OPERATIONAL RISK

Financial institutions remained operationally resilient despite challenges

Financial institutions continue to be operationally resilient, with no major system-wide disruptions in the second half of 2022. Operational risk losses remained small relative to the banking sector's capital and profits (0.04% and 0.4%, respectively). However, a rise in the number of payment-related fraud incidents, both globally and domestically, highlighted growing concern with cybercrimes, with more frequent attacks being observed and higher costs for affected parties as well as the wider economy. In Malaysia, 19,165 cases of online banking fraud involving RM94.6 million were reported by customers of financial institutions in the second half of 2022, up from the 9,735 cases totalling RM39.9 million reported in the first half of the year.

Efforts to combat cybercrime require a comprehensive and coordinated approach between regulators, law enforcement agencies, and the private sector. Internationally, the Financial Action Task Force (FATF)[37] acknowledges this need and has embarked on new initiatives focusing on cyber-enabled fraud and ransomware. These include publication of reports on latest trends and methods as well as recommendations to effectively curb ransomware activities. In addition, several financial regulators have issued supervisory guidance to financial institutions to strengthen controls against online banking fraud, while governments have led national anti-fraud campaigns to enhance consumer awareness.[38] In Malaysia and several other countries, national anti-scam centres have been established, in an effort to centralise rapid and effective responses to online scams.

The Bank and the financial industry have continued to intensify ongoing efforts to educate the public on cyber hygiene measures that play a critical role in preventing fraud. In addition, the Bank has required all banking institutions to further tighten fraud countermeasures against the increasingly sophisticated and continuously evolving nature of financial scams, which prey on social behaviours that increase vulnerabilities to fraud.[39] These measures include a requirement for banks to expedite the migration from short messaging service (SMS) one time password (OTP) to more secure forms of authentication for online activities or transactions by June 2023. Banks are also required to implement other safeguards, which include:

- removing all clickable hyperlinks in SMS and email communications;
- restricting customers to one mobile device for the authentication of online banking transactions;
- strengthening processes for enrolling new mobile devices and changing "trusted devices";
- tightening fraud detection rules and triggers for blocking suspicious transactions; and
- enhancing the cyber hygiene of customer devices used for online banking or payments services.

As of December 2022, all major banking groups have offered alternative authentication methods, and are progressively migrating all their customers to more secure methods. Banks also continue to refine and improve other security measures. These include stepping-up verification processes for mobile device enrolment, conducting call-back verifications, continuously fine-tuning fraud detection rules to block suspicious transactions, and conducting ongoing brand monitoring to detect and take down fake websites in collaboration with the Malaysian Communications and Multimedia Commission (MCMC). In addition, banks with elevated numbers of fraud cases have each appointed a Senior Independent Director to oversee the handling of fraud and data breach incidents, and coordinate with the National Scam Response Centre (NSRC) for faster tracing and interception of stolen funds. In November 2022, the financial industry also established a task force to develop strategies and to coordinate the timely implementation of industry-wide actions to combat financial fraud. These also include continuous efforts to raise public awareness of scam tactics, and to familiarise online banking users with the security features and controls that have been implemented.

[37] FATF is the global money laundering and terrorist financing watchdog. This inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

[38] For example, the United Kingdom's "Take Five to Stop Fraud" and the Australian government's "Stay Smart Online" campaigns.

[39] Countermeasures taken to combat the increase in online banking related frauds are listed in the BNM Financial Stability Review for First Half 2022.

Investigating Scam Incidents

The process of tracing, intercepting and potential recovery of stolen funds is complex and typically involves a considerable amount of time and resources, requiring coordination between various agencies, financial institutions and telecommunications companies. Critically, victims must inform their financial institutions or the NSRC immediately upon identifying unauthorised transactions, or after realising that they have been scammed. Using this information, financial institutions will temporarily block the affected accounts and begin tracing the movements of the funds. Law enforcement agencies would then initiate investigation, issue the necessary enforcement orders, and ultimately pursue the criminals behind the syndicates. While these steps appear straightforward, instantaneous fund movements into multiple accounts in different banks followed by immediate cash withdrawals pose significant challenges to the investigation. The sheer volume of transactions involved also complicates the task of distinguishing fraudulent transactions from genuine ones as a result of comingling of funds.

While operational losses from financial scams do not currently pose a risk to overall financial stability, their rising trend, left unabated, can affect public confidence in banks and payment infrastructure in more significant and uncertain ways. This calls for a nation-wide, coordinated response to educate the public, maintain strong preventive controls and bring criminals to justice.

Financial institutions continue to make substantial progress in strengthening overall technology risk management capability. In 2022, over 90% of financial institutions achieved substantial compliance with the Risk Management in Technology (RMiT) standards issued by the Bank, up from the 35% in 2020. Amidst the continued digitalisation of financial services, financial institutions continued to prioritise the management of technology risks and invest heavily in upgrading their information technology (IT) infrastructure. These upgrades have served to enhance system performance and service availability, improve resilience against operational disruptions, and mitigate risks of technology obsolescence. Supervisory reviews also revealed more focused oversight by boards and senior management teams on ensuring their IT systems, as well as the resources to maintain them, are able to cope with current and future anticipated needs. These supervisory engagements will also be used to expedite the closure of identified gaps in relation to good technology risk management and cyber security practices.

An ongoing priority for the Bank has been the management of risks associated with third-party service providers (TPSPs). While some progress has been made in mitigating operational disruptions from third-party system outages and data leakages, there remains a need to enhance visibility on sub-contractors hired by TPSPs, i.e., fourth-party service providers (4PSPs), especially given the concentration and contagion risks posed by some 4PSPs. An emerging area of risk relates to a growing reliance on and concentration in cloud service providers. To ensure financial institutions are carefully evaluating and managing such risks in their cloud strategies, the Bank will publish supplementary guidance to the RMiT policy document in 1H 2023 which will outline key expectations on cloud risk management for financial institutions. The Bank will also consult with the industry in 2H 2023 to establish common scenarios for an industry-wide joint business continuity plan (BCP) with critical IT TPSPs. Further measures are underway to conduct joint crisis simulation exercises (CSE) involving the Bank and selected industry players aimed at testing and further strengthening financial institutions' existing recovery and response plans in mitigating widespread operational disruptions. Collectively, these efforts are expected to improve visibility over the interconnectedness of service providers with the view to strengthen supply-chain risk management capabilities in the financial sector.

While operational disruptions relating to system outages and data leakages resulting from third-party failures have remained low so far, a growing trend of cyber breaches calls for continued vigilance. Major threats identified by the financial industry include breaches occurring in the environment of service providers, as well as increasingly sophisticated cybercrime campaigns such as malware-as-a-service and targeted phishing campaigns. These incidents further underscore the need to intensify the sharing of timely cyber threat intelligence. In this regard, seven new financial institutions were onboarded

to the Financial Sector Cyber Threat Intelligence Platform (FinTIP)[40] in the second half of 2022, bringing the number of entities participating in the network to 40. FinTIP continues to support efforts by the industry to further strengthen its cyber defences through the sharing of cyber threat intelligence among financial institutions. Ongoing efforts are being taken by FinTIP to enhance the coverage of localised threat intelligence sharing beyond the financial industry. This is achieved by collaborating with local cybersecurity agencies to capture real-time and enriched threat intelligence for a more timely assessment of the threat landscape.

Financial institutions continue to identify cyber risk as a top risk facing the industry in 2023 amid growing digitalisation and use of technology in finance, as well as widespread remote working arrangements which increase the potential for exploitation of vulnerabilities. This is expected to keep financial institutions focused on prioritising efforts to improve cyber resiliency.[41] Other key operational risks identified by financial institutions in the period ahead include regulatory non-compliance, competition for critical talent and outsourcing-related risks (Diagram 1.1).

Payment and settlement systems continued to maintain high system availability

The Real-time Electronic Transfer of Funds and Securities System (RENTAS)[42] and major retail payment systems (RPS) continued to maintain high system availability, with no cyber incidents detected in the second half of 2022.

In order to ensure high system availability, the Bank and Payments Network Malaysia Sdn Bhd (PayNet), as payment system operators of RENTAS and major RPS, respectively, continued to enhance control measures to maintain a strong degree of resilience

Diagram 1.1: Key Operational Risks and Mitigating Actions

Cyber threats

- Robust TPSP management process for constant identification, assessment and management of risks
- Implementation of 3-tier architecture, strengthened with security devices such as intrusion implementation systems (IPS) and intrusion detection systems (IDS)
- Annual penetration testing and 24/7 security monitoring, DDoS protection, access controls, patch management and cyber insurance
- Continuous security education and awareness, and specialised security training and certifications for IT personnel

Regulatory non-compliance

- Regular gap analysis and escalation of exceptions to senior management and board
- Timely compliance reviews of new regulatory requirements using risk-based approaches
- Enhancing internal procedures to introduce segregation of duties, independent checks, segmented system access control and multi-tier authorisation processes
- Action plans to support sustainability risk management, such as reviewing investment portfolios and introducing green energy funds

Competition for critical talent

- Benchmarking exercises to enhance recruitment and retention
- Enhancing talent management and succession planning

Outsourcing-related risks

- Strengthening internal processes for outsourcing and third-party risk management
- Establishing a working committee with service providers to monitor adherence to the service level agreement (SLA)
- Regular meetings with service providers on deliverables and issues
- Regular oversight by risk committees on outsourcing arrangements, with dedicated resources, proper governance and regularly updated risk registers
- Ensuring service providers maintain adequate business continuity plans (BCPs) and disaster recovery plans (DRPs)

Human error in executing tasks

- Strengthening internal controls and automating manual processes prone to human error
- Developing a thorough understanding of root causes to develop more effective processes and controls

Source: Bank Negara Malaysia

[40] FinTIP is a technology platform for local financial institutions to rapidly share cyber security threat intelligence and best practices.
[41] Based on the 2022/2023 Emerging Operational Risk Survey conducted by Bank Negara Malaysia.
[42] RENTAS is a real-time gross settlement system for interbank fund transfers, debt securities settlement and depository services for scripless debt securities.

against cyber threats, strengthen the management of critical service providers (CSPs) and further improve business continuity management (BCM):

- Various initiatives are being pursued to continuously strengthen the Bank and PayNet's cyber defence and response capabilities.
- RENTAS and Designated Payment Systems (DPS) were subjected to enhanced BCM requirements following the issuance of strengthened BCM expectations by the Bank in December 2022. The enhanced requirements, coupled with live-runs and BCP scenarios conducted successfully during the year, will further strengthen responses in the event of disruptions; and
- In line with recommendations by the Committee on Payments and Market Infrastructures (CPMI),[43] RENTAS and RPS operators are also enhancing policies and procedures for stronger management of CSPs. These include improvement in the governance and monitoring process, stronger due diligence and selective on-site reviews of CSPs.

Effective 10 February 2023, the Real-time Retail Payments Platform (RPP) has been prescribed as a designated payment system under the Financial Services Act 2013 and Islamic Financial Services Act 2013. This designation accords the Bank with additional powers under the law to issue directives to RPP participants and assume control of the operations of RPP in specific circumstances to safeguard financial stability and the provision of critical payment services.

[43] Annex F of the Principles for Financial Market Infrastructures published by CPMI outlines five oversight expectations for critical service providers i.e., risk identification and management, information security, reliability and resilience, technology planning and communication with users.

Artificial Intelligence in the Malaysian Financial System: Opportunities, Risks, and the Way Forward

Introduction

Recent years have seen artificial intelligence and machine learning (AI/ML) come of age with proven, real-world solutions being deployed across industries.

Breakthroughs in algorithms and techniques, greater abundance of data, and advancements in computational power have contributed to AI/ML's transformative impact and potential for businesses. At the same time, the growing pool of tech talent and expertise, scalable cloud infrastructure, and low cost solutions (e.g., open-source technology) have also lowered the barriers to adoption of AI/ML, thus hastening its adoption.

AI/ML promises new opportunities in finance...

In the area of financial services, the greater adoption of AI/ML techniques offers new propositions for enhancing customer experience and product offerings, particularly through product personalisation at-scale, and faster and more convenient service. AI/ML also helps unlock insights that enable FSPs to make better decisions, while also automating processes. In turn, these have the potential to help FSPs better manage risks, improve operational efficiency and productivity, and reduce cost.

In 2021, BNM conducted a preliminary survey on the use of AI/ML by FSPs with 25 respondents comprising banks, insurers and payments operators in Malaysia. The respondents were selected based on size and track record of digital initiatives, as well as participation in the Open API Implementation Group.[1] Diagram 1 captures the actual and potential use cases for AI/ML identified by respondents, which span across various functions and business lines.

The survey revealed that many FSPs in Malaysia are already actively using AI/ML techniques, with more initiatives under development. At present, AI/ML is most commonly being deployed in the areas of customer analytics and engagement, as well as for e-KYC and digital customer onboarding. Some banking institutions are also supplementing their credit underwriting processes with AI/ML techniques for selected financing products. The higher risk sensitivity of these AI/ML models promote prudent exposure to higher risk borrowers and more accessible services to deserving but underbanked customers. The survey also revealed strong interest and support from the senior management and boards of the FSPs. About half of the respondents considered AI/ML adoption as a potential game changer for the way they do business and are already looking for opportunities beyond the context of known use cases and current AI/ML projects. Diagram 2 sets out a summary of the key findings from the survey.

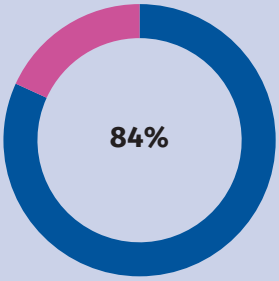
[1] Established by BNM in 2018 to promote standardisation of Open Application Programming Interface (API), which would enhance third party access to data, supported by the security, legal and governance frameworks necessary to protect customer data and financial institutions' core systems.

Diagram 1: Examples of AI/ML Use cases in Financial Services

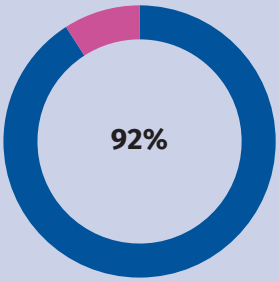
Source: Bank Negara Malaysia

Diagram 2: Summary of Selected

Most FSPs surveyed are actively using AI/ML or developing AI/ML projects...



21 out of **25** surveyed FSPs have at least one AI/ML project **in active use**

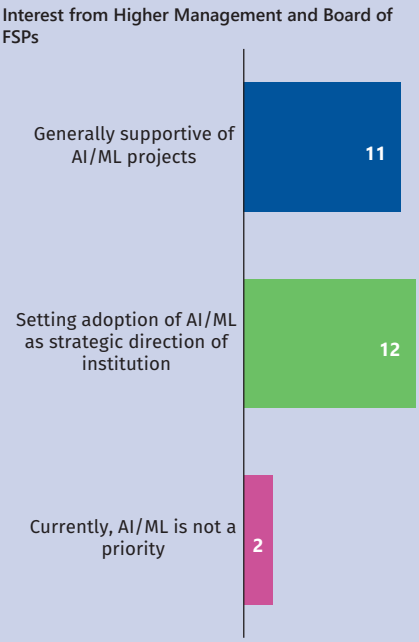


23 out of **25** surveyed FSPs have at least one AI/ML project **in development**

...mainly for customer analytics and engagement as well as KYC

	Top AI/ML Projects	No. of FSP by Use Case Areas
Banks	AML and fraud detection	13
Banks	KYC / Digital on-boarding	12
Banks	Customer Analytics & Engagement	8
Banks	Underwriting/scoring	8
ITOs	Customer Analytics & Engagement	2
ITOs	Human Resources	2
ITOs	Technology Risk Management	2
E-MI	KYC / Digital on-boarding	3
E-MI	Customer Analytics & Engagement	2

Enabled by the Management and Board of FSPs

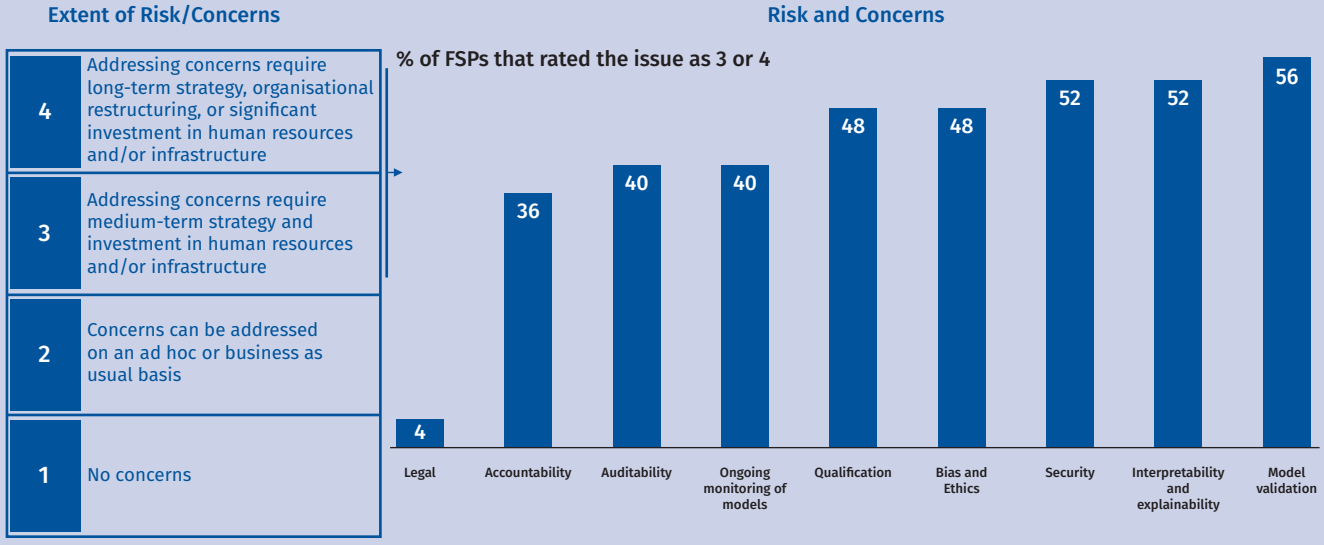


Source : Bank Negara Malaysia

...and risks which need to be carefully managed

However, the introduction and more pervasive use of AI/ML also raises a number of risks which the financial sector will need to manage. The survey surfaced several key AI/ML risks and concerns, as identified by FSPs (see Diagram 3).

Diagram 3: Risk and Concerns Identified in Adopting AI/ML

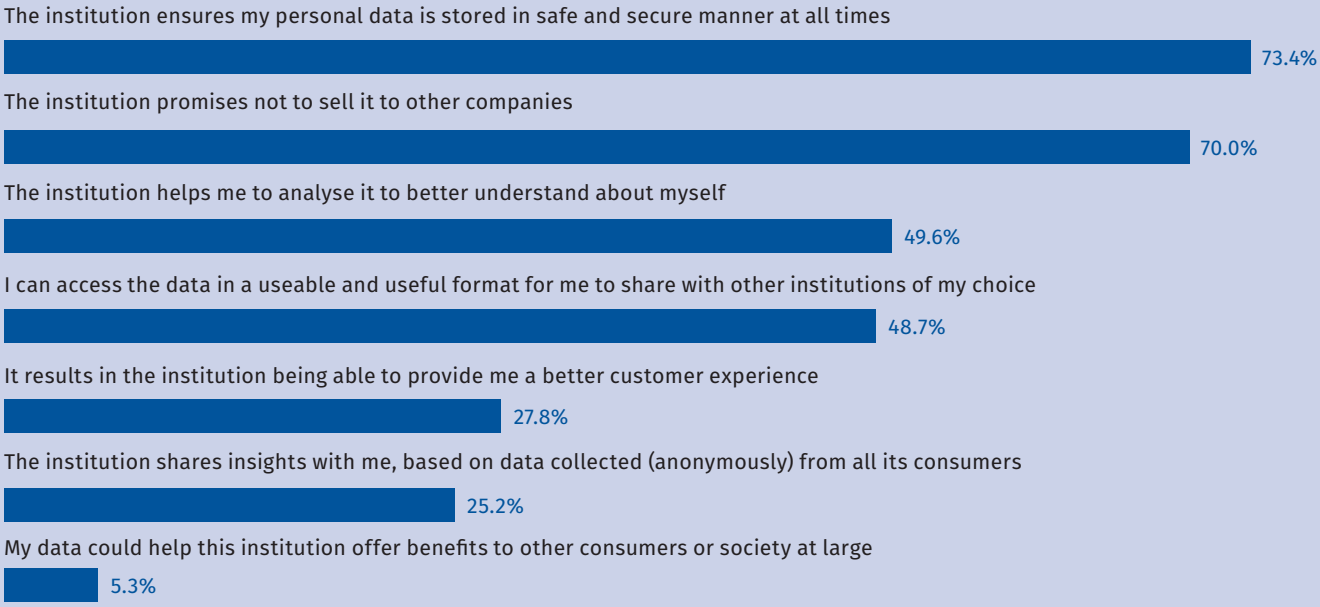


Source: Bank Negara Malaysia

Respondents to the survey cited model validation as the topmost concern of FSPs. Model risk is the risk that models fail to produce accurate results. As most AI/ML models and algorithms are significantly more complex than traditional linear models, model outputs can be difficult to explain and validate. The opacity of AI/ML systems may also delay the detection of any errors or inaccuracies. Timely validation of models, incorporating algorithms that are trained using updated data sets, is crucial in managing model risk and maintaining the predictive ability of the model. Without this, model performance typically deteriorates over time and could result in inaccurate predictions or larger than expected errors, which renders the model unreliable for decision-making. This could lead to undesirable outcomes, such as financial losses, or biased or unfair decisions which impact customers negatively, in turn, exposing FSPs to reputational and legal risks.

Another major aspect of model validation relates to data management and assurance of data quality. Some AI/ML systems require large volumes of data – including high-velocity transaction data – from a variety of sources. This requires robust enterprise data governance to ensure data reliability and quality. The use of a broader range of data, including personal data, also raises concerns about data security and privacy. According to an earlier survey on consumer trust conducted by BNM in 2021,[2] security and privacy are the most important determinants of consumer willingness to share personal data with financial institutions (See Diagram 4).

Diagram 4: Determinants of Consumer Trust in Sharing Data in Malaysia



*Percentages based on items ranked in top 3

Source : Bank Negara Malaysia

At a broader level, increased adoption of AI/ML by FSPs could potentially introduce new risks to financial stability, particularly if the models are poorly calibrated or inappropriately used. Examples of undesirable outcomes include discrimination of certain consumer groups, reduced operational resilience, or amplification of financial shocks from algorithm-driven behaviours. Such risks remain low at present based on the nature and extent of adoption of AI/ML by FSPs. Most FSPs are also approaching the implementation of AI/ML with appropriate caution and care. For instance, the implementation of AI/ML for credit underwriting is typically limited to selected financing portfolios, with close monitoring of the results before the scope is expanded gradually. There are also safeguards put in place by the FSPs to ensure AI/ML systems are kept in-check, such as monitoring of False Acceptance Rate for identity verification using e-KYC solutions.

[2] The survey titled "Consumer Trust Survey" was issued to the public in December 2021. The survey garnered 413 responses from individuals of all ages, income groups and education levels.

Regulations to promote responsible use of AI/ML

The global regulatory landscape governing the use of AI/ML remains relatively nascent. Nonetheless, an increasing number of financial regulators in economies such as Singapore, Hong Kong and the UK have published high level principles or issued guidance on best practices on the responsible use of AI/ML in the financial sector. Some of these documents were produced in collaboration with industry or academic experts. These issuances generally aim to ensure sound and transparent AI/ML systems, promote clear assignment of accountability, and ensure that FSPs pay careful consideration to fairness and other ethical concerns.

Diagram 5: Regulatory Requirements in Managing Risks from AI/ML Adoption

Fair Treatment of Financial Consumers (2019) requires FSPs to ensure that consumers are not subject to unfair discriminatory practices

Risk Governance (2013) states that "... use of models for identifying and measuring risk should be supported by robust processes for managing model risk"

Management of Customer Information and Permitted Disclosure (2021) sets out requirements relating to FSPs' practices and controls in handling customer information

Guidelines on Data Management and MIS Framework (2012) requires financial institutions to establish and maintain a sound data management and management information system (MIS) framework

Risk Management in Technology (2020) requires the technology risk management framework of a financial institution to include identification of risks from the adoption of new or emerging technology, and the associated controls and mitigations

Source: Bank Negara Malaysia

For Malaysia, FSPs are expected to observe existing regulatory requirements (see Diagram 5) in their use of AI/ML applications. While the existing body of standards addresses key risks and considerations that remain relevant to the use of AI/ML by FSPs, greater adoption – in terms of pervasiveness as well as specific use cases that have a higher bearing on critical risk drivers – could call for refinements to existing standards. In particular, further guidance around model interpretability and explainability may be needed as more insight is gained on FSPs' evolving practices. BNM will continue to closely monitor developments and innovations in the industry to inform its regulatory and supervisory approach in ensuring that the risks associated with AI/ML are understood and well managed.