OPERATIONAL RISK

Financial institutions remained operationally resilient

Preserving the operational and cyber resilience of financial institutions remained one of the key focus areas for BNM. In the second half of 2024, financial losses from operational risks reported by financial institutions continued to be small, accounting for only 0.03% of total banking system capital (1H 2024: 0.05%; 2H 2023: 0.03%). Financial institutions remain vigilant against operational disruptions, particularly given the rapidly evolving cyber threat landscape.

During the period, several cyber incidents were reported by the industry, although most of these were of minimal to low severity. The number of distributed denial of service (DDoS) attacks increased slightly, posing a persistent threat to the availability of financial institutions' online services. Financial institutions have in place adequate business continuity plans (BCP) to ensure their readiness to swiftly respond and recover from cyber incidents and minimise operational disruptions. BNM also continues to proactively monitor the cyber threat landscape and has intensified supervisory measures to combat and address these growing threats. These include updating policy requirements to address emerging risks and conducting targeted reviews to evaluate financial institutions' incident response capabilities.

Technical[34] and security debt[35] can contribute to an increase in the vulnerability of the financial industry to cyber threats. Given this, BNM has consistently required financial institutions to bolster their multi-layered defences. This includes ensuring that the rapid digitalisation of business processes is accompanied by adequate resources and expertise to manage execution risks and support operational resilience on a continuing basis amid evolving technological and cyber risks. Financial institutions' annual information technology (IT) expenditure has increased over the years, with a CAGR of 22% for the past three years. Notably, IT expenditure continues to represent a growing share of overall annual expenditure (2024: 23.3% of annual expenditure; 2023: 19.1%; 2022: 18.7%), reflecting its increasing strategic importance for financial institutions. The bulk of expenditures are towards:

- implementing technology refresh efforts, such as the replacement and adoption of better cybersecurity solutions;
- enhancing the management of IT infrastructure and network monitoring;
- augmenting threat intelligence and security monitoring services; and
- increasing training for IT and cybersecurity staff as well as key oversight and control functions to manage emerging cyber risks and trends.

The increase in annual IT expenditure was driven by major upgrades of data centre infrastructure to ensure operational resilience during peak periods, and the rapid pace of product innovation which has contributed to the heightened complexity of financial institutions' IT infrastructure operations. Several banks have launched multi-year programmes to modernise their IT systems. These include re-architecting their network and server infrastructures for better centralised control, agility and flexibility. Some banks continue to enhance IT operational efficiency such as through the adoption of cloud-based security solutions. Major banks primarily allocate capital expenditure to upgrade core systems approaching end-of-life, ensure a secure IT environment and enhance system capacity and backup infrastructure. In addition, development financial institutions and insurers and takaful operators are upgrading data centre capabilities to ensure prompt service recovery during peak periods, following regulatory expectations for high service availability to maintain public confidence. This is also amid a broader adoption of international standards and frameworks for robust information security management.[36]

As part of the increased efforts to ensure that financial institutions' BCP are comprehensive under a range of scenarios, banks were required to further develop more robust and integrated BCP testing. This will help preserve the continuity of banks' critical services and operations in an environment of increasingly complex inter-dependencies.

Financial institutions have identified managing cyber threats, ensuring regulatory compliance and mitigating

[34] Technical debt refers to the trade-off in IT where fixes, upgrades or improvements are delayed or implemented sub-optimally to meet deadlines or budget constraints. This results in additional future costs and effort to address accumulated and compounded issues.

[35] Security debt is a subset of technical debt that focuses on security, occurring when security best practices and protocols are deprioritised in favour of faster development or prioritisation in other areas. Over time, this leads to the gradual accumulation of vulnerabilities in the environment, making systems harder to defend and leading to higher costs and risks in the future.

[36] These include the ISO/IEC 27001 Information Security Management System (ISMS), the US National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Payment Card Industry Data Security Standard (PCI DSS).

social engineering tactics by fraud criminals as their core priorities in managing operational risks for 2025.[37] This is amid increasing sophistication in the modus operandi of threats to the industry and heightened expectations for financial institutions to be able to assure continuous service availability and secure digital services. These risks are at the top of the list due to their rapidly evolving nature, in line with the constantly changing landscape of the financial sector (Diagram 1.2).

To facilitate a more comprehensive and streamlined surveillance of operational risks within the financial system moving forward, BNM has further enhanced the centralised reporting of operational risks to the Operational Risk Reporting (ORR) system to capture more operational risk-related data. The ORR system supports the reporting and assessment of operational risk incidents to BNM, as well as monitoring of incident response actions by financial institutions. It covers fraud, conduct and disruptive incidents occurring in financial institutions. With the increased interfaces between critical banking operations and payment ecosystems, the recent onboarding of payment system regulatees to the ORR system will also provide a more comprehensive view of the overall exposure and resiliency of the financial sector towards operational risks.

Payment and settlement systems continued to maintain high system availability.

The Real-time Electronic Transfer of Funds and Securities System (RENTAS) and major retail payment systems (RPS) continued to maintain a high level of operational resilience and system availability throughout the second half of 2024. There was no major operational or cyber incident during this period. As part of continuous efforts to maintain system resiliency, further enhancements to the business continuity management of RENTAS and major RPS were made to improve system recovery measures in the event of extreme but plausible cyber attacks. Further details on the oversight of payment services can be found in the chapter on 'Promoting Safe and Efficient Payments and Remittance Services' in BNM's Annual Report 2024.

Diagram 1.2: Key Operational Risks and Mitigating Actions

Cyber Threats	The pervasiveness of cybercrime-as-a-service, combined with the emergence of AI-driven attacks, make cyber threats more complicated and sophisticated.	• Strengthened requirements on third-party and supply chain cyber risk management. • Improved preparedness and response to cyber incidents through industry-wide cyber drills. • Increased cyber threat intelligence sharing via FinTIP.
Regulatory Non-Adherence	Stricter regulations and increasing public scrutiny are increasing demands on financial institutions to ensure compliance, particularly in regulatory reporting and ensuring the availability of online services.	• Regular industry engagements to facilitate alignment and promote sharing of best practices. • Strengthened internal control functions for timely identification and rectification of compliance gaps. • Intensified supervisory oversight on IT risk management by financial institutions.
Social Engineering	Evolving scam modus operandi, such as rogue application scams, are increasingly deceiving customers into revealing their banking credentials or other sensitive information.	• Continuously raising public awareness of scam modus operandi via multi-channel approach. • Cross-sectoral collaboration via the National Fraud Portal (NFP) for expedited fraud response. • Improved fraud detection capabilities in financial institutions to detect and block suspicious transactions.
Human Errors	The growing volume of transactions, coupled with evolving internal processes post-digitalisation, increases the risk of errors and operational lapses.	• Strengthened internal controls and more frequent updates to standard operating procedures (SOPs) to reflect process changes. • Continuous capacity building for staff to reduce operational lapses. • Use of analytic tools to detect and prevent recurring errors.
Business Disruptions	Greater reliance on technology, systems and third-party service providers (TPSPs) exposes financial institutions to risks of service disruptions and system outages.	• Enhanced monitoring of critical systems performance and potential threats, including critical services delivered or supported by TPSPs. • Robust business continuity and disaster recovery plans, which are regularly tested to ensure effectiveness.

Source: Bank Negara Malaysia

[37] Based on the 2024/2025 Emerging Operational Risk Survey conducted by BNM.