory AI applications compared to the previous year. Over the same period, FSPs rolled out 30% more AI applications for limited and full deployment compared to 2023. The overall growth in reported AI applications in 2024 compared to the previous year may be attributed to the increased interest in exploring GenAI applications.

2.5 Based on interviews with select FSPs, we observed that AI is utilised across the value chain, supporting a wide range of activities across front, middle, and back-office functions. Most AI applications currently in development or expected to be deployed in the near-term are designed to augment rather than replace human decision-making. While we have not observed trends in the adoption of more autonomous agentic AI systems, this remains an area for potential interest as capabilities evolve.

2.6 As shown in *Exhibit 2* below, the most common AI applications developed or deployed in 2024 were for “customer analytics & marketing” and “internal operational improvements” segments, followed by “technology and cyber risk”, and “fraud and AML”. These segments saw the highest growth in AI projects, partly driven by increased exploration of GenAI, although most of these applications remain in the testing phase.

Exhibit 2

AI projects in the financial sector are deployed across various functions throughout the organisation, primarily in non-financial risk areas mainly for internal process improvements



AI projects* by use case segment and stage of deployment, by % share of total reported projects, 2024 (n=74)

* Number of projects can refer to number of initiatives, solutions, or models. † Including the use of AI to improve processes and automation in operational areas. ‡ Relating to the use of AI for tech risk and cybersecurity solutions to detect internal malware and respond to security threats. § Including the use of AI for internal monitoring purposes to manage conduct risk.

Source: BNM AI Survey 2024

Spotlight

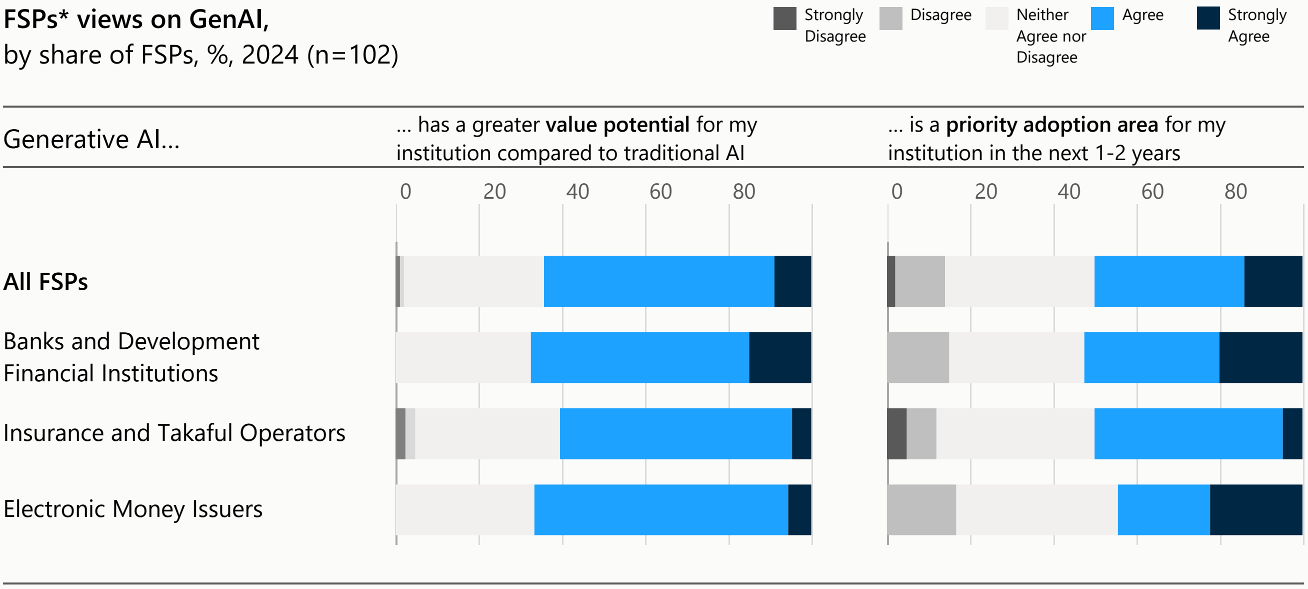
Adoption of Generative AI in Financial Services

In recent years, a confluence of technological and market developments has enabled the rapid advancement and adoption of Generative AI (GenAI) technologies. This includes exponential growth in computing power, the availability of vast and diverse datasets and breakthroughs in deep learning architectures such as transformer models. These developments have not only lowered the barriers to deploying sophisticated AI solutions across industries but also prompted FSPs to actively assess how GenAI can be integrated into their operations.

Exhibit 3 shows that a majority of FSPs recognise the potential benefits of adopting GenAI in their institutions and consider GenAI implementation a strategic priority in the next 1-2 years.

Exhibit 3

A majority of FSPs recognise the potential benefits of adopting GenAI in their institutions, and consider GenAI implementation a strategic priority in the next 1-2 years



FSPs* views on GenAI,
by share of FSPs, %, 2024 (n=102)

* Respondents include banks, development financial institutions, insurance and takaful operators, and electronic money issuers, irrespective of whether they have tested/ deployed AI projects or otherwise.

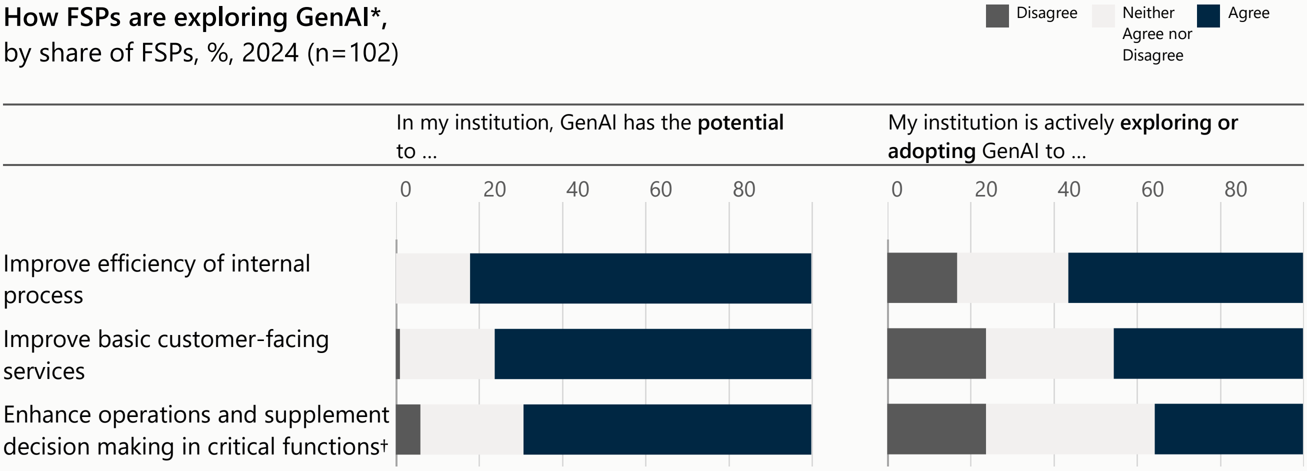
Source: BNM AI Survey 2024

While FSPs broadly acknowledge the strategic importance of GenAI, views remain divided on whether its greatest value lies in driving operational efficiencies or unlocking new revenue opportunities. *Exhibit 4* below offers a more nuanced view, highlighting where FSPs are currently focusing their efforts and where they anticipate the most impact.

Exhibit 4

FSPs recognise the broad potential in GenAI but are initially focusing adoption efforts on improving internal processes

How FSPs are exploring GenAI*,
by share of FSPs, %, 2024 (n=102)



* Respondents include banks, development financial institutions, insurance and takaful operators, and electronic money issuers, irrespective of whether they have tested/ deployed AI projects or otherwise. † For example, core banking and payment systems, risk assessment processes, sensitive customer interactions, and credit and insurance underwriting for critical portfolios.

Source: BNM AI Survey 2024

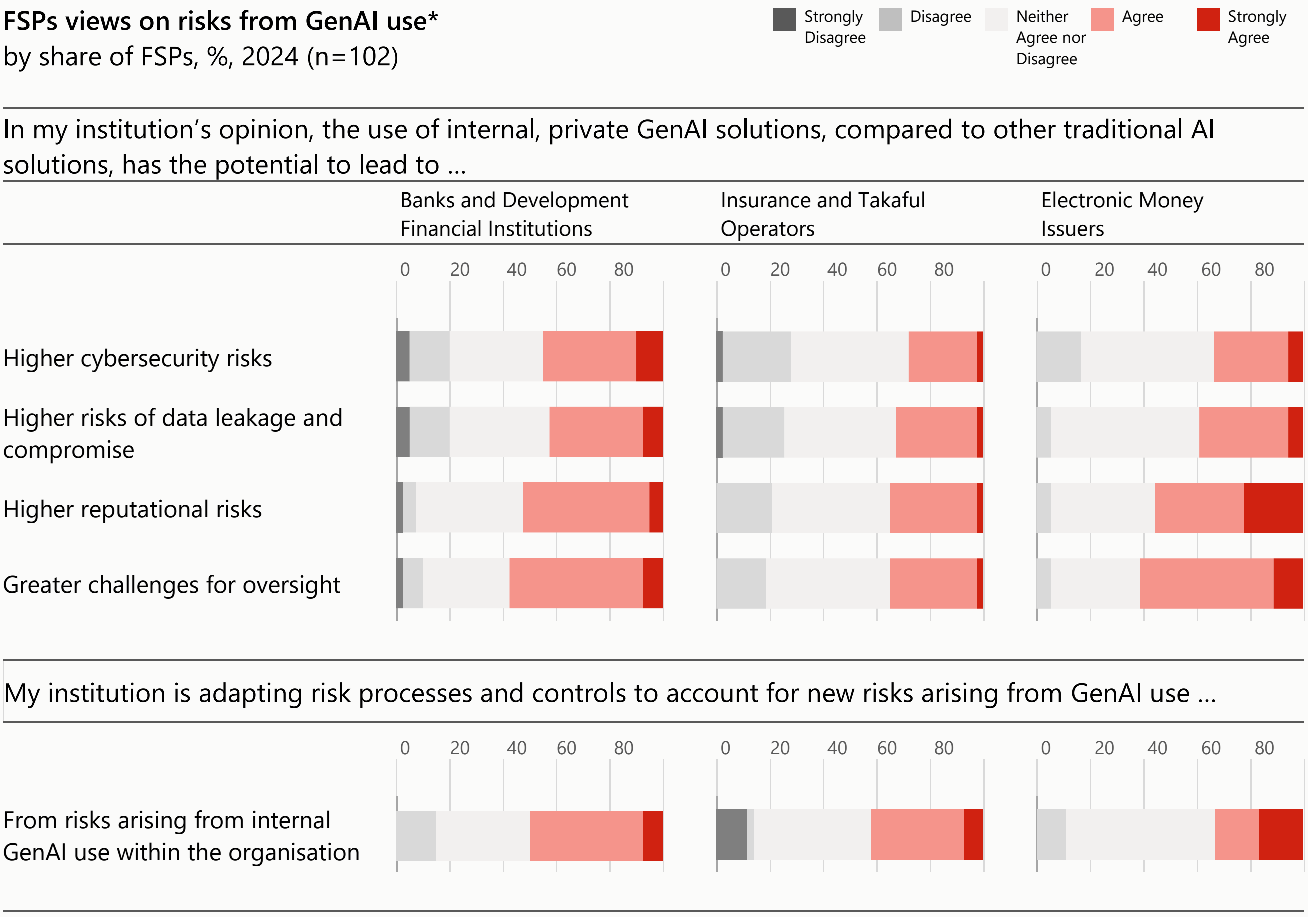
A significant majority of FSPs recognise the strong potential of GenAI to enhance and increase the efficiency of internal processes, with many actively exploring or already adopting GenAI for these use cases. Examples include productivity tools such as AI chatbots for staff queries, claims assessment tools, HR onboarding, and internal communications.

While many FSPs are actively exploring GenAI for internal process improvements across the institution, executive level engagement appears more limited. Despite strong and growing organisational interest, only one in five FSPs responded that their senior leaders and C-suite executives are actively using internal or publicly available GenAI tools for their own work.

Many FSPs are already grappling with operational and compliance risks associated with internal GenAI use. As illustrated in *Exhibit 5*, banks that are ahead in GenAI adoption are particularly attuned to the risks associated with internal use and are adapting risk management processes to address them.

Exhibit 5

Banks are more concerned of risks when using internal GenAI (vs traditional AI), prompting considerations on appropriate risk management processes



* Respondents include banks, development financial institutions, insurance and takaful operators, and electronic money issuers, irrespective of whether they have tested/ deployed GenAI projects or otherwise.

Source: BNM AI Survey 2024

Admittedly, GenAI has introduced a new set of cybersecurity challenges for FSPs, particularly as bad actors increasingly exploit the technology for malicious purposes (e.g., use of GenAI to generate malicious software or AI-generated scripts). Moreover, GenAI has enabled more sophisticated cyber threats, including deepfakes, advanced phishing scams, and identity fraud that are harder to detect and defend[10]. In response, FSPs have begun updating their internal controls to better manage these emerging threats.

To conclude, as FSPs in Malaysia continue to explore the transformative potential of GenAI, they are also becoming more attuned to emerging risks associated with this new technology. Many are taking a proactive, yet cautious stance. Customer-facing GenAI applications remain limited, and FSPs have not yet indicated plans to explore GenAI applications in financial risk areas. When implemented in a safe and responsible manner, GenAI technologies can unlock meaningful gains for enhancing consumer outcomes and improving operational efficiency. A balanced innovation and risk management approach will be critical as the financial sector navigates the next phase of GenAI responsible innovation.

[10] FRBNY (2025), IMF (2023).

2.7 Based on interviews and survey feedback, we anticipate that FSPs will continue to focus on developing AI applications in non-financial risk areas[11], such as for fraud detection and customer analytics applications. In contrast, financial risk related applications, such as pricing, scoring, and underwriting, have seen comparatively slower growth in the number of AI projects.

2.8 Notably, FSPs are increasingly shifting from siloed, business unit-specific AI deployments toward more centralised and institution-wide operating models. In 2024, over a third of FSPs indicated that all AI projects within their institutions are initiated and guided by an institution-wide AI strategy, and over a quarter of FSPs have established AI Centres of Excellence (CoE) to execute these projects.

2.9 A growing number of AI applications are being developed internally by FSPs. Some FSPs have reported a preference for in-house development to support better alignment with internal policies and regulatory requirements, enable better customisation to business needs and address transparency concerns associated with the use third-party models and applications. FSPs are also seeking to develop in-house capacity to build, maintain, oversee, and monitor AI applications in the longer term.

2.10 Looking ahead, BNM will continue to engage FSPs to enhance our understanding of both the opportunities and challenges associated with AI adoption in the financial sector. These efforts will support our broader objective of fostering responsible innovation across the industry.

[11] For the purposes of this discussion paper, "non-financial risk areas" refer to the set of AI use cases that do not directly impact capital adequacy, financial risk modelling, or balance sheet metrics. These include but are not limited to applications focused on operational efficiency, customer analytics, fraud detection, compliance monitoring, and other internal control functions.

Box Article 2

Case Study

AI at BNM: Machine Learning for Anomaly Detection in Money Services Business (MSB) Outlets

In a meeting room at BNM, a team of data scientists and MSB supervisors gathered around a geospatial dashboard. The screen displayed a map of Malaysia, dotted with hundreds of MSB outlets. Some glowed red, flagged as potentially anomalous by a new machine learning model. For the team, the model offered a new tool, one that could significantly improve supervisory efficiency and effectiveness in risk detection.

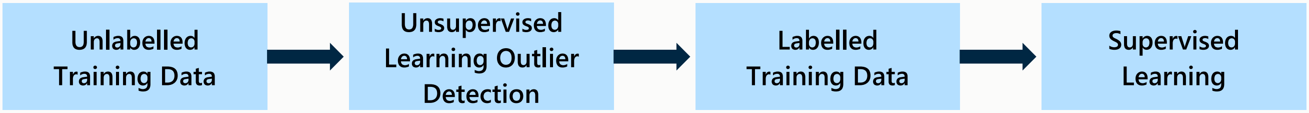
The MSB supervision team at BNM had long recognised the risks inherent within the MSB sector. With more than 80% of over 250 licensed MSBs operating across the country permitted to conduct currency exchange through physical outlets, the cash-intensive and cross-border nature of the sector presented heightened exposure to money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks. This increasingly challenges the effectiveness of traditional oversight methods.

The SupTech journey

Before 2017, the MSB supervision team's approach relied heavily on manual examinations to identify and monitor ML/TF/PF risks. However, the approach was limited by the manual analysis on the sample data collected, static risk profiles and assessments. Consequently, supervisory resources were stretched thin.

In early 2017, BNM established a data analytics unit to support its supervisory mandate in the MSB sector. The unit's goal was to collect and transform raw, granular transactional data from MSBs into actionable risk insights through supervisory technology (SupTech) applications. These in-house developed applications operate at three levels – industry, entity and customer, with entity-level analytics being a key focus. With limited resources and a growing number of MSBs, the approach offered a scalable way to apply proportionality in oversight and bring greater consistency to supervisory assessments. However, the lack of precisely labelled data presented a challenge in training a robust model, prompting the unit to explore a weakly-supervised learning approach that could operate effectively under such constraints.

Weakly-supervised machine learning framework



The machine learning framework

The weakly-supervised machine learning framework integrates both unsupervised and supervised learning, which are trained on multiple features extracted from the transactional, outlet and geolocation data of the MSB outlets for a robust anomaly detection. Referring to the framework, it first applies an unsupervised Isolation Forest (IF) model to the data to identify anomalous outlets across multiple features. These anomalies then serve as training labels for the supervised machine learning, refining detection accuracy.

A key benefit of this framework is its ability to accommodate noisy or imperfect labels, due to the limited real-world cases on anomalous outlets. This iterative method improves the model's adaptability while maintaining oversight of emerging risks.

To enhance the model's explainability, Shapley Additive exPlanations (SHAP) values and partial dependence plots are used to assess feature importance, ensuring transparency in anomaly detection. Overall, the integration of multiple data sources and machine learning techniques strengthens risk monitoring in MSB supervision.

Usage and further improvements

The detection output from the machine learning model is visualised in a geospatial dashboard to facilitate analysis and supervisory planning. This dashboard maps the identified anomalous and normal MSB outlets, enhancing risk identification and targeted supervision.

Further enhancements include refining model accuracy through continuous learning and expanding data sources to improve anomaly detection. Ultimately, the model demonstrated the potential of integrating machine learning and geospatial analytics in financial supervision, offering a proactive approach to risk management.

For feedback

2. How frequently should BNM engage with FSPs on AI-related matters, and through which channels, e.g., surveys or consultations?
3. What parameters or indicators should BNM consider in future engagements with FSPs to better assess AI adoption, maturity, and impact across the sector?
4. How do you see AI evolving in the Malaysian financial sector over the next 3-5 years? BNM invites your views on emerging trends, opportunities, and potential challenges that may shape the sector’s AI trajectory.

3 Benefits and Risks of Artificial Intelligence Adoption

The use of AI has the potential to bring significant benefits to both consumers and FSPs…

3.1 AI has the potential to revolutionise the financial sector, transforming how institutions operate, make decisions, and interact with customers. FSPs adopting AI may already be experiencing efficiency gains through the automation of routine tasks, improvement in risk management capabilities, and developing AI-driven product offerings. Furthermore, this technology has the potential to enhance the delivery of financial services to customers, thereby improving financial inclusion outcomes.

3.2 For example, the responsible use of AI in scoring (e.g., underwriting and credit) could enable FSPs to offer products that meet the unique needs of unserved and underserved segments, including "thin-file" customer segments with limited financial histories. This includes addressing working capital needs and providing tailored protection coverage for microentrepreneurs and lower-income groups. Improvements in model accuracy and scoring could lead to lower non-performing loans (NPLs) and risk mitigation costs, translating into more affordable financing access for consumers.

3.3 Globally, FSPs are actively exploring chatbots, virtual assistants, and similar applications to enhance customer experience[12]. AI has also been used to improve customer experience and convenience in some customer-facing applications in recent years, notably AI-driven electronic Know-Your Customer (e-KYC) solutions that facilitate digital account opening experiences. Developments in GenAI promise to take this a step further.

3.4 The application of AI in fraud detection enables FSPs to more accurately identify suspicious activities, reduce false positives, and prevent financial crimes in real time. Advancements in AI are continuously enhancing these capabilities by analysing behavioural anomalies, detecting fraudulent transactions with greater precision, and mitigating social engineering threats (e.g., phishing). These advancements have the potential to reduce fraud-related losses for customers and FSPs, ultimately leading to greater trust in the financial ecosystem.

[12] NVIDIA (2024).

However, AI adoption may intensify existing risks ...

3.5 A major challenge of AI revolves around ensuring fair usage of the technology. AI models could exacerbate biases and discrimination, especially when the underlying input data is flawed or of low quality. For example, AI models trained on biased data in credit underwriting may lead to unintended consequences, including discrimination or pricing out of certain segments (e.g., education, gender, etc.). Moreover, the use of GenAI models has introduced further complexity to associated risks such as model opacity and lack of explainability, heightening the difficulty in estimating unintended consequences. Strong data governance and management as well as explainable models are therefore crucial when embarking on AI projects.

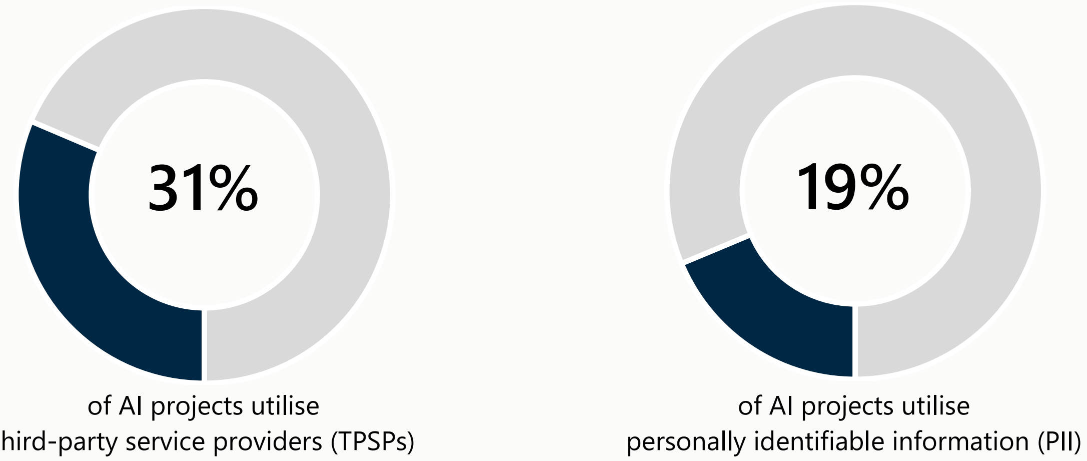
3.6 Greater adoption of AI could lead to a large increase in models adopted across FSPs in increasingly wide applications. A greater reliance on such models to assist or directly manage decision-making activities in the absence of compensating model risk management controls could give rise to a greater risk for model errors or misuse of model outputs beyond their intended purpose. This could lead to adverse consequences that result in financial loss, regulatory non-compliance, or reputational damage.

3.7 The use of internal or public GenAI tools could lead to heightened non-financial risks. This includes heightened third-party risk due to dependencies on a small set of foundation model developers, and legal risk from violations of intellectual property rights (IP) or data privacy laws due to improper development of AI foundation models. Where sensitive information is used in model training or shared across systems without proper classification and access controls, FSPs may face a heightened risk of data leakage. This risk is especially pronounced in GenAI environments, where models may inadvertently retain or reproduce sensitive data. According to the BNM AI Survey 2024, dependency on third-party service providers was the biggest concern for banks and ITOs, followed by concerns related to cloud usage in AI. Nevertheless, *Exhibit 6* highlights that most AI projects in testing or deployment at FSPs do not currently utilise third-party service providers or personally identifiable information.

Exhibit 6

Most AI projects in testing or deployment at FSPs do not utilise third-party service providers or personally identifiable information

Share of AI projects reporting the use of TPSPs or PII data, 2024 (n=74)



Source: BNM AI Survey 2024

3.8 More broadly, convergence by the financial sector on the use of the same foundation models and/ or the same datasets may introduce or amplify interconnections among FSPs[13]. Correlation across model outputs from FSPs could exacerbate procyclicality and herding behaviour, which could contribute to synchronised reactions during periods of volatility. As AI adoption scales, these dynamics may introduce new channels of systemic risk that may have significant implications for financial stability.

3.9 The deployment of AI technologies in the financial sector may inadvertently contribute to climate-related risks, particularly transition risks. AI applications utilising on-premise data centres or energy-intensive IT infrastructure could contribute to higher Scope 2 emissions, while reliance on third-party cloud services or AI vendors may contribute to Scope 3 emissions[14]. Left unaddressed, these emissions could increase FSPs' transition risk exposure.

[13] FSB (2024a).

[14] The Greenhouse Gas Protocol separates emissions into three scopes – Scope 1 covers direct emissions from owned or controlled sources, Scope 2 covers indirect emissions from purchased electricity consumed by the reporting entity, and Scope 3 covers indirect emissions from assets not owned or activities not controlled by the reporting entity along its value chain (upstream and downstream).

AI adoption could introduce new forms of risk…

3.10 The increasing complexity of AI models, particularly those incorporating continuous or reinforcement learning may pose challenges for model generalisability and explainability for predictions in real-world scenarios. Models that are continually retrained with new data may be prone to overfitting and struggle to respond appropriately to unforeseen market events. In addition, such models may behave like "black boxes" which can create significant challenges to effective model validation. A further concern is the risk of data poisoning, where malicious or low-quality data is intentionally or inadvertently introduced during retraining, potentially corrupting model outputs and degrading performance over time. Without adequate technical or human controls, these issues can lead to performance instability over time, reducing the reliability of such models.

3.11 A major risk in the use of GenAI is "hallucinations", where GenAI applications perceive patterns or objects that are non-existent, and create outputs that are nonsensical or altogether inaccurate[15]. For example, where GenAI is used to augment or replace customer service chatbots, hallucinations could lead to incorrect instructions or improper advice being delivered to customers.

3.12 Additionally, external risks arising from the use of AI by malicious actors are likely to affect organisations regardless of whether they deploy AI systems, introducing new sources of cyber risk. For example, GenAI has enabled scammers to increase the sophistication of scam attacks and disinformation campaigns. Email phishing attempts have become increasingly difficult to distinguish as GenAI vastly expands hackers' ability to produce credible phishing emails.

3.13 Malicious actors armed with GenAI tools have also created realistic videos, fake IDs, and false identities to mislead their intended victims. This extends to the creation of hyper-realistic deepfakes of company executives to prompt unlawful money transfers. In some jurisdictions, GenAI tools have been used in mass e-KYC attacks on banking institutions.

3.14 A heightened prevalence of AI-enabled scams may undermine consumer confidence in digital financial services. Potentially, this might cause some consumer segments to withdraw from digital services such as online banking, for fear of falling victim to scams. This would risk the significant progress made in advancing financial inclusion through digitalisation.

3.15 *Exhibit 7* illustrates a clear trend of increasing confidence among FSPs in managing AI-related risks, which appear to correlate with greater levels of testing and deployment. This suggests that initial hesitations by some FSPs may have been driven

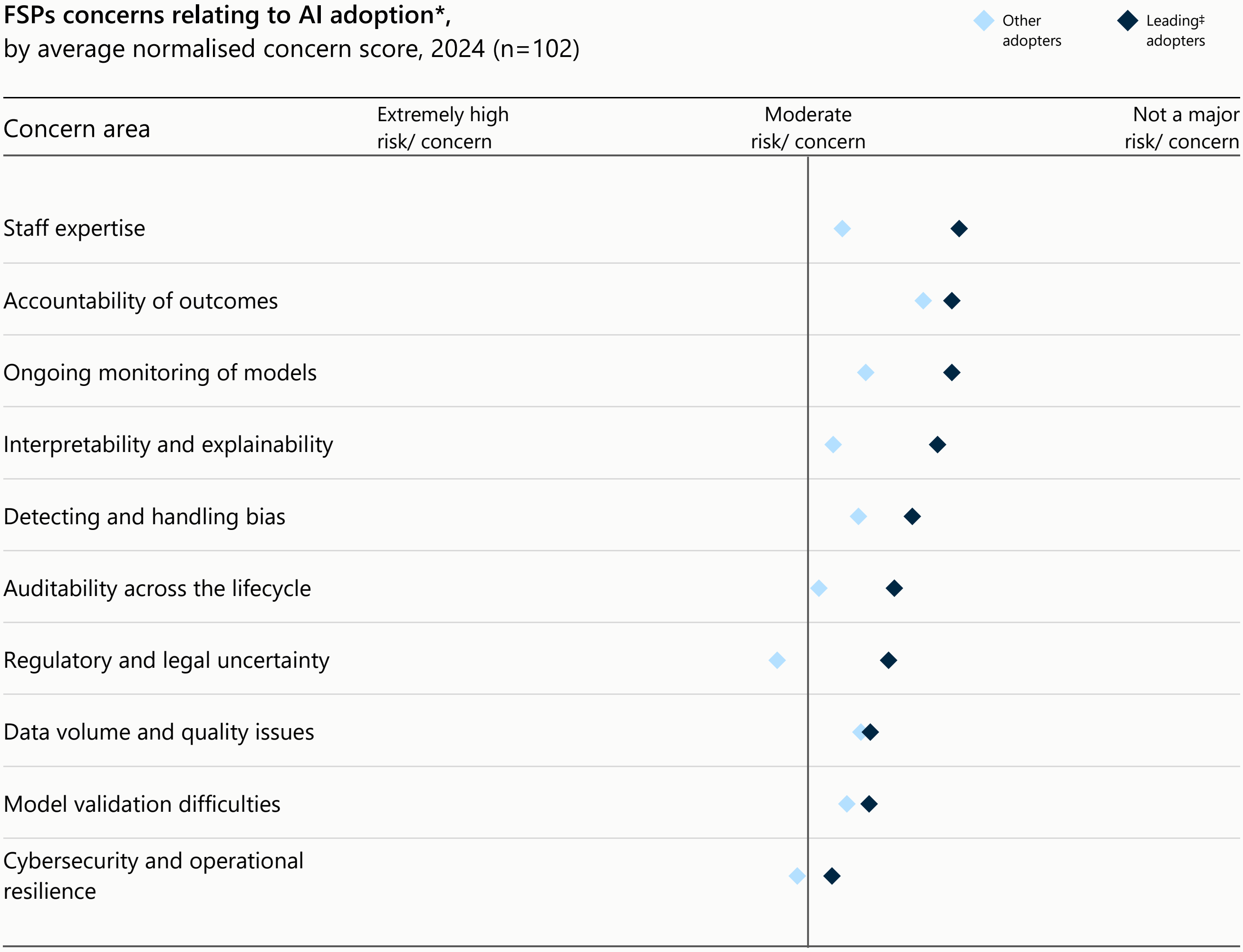
[15] IBM (2023).

largely by limited internal expertise and unfamiliarity with AI technology. These challenges can be progressively addressed through capacity building and as FSPs gain hands-on experience with deploying AI projects.

Exhibit 7

Leading adopters report greater confidence in managing concerns around staff expertise, interpretability and explainability of models, and regulatory and legal uncertainty

FSPs concerns relating to AI adoption*,
by average normalised concern score, 2024 (n=102)



* Referring to banks, DFIs, insurers, and e-money issuers who have reported at least one AI project (i.e., excluding non-adopters). ‡ Leading adopters refer to the top quintile of FSPs by reported AI projects, whereas other adopters refer to other FSPs outside of the top quintile.

Source: BNM AI Survey 2024

For feedback

5. Are there any novel emerging benefits and risks associated with the use of AI in financial services that are not addressed in this discussion paper?
6. Among the benefits and risks outlined in this section, which do you believe warrant greater attention from FSPs and regulators in the next 1-2 years and beyond?
7. What key actions has your organisation taken to mitigate the risks associated with AI deployment?
8. How does your organisation plan to identify and manage AI-related risks to consumers, while ensuring that AI-driven services are delivered efficiently, transparently, and fairly?
9. Looking ahead, how do you expect the benefits and risks of AI adoption in financial services to evolve over time?

Part B: BNM's Approach to Artificial Intelligence Adoption in the Financial Sector

4 Regulatory Approach

4.1 Globally, the regulatory approach for AI at national or regional level varies significantly. Some jurisdictions have enacted regulations and laws[16] whereas others have issued non-binding guidelines to spur responsible and ethical AI development[17]. In Malaysia, the Ministry of Science, Technology and Innovation issued the National Guidelines on AI Governance & Ethics in 2024 which is a national-level voluntary guideline that calls for end users, policymakers, and technology providers to prioritise ethical and responsible use of AI across all sectors[18].

4.2 At the sectoral level, financial regulators in other jurisdictions are evaluating whether AI adoption can be managed through existing regulatory frameworks, or whether a new approach is necessary. Some financial regulators have issued guidance on the use of AI in financial services, typically in the form of high-level principles for responsible use. Additionally, some jurisdictions are looking to implement binding rules for specific financial services activities[19], whereas other jurisdictions prefer to strengthen or expand existing rules to ensure they sufficiently address potential risks[20].

4.3 BNM reiterates our commitment to preserving the principles of parity, proportionality and neutrality in our approach to the oversight of AI-related activities in the financial sector. This means that activities bearing the same types of risks will be regulated the same way ("parity"), while regulatory expectations and supervisory rigour are calibrated to commensurate with the materiality and likelihood of risks ("proportionality") and agnostic to different technologies, systems, and approaches in the achievement of outcomes ("neutrality").

4.4 In the Malaysian financial sector, FSPs are currently subject to technology-agnostic, outcome-focused regulatory requirements that remain applicable where financial services utilise AI technologies. Many of the risks associated with AI are not new to the financial sector. Moreover, most AI applications being explored or deployed in

[16] For example, in the EU and in China – see OECD (2024b).

[17] For example, in the UK, the US, Singapore, Japan, and others – see OECD (2024b).

[18] Ministry of Science, Technology and Innovation (MOSTI) launched the National Artificial Intelligence Governance and Code of Ethics Guidelines (AIGE), in line with the National AI Roadmap (2021 – 2025). In addition, the National AI Office (NAIO) is focusing on 7 deliverables including an AI Technology Action Plan (2026 – 2030). – see MOSTI (2024).

[19] For example, reducing conflict of interest associated with an FSP's use of predictive technologies with interactions with investors and investors' own interest.

[20] Particularly in areas related to model risk management.

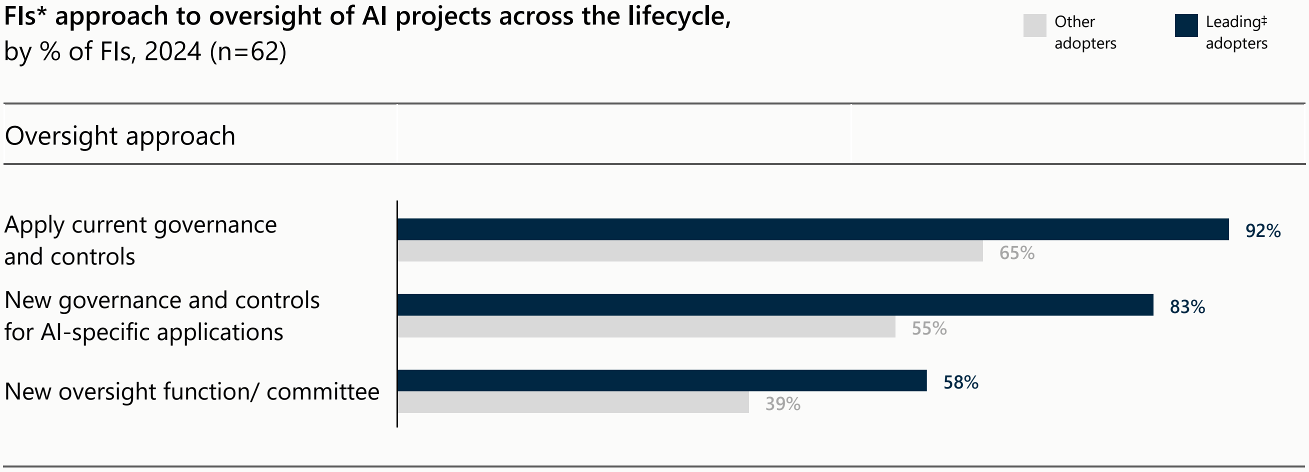
the near future are expected to focus on non-financial risk areas. These applications are also unlikely to fully replace human decision making, particularly for critical tasks or high-stakes decisions. As such, the existing regulatory framework remains broadly adequate in addressing risks posed by AI at this stage.

4.5 As FSPs increasingly integrate AI into their operations, FSPs are expected to develop holistic risk management and oversight practices across the lifecycle of AI models within their institutions. BNM expects FSPs to be able to implement adequate controls on AI deployment that are proportionate to the complexity, potential risks, and intended use of AI models within their institutions. *Exhibit 8* below illustrates how several leading adopters have responded to oversight challenges by establishing dedicated governance structures and oversight functions[21] for AI initiatives.

Exhibit 8

Leading adopters have adopted new governance and controls as well as established new oversight functions for AI projects at a faster pace compared to other adopters

FIs* approach to oversight of AI projects across the lifecycle,
by % of FIs, 2024 (n=62)



* Referring to banks, DFIs, and insurers who have reported at least one AI project (i.e., excluding non-adopters). E-money issuers are not captured in this exhibit. ‡ Leading adopters refer to the top quintile of FSPs by reported AI projects, whereas other adopters refer to other FSPs outside of the top quintile.

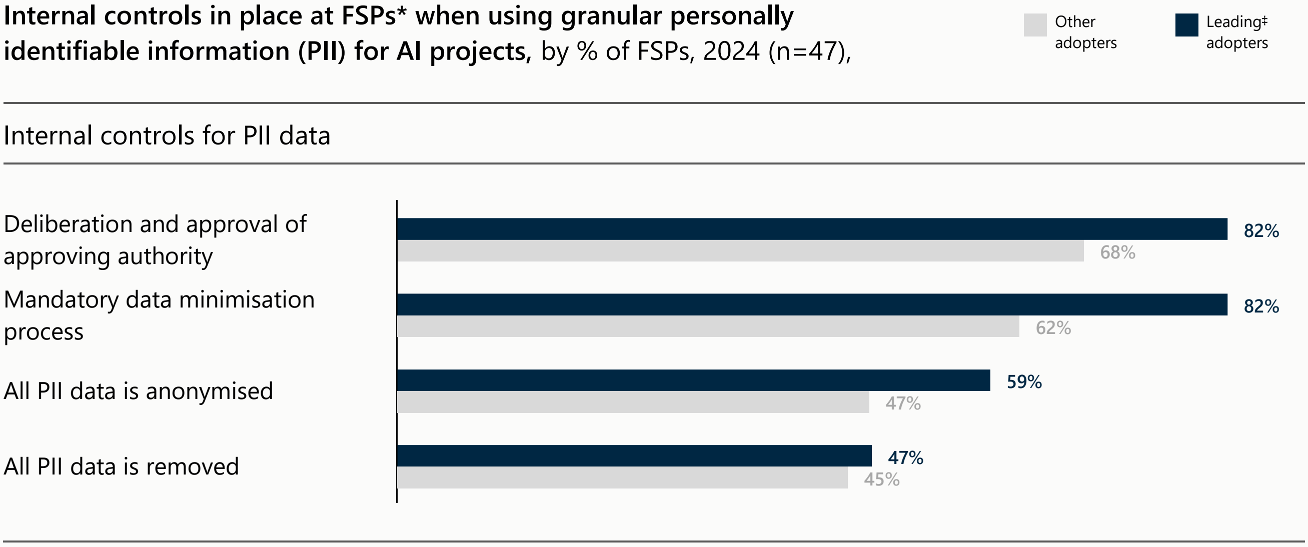
Source: BNM AI Survey 2024

[21] Some FSPs may already have in place dedicated oversight controls or governance functions that address AI-specific applications. In such cases, these institutions have reported that no additional new governance/ controls/ oversight structures were required, as existing oversight mechanisms were deemed sufficient.

4.6 As AI applications increasingly rely on large volumes of data to develop models to generate outputs, FSPs are expected to ensure that the responsible handling of data, especially personally identifiable information (PII) continues to remain a critical area of focus. FSPs are expected to ensure continued compliance with existing and emerging regulatory requirements[22] and adopt ethical data practices. This includes but is not limited to ensuring transparency in data sourcing, obtaining informed consent and implementing sound data management practices. While less than half of AI projects by our FSPs currently utilise PII, many FSPs have implemented internal controls to mitigate risks and minimise undesirable outcomes in projects where PII is involved. *Exhibit 9* illustrates different controls that are being applied by FSPs when managing PII data for AI projects.

Exhibit 9

FSPs have implemented various internal controls to minimise undesirable outcomes for AI projects with PII data



Internal controls in place at FSPs* when using granular personally identifiable information (PII) for AI projects, by % of FSPs, 2024 (n=47),

* Referring to banks, DFIs, insurers, and e-money issuers who have reported at least one AI project involving PII data (i.e., excluding non-adopters or FSPs who did not adopt an AI project involving PII data). ‡ Leading adopters refer to the top quintile of FSPs by reported AI projects involving PII data.

Source: BNM AI Survey 2024

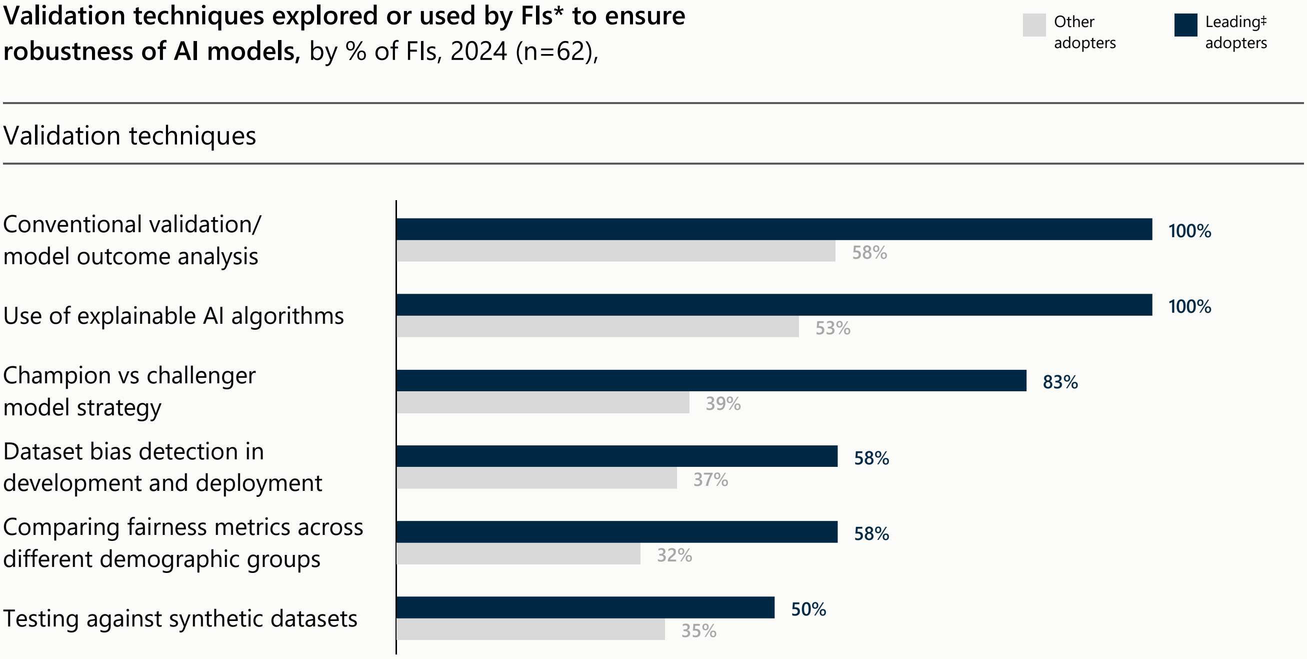
[22] FSPs should also take note of the recent amendment to the Personal Data Protection Act (PDPA) in 2024, as well as corresponding existing and upcoming issuances of guidelines, circulars, and standards pursuant to the amended act by the Personal Data Protection Commission (Persuruhjaya Perlindungan Data Peribadi) where appropriate and relevant to the use of AI in financial services.

4.7 A recent survey conducted by the Chief Risk Officer's Forum (CRO Forum)[23] in November 2024 revealed that out of a sample of 14 banks with AI applications, 11 CROs reported that their banks have in place model risk management frameworks that apply to AI models. Based on the survey, the common components of model risk management frameworks include model definition and scope, governance, data quality requirements, as well as model development, monitoring and implementation. Moreover, model validation, often embedded in development and monitoring phases, has been cited as a particularly critical step in ensuring the reliability and integrity of AI applications. *Exhibit 10* highlights how leading adopters are placing greater emphasis on model validation and are exploring a broader range of validation techniques to support responsible AI deployment.

Exhibit 10

Leading adopters view validation as a key step in AI deployment and have explored various validation techniques

Validation techniques explored or used by FIs* to ensure robustness of AI models, by % of FIs, 2024 (n=62),



* Referring to banks, DFIs, and insurers who have reported at least one AI project (i.e., excluding non-adopters). E-money issuers are not captured in this exhibit. ‡ Leading adopters refer to the top quintile of FSPs by reported AI projects, whereas other adopters refer to other FSPs outside of the top quintile.

Source: BNM AI Survey 2024

[23] Chief Risk Officers' Forum of the Asian Institute of Chartered Bankers.

4.8 The examples and exhibits above highlight emerging best practices that may serve as useful reference points for the broader industry. FSPs are expected to consider laws and regulations relating to personal data protection and IP rights, as well as other best practices set by global standard-setting bodies[24].

4.9 As AI adoption in financial services accelerates, **responsible AI principles** are increasingly recognised as a necessary complement or overlay to existing regulatory and governance frameworks. Principles such as reliability, accountability, transparency, fairness, and ethical use[25] can be embedded into existing institutional processes that govern the design, deployment, and monitoring of AI applications. Such an integration would help guide responsible decision making by FSPs around AI use, complementing existing controls and helping institutions navigate emerging risks in a proportionate manner. In 2024, leading FIs with the majority of AI projects deployed generally reported alignment with common responsible AI principles.

4.10 Building on the growing alignment around responsible AI principles, BNM encourages industry-wide collaboration to further harmonise and localise responsible AI principles applicable to the Malaysian financial sector. In this regard, the CRO Forum took a significant step forward in 2024 by developing the **AI Governance Framework**[26], an industry-led guideline outlining responsible AI principles and best practices for managing AI-related risks. *Exhibit 11* outlines a summary of guiding principles in the framework. This initiative reflects the banking industry's commitment to responsible innovation and marks an important milestone in operationalising responsible AI principles within the context of the Malaysian financial sector. BNM commends this effort and is looking forward to the publication of the AI Governance Framework as a strong foundation for sectoral leadership in responsible AI.

[24] For example, National Institute of Standards and Technology (NIST) AI Management Framework, Basel Committee on Banking Supervision (BCBS)' Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239), and others.

[25] MAS (2018), OECD (2024b).

[26] AICB (forth.).

Exhibit 11

Summary of responsible AI principles under the AI Governance Framework

Fairness	• AI-driven decisions do not discriminate or create harmful bias against any individual or group of individuals. • Differential treatments between different individuals or groups of people should be justifiable. • The use of personal attributes as input factors for AI-driven decisions should be justifiable.
Ethical	• Use of AI complies with all relevant laws and regulations. • Use of AI is aligned to the financial institution's corporate values, ethical standards, and code of conduct.
Accountability	• Board and senior management are accountable for all AI strategies and outcomes. • Use of AI for decision-making is approved by an appropriate, competent internal authority. • Financial institutions are accountable for both internally developed and externally sourced AI applications.
Transparency	• Use of AI is sufficiently disclosed and communicated to those affected where appropriate, commensurate to level of materiality, without revealing proprietary or security-critical information.
Explainability	• There should be sufficient level of explainability over the underlying design and intent of AI applications, commensurate to the level of materiality, without revealing proprietary or security-critical information. • AI systems processes should be well-documented and traceable, with clear and understandable records of decisions, datasets, and processes used to yield the systems' decisions. • When explainability is limited or difficult, it should be supported by valid justifications.
Reliability	• Trained AI models are adequately tested and validated to ensure accuracy, relevance, and robustness in handling errors, invalid inputs, or stressful conditions for deployment and ongoing use.
Security	• Maintain privacy, data protection, and security throughout the data lifecycle, by employing robust data governance and management. • Implement appropriate controls and security measures to ensure the robust security and resilience of AI systems and protect against new threats. • Comply with relevant laws and regulations and implement appropriate controls where possible to protect data.

Source: AI Governance Framework (forthcoming), AICB. Produced by the Chief Risk Officers' Forum and supported with inputs from the Chief Information Security Officers' Forum.

4.11 BNM encourages other segments of the financial sector to build on this foundation through the support of respective industry associations, whether by aligning with AI Governance Framework or developing complementary approaches tailored to their specific contexts. Broader alignment to responsible AI principles across the financial sector will be key to ensuring consistent and effective governance of AI across the financial ecosystem.

4.12 As AI technologies and state of adoption in FSPs continue to grow and evolve, we recognise that AI use may introduce new risks that are not adequately addressed by the existing regulatory framework. BNM remains vigilant to developments in AI and closely monitor its usage across FSPs. In line with the principles of parity, proportionality, and neutrality, an escalation in supervisory focus may be considered if AI-related risks become more material, for example, due to widespread use of AI applications in critical functions or to replace human decision making. Where relevant, we may explore the need to introduce new regulatory expectations should the need arise in the future.

For feedback

10. Do you consider the current technology-neutral regulatory framework to be broadly sufficient in addressing risks associated with AI at this stage of development and adoption? In your view, what key risks associated with AI should be addressed through specific regulation?

11. Are there specific areas where regulatory clarity, flexibility, or guidance would support responsible AI adoption? Please specify area, the applicable regulation, or policy document (if any), together with supporting information and rationale.

12. Are industry-led guidelines useful in complementing regulatory expectations for the responsible and ethical use of AI? Are there any additional principles, safeguards or considerations that should be reflected in future guidance? What role should BNM play in supporting the development, adoption or harmonisation of industry-led standards and guidelines in the future?

13. Has your institution encountered AI-related regulatory requirements or supervisory expectations in other jurisdictions? What lessons or practices could be relevant for the Malaysian context?

5 Development Approach

5.1 Looking ahead, BNM seeks to advance responsible adoption and use of AI across the financial sector, as part of a wider lens of advancing digitalisation as outlined in the Financial Sector Blueprint 2022 – 2026. As the financial sector embraces AI-driven enhancements, we remain committed to fostering a facilitative environment for responsible innovation while ensuring the regulatory approach evolves in step with technological advancements.

5.2 We are of the view that a key step in advancing responsible innovation is prioritisation of "**win-win-win**" use cases – AI applications that deliver value across three dimensions:

i) benefiting consumers,

ii) enhancing business outcomes for FSPs, and

iii) aligning with regulatory objectives for financial stability, development, and inclusion.

5.3 For example, AI-driven fraud detection and AML applications represent a clear win-win-win use case. These applications leverage AI to enhance real-time transactions monitoring, identify suspicious activity with greater accuracy, and lower false positive rates. This benefits both consumers and FSPs by minimising fraud related losses and improving the efficiency of compliance processes. Furthermore, such applications contribute towards strengthening the integrity of and trust in the financial system, aligning with BNM's regulatory objectives.

5.4 Another example of a win-win-win use case is AI-powered personal financial management tools that leverage consumer-permissioned data[27]. These tools use AI to analyse financial behaviours and provide tailored recommendations for budgeting, saving, and debt management. This benefits consumers by improving financial literacy and helping them make better informed decisions, while FSPs gain a deeper customer engagement and the ability to offer more relevant products and services. At the same time, these applications support BNM's regulatory objectives of improving financial inclusion and responsible financial behaviour.

5.5 BNM recognises that existing regulatory frameworks may not fully cater to every AI use case, particularly more innovative or novel ones. In this regard, the BNM Regulatory Sandbox (Sandbox) plays a key role in providing regulatory flexibility by facilitating testing of innovative AI use cases where there are regulatory impediments. The Sandbox enables FSPs to assess the feasibility of AI applications whilst providing BNM insights to form better views on both opportunities and risks associated with

[27] Among others, potentially through the implementation of Open Finance.

these innovations. To date, the Sandbox has supported the testing of innovative use cases and business models, including digital remittance, e-KYC, Buy-Now-Pay-Later, and digital insurance. Moving forward, BNM particularly encourages testing of win-win-win use cases that focus on enhancing risk management, strengthening anti-fraud measures, and improving customer experience.

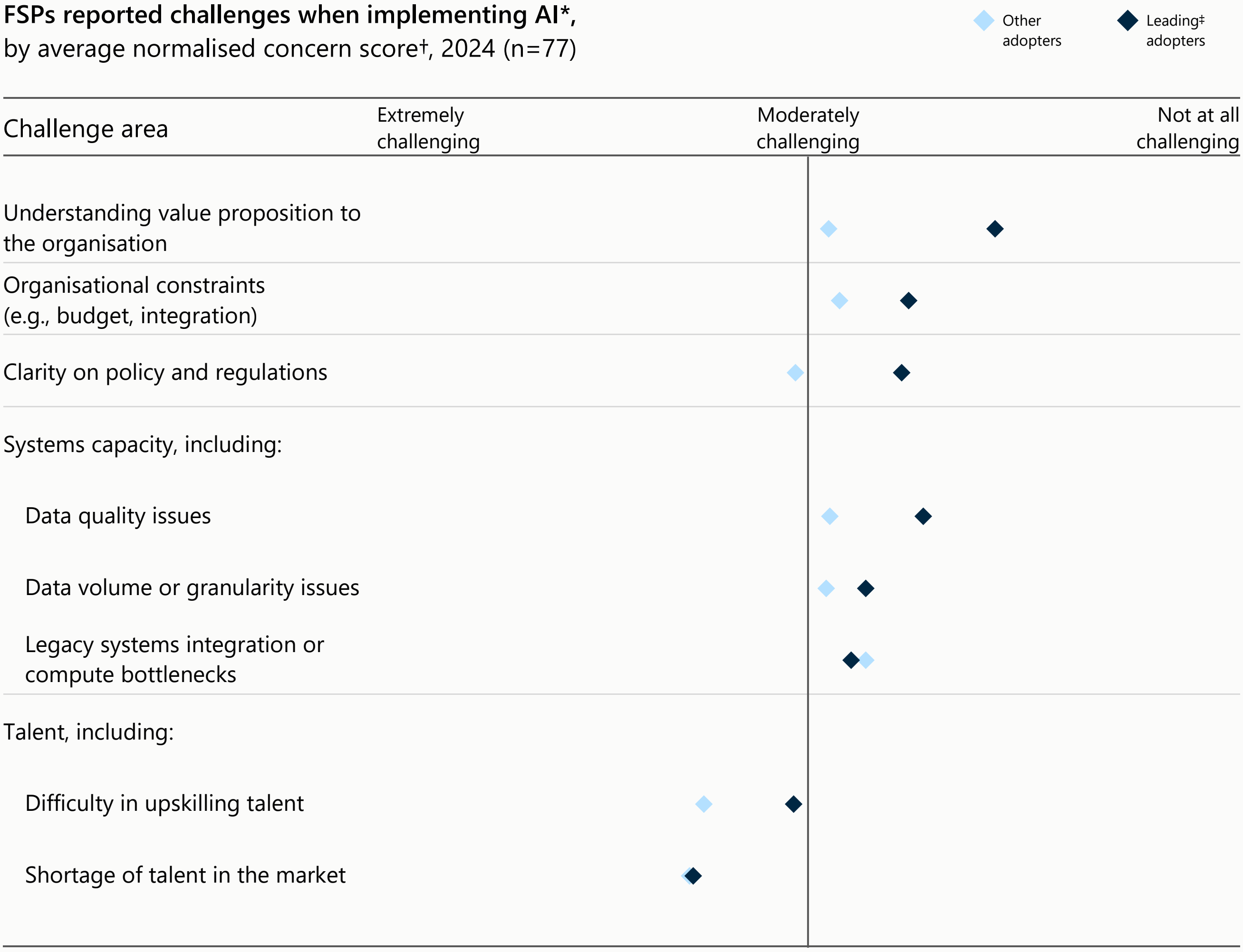
5.6 BNM acknowledges that FSPs face several challenges in adopting AI within their institutions. These include talent shortages, limited data readiness, and difficulties integrating AI with legacy systems. While these challenges are not unique to AI adoption, they can reduce FSPs' capacity to explore AI use cases and may slow the pace of innovation.

5.7 *Exhibit 12* highlights that leading adopters appear better equipped to navigate common implementation challenges compared to other FSPs. This suggests that early and iterative adoption can help institutions build internal capabilities and accelerate talent development. Therefore, FSPs are encouraged to take a proactive approach to responsible AI testing and deployment, supported by appropriate safeguards.

Exhibit 12

Leading FSPs demonstrate greater ability in overcoming AI implementation challenges, though talent shortage remains a shared concern

FSPs reported challenges when implementing AI*,
by average normalised concern score†, 2024 (n=77)



* Referring to banks, DFIs, insurers, and e-money issuers who have reported at least one AI project (i.e., excluding non-adopters). ‡ Leading adopters refer to the top quintile of FSPs by reported AI projects, whereas other adopters refer to other FSPs outside of the top quintile.

Source: BNM AI Survey 2024

5.8 While efforts by FSPs at an organisation-level is essential in overcoming AI implementation challenges, a broader industry-wide collaboration could support more effective and responsible AI adoption across the financial sector. BNM has identified the following key areas that could benefit from industry-wide collaboration:

i) **Developing industry guidelines and best practices for AI risk management and governance**, including the application of responsible AI principles and general principles for effective model risk management. Industry-led guidelines can promote consistency in how FSPs approach AI-related risks, while fostering trust in AI-enabled financial services.

ii) **Facilitating knowledge-sharing on AI implementation and risk management**, including industry-wide discussions and forums to exchange insights on the development and deployment of win-win-win AI use cases, emerging model validation techniques and responsible innovation. A collaborative approach can help FSPs accelerate adoption and leverage collective expertise in managing AI risks.

iii) **Strengthening talent pipelines and AI expertise within the financial sector** through coordinated efforts to attract, train, and retain AI talent within the sector. This may involve partnerships with technology service providers, academic institutions and training bodies. It is important that these efforts address all parts of the talent value chain, from attracting new entrants and upskilling existing staff, to developing leadership capabilities in AI governance.

iv) **Enhancing consumer awareness and understanding of AI in financial services** through targeted education and financial literacy initiatives. These should aim to build public trust by explaining the benefits and responsibilities of interacting with AI-enabled services, while also raising awareness of potential risks such as data privacy concerns and deepfake fraud schemes.

5.9 By bringing together industry players, regulators, and other stakeholders in a structured forum, we believe that collaboration in these areas can accelerate discovery, learning, and alignment on emerging AI deployment and risk management practices. In this regard, BNM is open to facilitating regulatory dialogues as needed to proactively explore how the existing regulatory framework may evolve in response to address AI developments.

5.10 To conclude, BNM encourages FSPs to engage proactively through relevant platforms, including industry associations, to raise and advance discussions on AI in financial services, particularly in the above key areas. Where appropriate, this could include exploring or empowering dedicated working groups comprising FSPs, industry associations, technology providers, and other stakeholders. By leveraging existing structures while remaining open to more targeted collaboration where needed, the financial sector can collectively drive industry-wide progress in laying a strong foundation for responsible innovation.

For feedback

14. What are key opportunities for AI innovation in the financial sector that remain unexplored? What are some win-win-win use cases that your institution has identified and is keen to explore?

15. How can the Sandbox programme be enhanced to better support the development, testing, and deployment of AI innovations in financial services? Are there specific features or support mechanisms that would make the Sandbox more accessible or impactful for AI-related use cases?

16. What challenges or opportunities in AI adoption would benefit most from industry-wide exploration or collaboration? What forms of collaboration (e.g., working groups, joint pilots, etc.) would be most effective in enabling testing and scaling of impactful use cases and resolving key implementation challenges?

17. Would your organisation be interested in participating in BNM-facilitated knowledge exchange sessions with other industry players or stakeholders? If yes, what topics or areas should be included in such discourse?

18. Please suggest the role BNM could play in facilitating and supporting industry-led initiatives that promote knowledge sharing and collaboration on AI-related matters within the financial sector.

References

AICB (forth.) Asian Institute of Chartered Bankers (AICB). (forthcoming). Artificial Inteligence Governance Framework. *Produced by the Chief Risk Officers' Forum with inputs from the Chief Information Security Officers' Forum of AICB.*

BNM (2022) Bank Negara Malaysia (BNM). (Jan 2022). Financial Sector Blueprint 2022-2026.

BNM (2023) Bank Negara Malaysia (BNM). (Mar 2023). Artificial intelligence in the Malaysian financial system: opportunities, risks, and the way forward. *Financial Stability Review 2H 2022 pp. 27-31.*

BNM (2024) Bank Negara Malaysia (BNM). (Jul 2024). Closing remarks by Deputy Governor Adnan Zaylani Ahmad Zahid at the 3rd Malaysian Banking Conference 2024.

BCBS (2013) Basel Committee on Banking Supervision (BCBS). (Jan 2013). Principles for effective risk data aggregation and risk reporting. *BCBS 239.*

BCBS (2022) Basel Committee on Banking Supervision (BCBS). (Mar 2022). Newsletter on artificial intelligence and machine learning.

BCBS (2024) Basel Committee on Banking Supervision (BCBS). (May 2024). Digitalisation of finance.

BIS (2024a) Hernández de Cos, P. (Apr 2024). Managing AI in banking: are we ready to cooperate? *Keynote speech by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the Institute of International Finance Global Outlook Forum, Washington DC, 17 April 2024.*

BIS (2024b) Aldasoro, I., Gambacorta, L., Korinek, A., Shreeti, V., & Stein, M. (Jun 2024). Intelligent financial system: how AI is transforming finance. *BIS Working Papers No. 1194.*

BIS (2024c) Bank of International Settlements (BIS). (Jun 2024). Artificial intelligence and the economy: implications for central banks. *Annual Economic Report 2024 Chapter 3.*

BIS (2024d) Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (Dec 2024). Regulating AI in the financial sector: recent developments and main challenges. *FSI Insights on policy implementation No. 63.*

BIS (2024e) Lee, V. W. S., & Sarip Abidinsa, S. A. B. (Nov 2024) Machine learning for anomaly detection in money services business outlets using data by geolocation. *IFC Working Papers No. 23.*

BoE (2022a) Bank of England (BoE). (Oct 2022). Machine learning in UK financial services.

BoE (2022b) Bank of England (BoE). (Oct 2022). Discussion paper on artificial intelligence and machine learning. *DP 5/22.*

BoE (2023a) Bank of England (BoE). (May 2023). Model risk management principles for banks. *PS 6/23.*

BoE (2023b) Bank of England (BoE). (May 2023). Model risk management principles for banks. *SS 1/23.*

BoE (2023c) Bank of England (BoE). (Oct 2023). Feedback statement on artificial intelligence and machine learning. *FS 2/23.*

BoE (2024) Bank of England (BoE). (May 2024). Monsters in the deep? – speech by Jonathan Hall. *Given at University of Exeter Business School.*

BoE (2025) Bank of England (BoE). (May 2025). Artificial intelligence consortium.

DOSM (2025) Department of Statistics Malaysia. (Apr 2025). ICT use and access by individuals and households survey report 2024.

EU (2021) European Union Commission. (Apr 2021). Impact assessment of the regulation on artificial intelligence.

EU (2023) European Union Parliament. (Jun 2023). EU AI Act: first regulation on artificial intelligence.

FRB (2011) Board of Governors of the Federal Reserve System. (Apr 2011). Guidance on model risk management. *SR 11-7.*

FRBNY (2025) Federal Reserve Board of New York. (Apr 2025). Speech by Governor Michael S. Barr on Deepfakes and the AI Arms Race in Bank Cybersecurity.

FSAJ (2021) Financial Services Agency of Japan (FSA). (Nov 2021). Principles for model risk management.

FSB (2024a) Financial Stability Board (FSB). (Jun 2024). Remarks on artificial intelligence in finance. *Remarks by Nellie Liang, US Under Secretary for Domestic Finance and Chair of the FSB Standing Committee on Assessment of Vulnerabilities at the OECD-FSB Roundtable on Artificial Intelligence in Finance, May 2024.*

FSB (2024b) Financial Stability Board (FSB). (Nov 2024). The financial stability implications of artificial intelligence.

HKMA (2019) Hong Kong Monetary Authority (HKMA). High-level principles on artificial intelligence.

IAIS (2023) International Association of Insurance Supervisors (IAIS). (Dec 2023). Regulation and supervision of artificial intelligence and machine learning (AI/ML) in insurance: a thematic review.

IAIS (2024) International Association of Insurance Supervisors (IAIS). (Nov 2024). Draft application paper on the supervision of artificial intelligence.

IBM (2023) IBM. (Sep 2023). What are AI hallucinations?

IMF (2023) International Monetary Fund. (Aug 2023). Generative Artificial Intelligence in Finance: Risk Considerations. *Fintech Notes 2023/006.*

KRI (2025) Khazanah Research Institute. (Jan 2025). AI Governance in Malaysia: Risks, Challenges, and Pathways Forward.

MAS (2018) Monetary Authority of Singapore. (Nov 2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector.

McKinsey (2024) McKinsey. Executive's guide to developing AI at scale.

MOSTI (2024) Government of Malaysia. (Sep 2024). The national guidelines on AI governance & ethics. *Ministry of Science, Technology, and Innovation.*

NIST (2023) National Institute of Standards and Technology (NIST). (Jan 2023). AI risk management framework.

NVIDIA (2024) NVIDIA. (2024). Generative AI for customer service and support.

NVIDIA (2025) NVIDIA. (2025). State of AI in financial services. *Survey report*.

OECD (2023) OECD. (Dec 2023). Generative AI in finance. *OECD Artificial Intelligence Papers No. 9.*

OECD (2024a) OECD. (Mar 2024). Explanatory memorandum on the updated definition of an AI system. *OECD Artificial Intelligence Papers No. 8.*

OECD (2024b) OECD. (Sep 2024). Regulatory approaches to artificial intelligence in finance. *OECD Artificial Intelligence Papers No. 24.*

OSFI (2024) Office of the Superintendent of Financial Institutions (OSFI). Draft guideline E-23 – model risk management.

Acknowledgements

By Ian Lee, Atiqah Zaki, Joshua Chin, Ong See Qi, and Ong Jing Yee
Financial Development and Innovation Department | August 2025 | aipolicy@bnm.gov.my