BNM Discussion Questions	GAIAM 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?	We support a formal sector-specific regulatory definition, mainly for these reasons: • From what we gather, the local development efforts of FSPs focus on the downstream tech stack (e.g. application and operation layers of AI) rather than building the LLM internally itself. There is a tendency to integrate with established AI systems (either open source or closed source) or engage external third-party service providers (TPSP) for AI-as-a-Service. • The practice of "AI washing" is increasing, where the AI label is liberally stated or exaggerated on a financial product or service even though it may just feature basic rule-base logic / machine-learning (ML) with narrow purposes. This could be misleading to consumers who expect credible reasoning from AI. A contextual definition could help sharpen the regulatory perimeter or scope. For example: • It can refer to an "AI system" that is *"developed or deployed or distributed by a financial institution in the Malaysia market, whether directly or indirectly in the course of its commercial activity, in return for payment or free of charge"*.[2] • A financial product or service *"which purports to be an AI system or is marketed as an AI system shall be captured by these regulations"*.
2. How frequently should BNM engage with FSPs on AI-related matters, and through which channels, e.g., surveys or consultations?	As generative AI is developing rapidly during this critical formative stage, we recommend that BNM conduct regular pulse checks through surveys and stakeholder consultations.

[2] The definition of "AI system" proposed by OECD (2024) and adopted by BIS (2025) is broad enough for this purpose: *"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."* Source: Bank of International Settlements, Governance of AI Adoption in Central Banks, 29 January 2025.

	This enables timely assessment of emerging trends, risks, and opportunities, to ensure that regulatory approaches remain effective and relevant.
3. What parameters or indicators should BNM consider in future engagements with FSPs to better assess AI adoption, maturity, and impact across the sector?	No direct feedback as we are not an FSP.
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.	As AI rapidly advances, Malaysians may increasingly rely on unregistered AI-driven investment advisors to compare rates or optimize their portfolios, presenting a significant opportunity for financial service providers (FSP). AI-based tools can manage wealth holistically, i.e. allocation and rebalancing of all asset types including banking and insurance, not just capital market products. The AI usage may not be a direct customer interaction of giving advice, but is used indirectly for financial decision making on request by: • Analysing current business sentiment and emerging trends by processing or synthesizing various sources of information; • Analysing historical financial information to make predictions about future market trends and economic conditions; • Analysing past and current behaviour on repayment of loans to produce a rating on creditworthiness or bankability. Regulators (in conjunction with the Securities Commission) should closely monitor this development to ensure investor protection and market stability. Although premature intervention may be seen as stifling innovation, robo-advisory is not new and has significant overlap with Digital Investment Management regime, which is already being regulated.
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?	**<u>Multimodal Risk in Enterprise AI Deployment</u>** In practice, most banks will be more inclined to rely on models sourced from major technology providers such as OpenAI, Microsoft, Google, or Anthropic — instead

	of building AI systems from scratch. Even though using third parties is cited as "the biggest concern for banks and ITOs" (page 18 per BNM AI Survey 2024), it is still the most pragmatic route from a cost and tech-maintenance perspective. When banks adapt these pre-trained models for their own purpose with internal tooling and custom functionalities, they introduce new layers of risk, thereby necessitating fresh rounds of risk assessment. The operational processes become intricate and escalate rapidly: • Risk evaluations may be needed at multiple stages, and it remains unclear exactly when (before, after, throughout each modification) these assessments should occur and what the risk materiality thresholds are respectively. Even so, proactive protocols must already be established to address issues before they escalate into critical problems. • Deciding who is responsible for conducting these checks and tests (in lean IT departments), making go/no-go decisions, and at which points in the AI development lifecycle, would be a significant challenge. This is further complicated by the need to strike a balance with other priorities such as operational efficiency. • 'Human-in-the-loop' interventions may not be able to cope with the speed of AI model interactions, which means real-time monitoring measures must buckle up. All this requires manpower resources and upskilling of frontliners which banks may not be prepared for. • There are limits to the conventional MRM (Model Risk Management) approach for AI systems, especially multimodal ones, due in part to foundation model opacity and difficulty in baseline setting, though this might improve with the bank's experience curve over time. • As part of effective organisational governance, there must be independent validation and code audits by those with the requisite skills and incentives to objectively review AI applications in the bank. There has to be adequate investment to train the

	validation staff with technical expertise on the specific AI area, and inventorization of AI skillsets across the whole bank. For example, a bank may create a solution that combines the LLM with simple generative and agentic tools (e.g. chat with customers to discover needs, score to approve or reject application, onboarding with ID verification), which connects to internal databases (e.g. interest rates and promotion criteria) as well as the internet. This solution is 'multimodal' with numerous points of interaction and risk exposure — which amplifies in complexity and vulnerability with every tool and database added to it, each requiring risk assessment. Banks must take a candid look at their current position on the operational stress continuum, as well as cost-benefit analyses and governance mechanisms, to ensure that their should-be capabilities match their as-is needs before planning for market deployment. Even though data concerns can largely be allayed (as customer PII are filtered or redacted, per para 4.6), the Risk Management Committees (RMC) of banks may still stay cautious or averse to the 'long tail' of incalculable cross-functional 'multimodal risk' which is currently not well-understood or dimensioned. All mitigation measures, including OPSEC, BCP, and DRP (beyond just IT), must be aligned to ingest this risk.
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?	**[Exhibit 7] Staff Expertise and Accountability of Outcomes** There is a flip side to AI usage among staff of financial institutions which may warrant supervision or control. As more banks encourage their staff to maximize productivity with AI, it can lead to the proliferation of unauthorized or unmonitored AI into the bank that bypass governance protocols. This will increase the risk of data leakage or non-compliant behavior. The trend of staff using external AI software or hardware (that is not approved and supported by the bank's IT department) is growing and is a shadow threat

	"hiding in plain sight".[3] A third of successful cyber-attacks are based on this, while more than two thirds (77%) of IT professionals identify this as a major issue soon. For example, banks often unknowingly let AI tools to "sneak" into their operations by their own staff or departments when: • A relationship manager uses ChatGPT (or other LLM) to draft investment summaries or correspond with clients (via email). This could lead to breach of data privacy and inaccurate financial advice. • The reporting department uses AI to summarize lengthy regulatory filings and legal documents. This may cause company secrets and confidential disclosures to be exposed to third-party servers. • AI-driven features are added or embedded to existing financial models via vendor updates, which are not validated or reviewed in the bank's model inventory. The exposure is worse if staff bring work home and use their free personal AI accounts. According to reports, corporate data going into GenAI apps jumped 30X in a year with half of workers surveyed admitted to putting sensitive data into chatbots.[4] While many FIs have disabled USB ports and limited online usage to intranets among staff, the profusion of AI presents a new challenge. Even though it can be argued that the info uploaded to the AI model is 'data at rest' and not compromised, it could potentially be obtained (e.g. with 'prompt leaking') or shared across other tenants (of the same AI service provider). Also, it could be considered an audit failure as the bank has no record of the AI's use, making it invisible to auditors and regulators. It'd be

[3] Forvis Mazars, "Shadow IT: The Cyber Threat Hiding in Plain Sight", April 2025.

[4] Axios, "Workers Spill Company Secrets with Chatbots", July 31, 2025: "Nearly half (47.42%) of sensitive uploads to Perplexity were from users with standard (non-enterprise) accounts. About a quarter of the prompts with sensitive information came through the free version of ChatGPT, and another 15% of sensitive prompts were submitted via free versions of Google Gemini accounts. Overall, including free and paid tiers, ChatGPT was by far the biggest source of prompt-based information exposure, followed by Microsoft Copilot and Google Gemini."

	another failure if the bank does not keep a complete inventory of AI tools in the organization, including the unauthorized ones used by staff. Note: A real-life incident was relayed to us by someone in a large public listed company. One HR staff uploaded sensitive payroll information to the AI system to generate a benchmarking report. Although the report is redacted without PII, the payroll must be entirely removed from servers (if possible), so the AI won't generate it as a prompt output when a curious user asks!
7. What key actions has your organisation taken to mitigate the risks associated with AI deployment?	No direct feedback as we are an industry association that promotes and advocates GenAI (i.e. not a first-hand implementer).
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?	As above. While we are pleased to witness significant advancements of GenAI in the finance sector, the rapid pace of its development and the full scope of 'experienced' and 'emerging' risks remain unobserved, unreported, and unpredictable. Our priority is to engage industry members and deepen our understanding to better navigate this evolving landscape. We're continuously learning too! We propose a two-step approach to managing AI-related risks for consumers: • Informed Consent: First, they should be clearly informed that AI-driven services remain at an experimental stage, which requires full awareness and acknowledgement of its risks. • Risk Profiling: Second, given the potential risks inherent in these AI-driven services, they should be classified as high-risk investments when associated with AI optimization. This aligns with the need for transparency and consumer protection as emphasized in BNM's recent AI regulatory framework discussions, which call for fairness, accountability, and heightened user awareness in AI adoption within financial services.

9. Looking ahead, how do you expect the benefits and risks of AI adoption in financial services to evolve over time?	**For Consumers** Ultimately this depends on how each FSP utilizes AI and adapts to market conditions, and whether it offers more benefits than risks. One member mentioned parallels with the regulatory approach taken for Full Self Driving (FSD) technology. If regulators do not permit fully automated AI deployment in financial services, the risks remain minimal since AI would only be used to assist and advise, with ultimate decisions retained by humans. However, if full automated AI deployment is allowed, then regulatory preparedness becomes crucial to ensure accountability and responsibility. In other words, it is essentially a yes-or-no response, contingent on how risks associated with AI are managed, acknowledging that increased automation may necessitate more specific regulatory oversight. **For Financial Service Providers** One member cautioned that FSP concerns on "cybersecurity and operational concerns" seem to be downplayed to the least risk, relatively (Exhibit 7). FSPs will tend to deploy pre-trained models and rely on third-party APIs to save on development time. But this could backfire on the FSP if there is no adequate security assessment on the API attack surface. For instance, how can it detect and prevent unauthorized API calls via 'prompt injection' attacks, or 'model extraction' efforts that leverage weaknesses in API rate limiting and authentication protocols? How can it ensure that the permissions set for the AI model will not spread risks on other systems via API connections? In other words, the risk mitigation plan of the FSP has to evolve with AI risks first to protect the FSP's own safety, before it thinks of launching AI benefits to users.
10. Do you consider the current technology-neutral regulatory framework to be	We propose that BNM consider adopting a risk-based regulatory framework for AI, similar to the European

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?	Union's AI Act. The EU approach categorises AI systems into risk levels, with each category carrying different regulatory obligations. This ensures proportionate safeguards without stifling innovation. How it works in the EU (for reference):[5] • Unacceptable Risk AI – AI systems that present clear threats to safety, rights, or against public policy (e.g. social scoring, manipulative subliminal techniques) are outright prohibited. • High-Risk AI – AI systems with significant impact on health, safety, or fundamental rights (e.g. credit scoring, recruitment, biometric identification) are allowed but subject to strict compliance obligations (risk assessments, documentation, data quality, transparency, auditability). • Limited Risk AI – Systems with moderate risks (e.g. chatbots, emotion recognition) require transparency obligations, such as informing users they are interacting with AI. • Minimal/No Risk AI – Everyday AI with negligible risk faces no regulatory burden, but voluntary codes of conduct may apply. Why this is useful for Malaysia: • Provides clarity and proportionality: higher-risk applications are more tightly controlled, while lower-risk ones are not overburdened. • Aligns with international best practices, facilitating cross-border consistency and trust in Malaysia's financial sector. • Enhances consumer protection without unnecessarily constraining beneficial AI adoption by financial service providers. We recommend BNM explore this tiered risk framework as a foundation for future AI regulation in Malaysia's financial sector, ensuring that requirements are calibrated to the actual risks posed by AI systems.

[5] The EU Artificial Intelligence Act at https://artificialintelligenceact.eu/.

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.	**<u>Explainability May Create Counterproductive Risks</u>** Addressing the issue of explainability is not straightforward in multimodal AI which entails both deterministic outputs and probabilistic guesses at each step of the way to arrive at a decision. The bank might end up inviting more questions or disclosing more than it should — and expose itself to security hacks, model theft, etc! Some outputs are not "explainable" (and a small degree of inconsistency in output is to be expected). The public may have to accept some trade-offs between performance and explainability i.e., not full but partial explainability. An alternative way to redress explainability is to have an 'error reporting and handling' mechanism to recognise errors, fine-tune the model, and benchmark against the level of inconsistency or inaccuracy.[6] Note: We are also following the international regulatory development on this.[7] **<u>Convergence of AI and Open Banking Initiatives</u>** We believe that AI access to personal data should be restricted exclusively to certified AI models that utilize locally hosted LLMs. We strongly object to the use of cloud-based LLMs for accessing personal data due to concerns over data privacy, control, and security. Nonetheless, we are mindful that enforcement is not so simple as there are various points of failure and vulnerability which FSPs have no control of. Note: This stance aligns with the emphasis in BNM's AI regulatory framework on responsible data governance, safeguarding consumer privacy, and minimizing risks associated with outsourcing sensitive data processing to external cloud providers. Our specific attention is on open banking and how AI will be applied by fintech startups on PII data, if these

[6] Hugging Face, The Big Benchmarks Collection and Open LLM Best Models, (updated) November 2024.
[7] Bank of International Settlements, FSI Insights on policy implementation No 63: Regulating AI in the financial sector: recent developments and main challenges, December 2024.

	data will be recycled for other purposes (e.g. to train LLMs), whether there are regulatory limits on consent and collection on PII, whether they are subject to the same AI rules as FSP etc. ("same risk, same activity, same rules")? This includes credit reporting agencies (CRA) that do not come under the direct regulatory purview of BNM.
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?	We have been following, as an association, the development of ISO/IEC 42001:2023.[8] This is an international, certifiable standard for establishing, implementing, maintaining, and continually improving Artificial Intelligence Management System (AIMS). It helps ensure the responsible, ethical, and transparent development and use of AI by organisations — by addressing trust, fairness, data protection, accountability, and compliance with regulations. While there are other existing frameworks or guidelines, ISO/IEC 42001 is the only one that is certifiable (the world's first) and is applicable to all types of organisations providing or utilising AI-based products or services, regardless of industry.
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?	Not applicable (for us as a Malaysian association).
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?	From what we observe, the key opportunities (based on the current level of competencies in the local market) include: • AI infrastructure development (e.g. on premises, in the cloud, or SaaS) and services (e.g. infra provisioning, workload management, resource monitoring, orchestration and job scheduling). • AI software, including e.g. ML/DL (machine learning or deep learning) frameworks and 'fine-tuning' AI models specifically for finance applications.

[8] International Standards Organisation, ISO/IEC 42001:2023 (Information technology — Artificial intelligence — Management system), 2023.

	• GenAI-assisted financial advisory services utilising pre-trained or custom models, along with automated workflows (e.g. data processing, training programmes, optimisation, deployment) that are integrated into the enterprise system. We believe individuals, companies and government agencies will all use GenAI soon. GenAI functionalities will be embedded in applications such as mobile phones, laptops and cars. • Business opportunities will emerge in how to build and maintain AI infrastructure and software, how to integrate AI pretrained models into various systems, and how to train AI models. • The biggest hindrance to seize these opportunities is not the lack of technology or resources, but (a) nurturing a sufficient AI-skilled talent pool and (b) maintaining a sufficiently diverse AI talent inventory in Malaysia, which will need to be comprehensively addressed by the government and private sector, along with associations like ours.[9]
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?	The Sandbox programme can be enhanced to better support the development, testing, and deployment of AI innovations in financial services. Given AI's heavy reliance on LLM and training datasets, the Sandbox should ensure that data remains locally retained and that only certified LLM models are used. Exposure to unknown or compromised LLM models risks personal data leaks and breaches of decision-making process confidentiality. Therefore, maintaining strict controls on model provenance and data locality within the Sandbox is essential to safeguard consumer privacy and maintain trust.
16. What challenges or opportunities in AI adoption would benefit most from industry wide exploration or collaboration?	Given the data repository that BNM has, there could be public-private collaboration on building 'synthetic datasets' with CCRIS for credit modelling and alternative scoring. As for the banking industry, it can aggregate profiles and transaction patterns of mule accounts for

[9] Luca Spinelli, Building Trustworthy AI In Malaysian Banking: Overcoming Data, Compliance and Talent Challenges, Business Today, 4 April 2025. According to an IDC survey, 41% respondents state there are not enough AI talent. The Asian Institute of Chartered Bankers also says Malaysia urgently needs structured upskilling.

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?	predictive and discriminative modeling (to identify which accounts are at risk). These datasets can be enriched or overlaid with data harvested from telcos and payment networks, to identify criminal behavior, location and concentration.
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?	Yes. As an association, we provide educational resources to the public e.g. introducing AI concepts related to business finance. These are posted regularly on our LinkedIn page.[10] We also host meetups for members.
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.	The tech philosophy 'Ubuntu' is quite relevant for the industry with the advent of AI – we become more authentic as human beings, *if and only if*, we work together. Hence the saying, "to go fast, go alone; to go far, go together" for long-term sustainable progress of the local industry with regulator support. At the same time, there is still a limited understanding among Malaysians about the current state and rapid pace of Gen AI development. Bad actors are typically early adopters of technology; and AI financial crime will flourish and try to outpace compliance and surveillance practices. In our humble opinion, AI innovation can't be easily stopped or slowed by regulation (nor should it be), as it has become too pervasive. However, the industry's 'responsible innovation' and regulator's role can be guided by the 'common good' and 'do no harm' approach: • Open knowledge sharing among Fis without reprisal, particularly on security failure and fraud attempts, with sitrep and spotrep to BNM and industry working groups during critical events. • Standards are aligned and prescribed for the industry (not just based on broad ethical principles). This is to build a trust and credibility seal with the

[10] https://my.linkedin.com/company/the-gaiam

	public, which could act as a moat against bad actors. • Education has to be the first line of enforcement (as AI scammers are hard to find and prosecute). Also, due to wide disparity in the digital literacy of the public, some AI products may have to be restricted to 'sophisticated' users (just like the handling of securities). • Regulators should pace this – either to 'go slower' or 'go faster' (rather than go/no-go). The AI sector boom is also met with justifications to decel, as it may lead to 'financial exclusion' (due to the digital divide mentioned above) rather than inclusion.