OPERATIONAL RISK

Continued vigilance in the financial sector to safeguard operational resilience against persistent threats

Continuous efforts by financial institutions to ensure strong operational risk management practices and fraud controls remain critical to support the financial system's operational resilience in an environment of rapid digitalisation of financial services with increasing reliance on third-party service providers (TPSPs). Operational incidents continue to test the detection, monitoring and recovery capabilities of financial institutions. While financial losses from operational risks reported by financial institutions remained low (1H 2024: RM183.9 million; 1H 2023: RM188.6 million), moderate disruptions to online banking services occurred in a few incidents during the period. This called for stronger measures in some institutions to ensure more robust incident response plans and closer monitoring of third-party risks. Financial institutions that fail to meet prescribed regulatory standards to ensure a high level of availability[30] of services will be subject to strong supervisory or enforcement actions, including directives to strengthen controls, increased capital requirements for operational risk and administrative monetary penalties (AMP).

Technology and cyber-related risks will continue to pose challenges to the management and supervision of operational risks within the financial system. The growing sophistication of tools and techniques used by threat actors, as well as the targeting of TPSPs as a means of gaining access to financial institutions' systems or data, further increases the demands faced by financial institutions in their ongoing efforts to secure their environment. Financial institutions continue to invest significant resources in enhancing their cyber security detection and mitigation processes. The annual information technology (IT) expenditure on cyber security alone by financial institutions has increased the most in 2024, extending successive years of double-digit increases in cyber security budgets.

Higher operational risk management standards applied by BNM to payment service providers have also raised the level of cybersecurity risk controls observed by e-money issuers (EMIs) and merchant acquirers, with ongoing improvements observed in the cybersecurity maturity level of these players. Proactive information sharing between BNM and the industry on cyber threat intelligence via the Financial Sector Cyber Threat Intelligence Platform (FinTIP) continues to support financial institutions' threat detection and incident response capabilities. The number of cyber threat intelligence reports shared on FinTIP increased by 40% in the first half of 2024 compared to the same period last year. In addition, efforts to educate and enforce strong cyber hygiene practices among staff and customers remain crucial to build and maintain strong foundational cyber security defences.

To further strengthen financial institutions' operational resilience, BNM will be introducing enhanced expectations on managing cyber risks associated with TPSPs. These include expectations for financial institutions to:

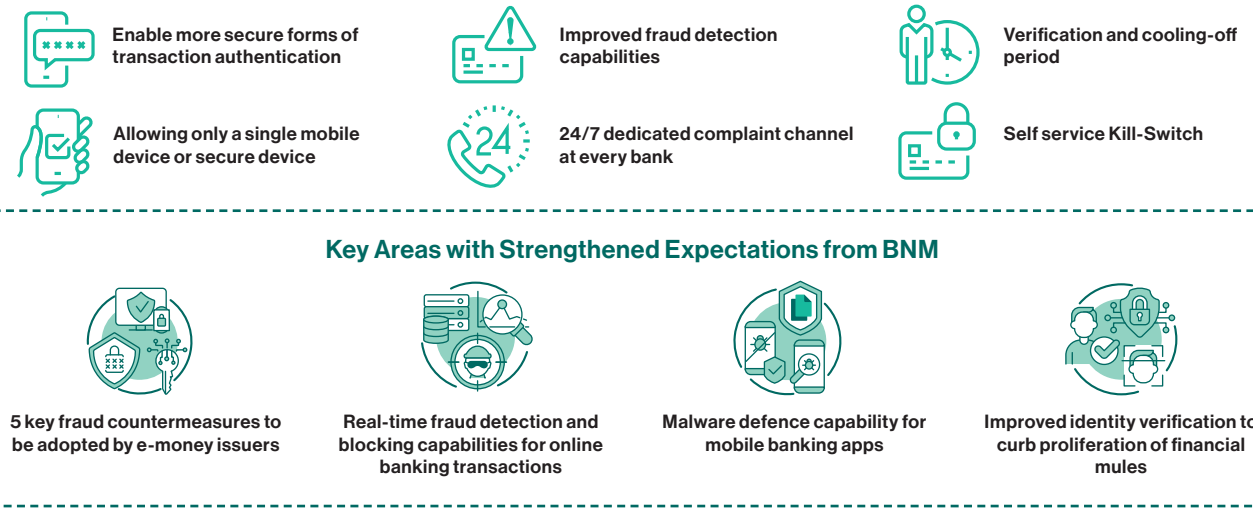
- obtain information necessary to understand and identify potential vulnerabilities associated with their TPSPs' cyber security posture and supply chains;
- conduct regular joint testing of business continuity plans (BCP) and disaster recovery plans (DRP) with material TPSPs; and
- identify and prepare alternate TPSPs to provide redundancy and maintain essential services during disruptions.

Regular IT stress testing remains an integral step to improve financial institutions' capacity to respond and recover from extreme events or external shocks arising from IT disruptions and cyber-attacks. Following a recent thematic review conducted by BNM on banks' IT stress testing programmes, BNM issued guidance on common stress scenarios and minimum shock parameters for IT stress testing to encourage greater consistency in the rigour of IT stress tests conducted by banks, and identify common response and recovery actions across banks that could pose systemic risks.

Financial institutions remain vigilant against new forms of financial fraud and are continuously refining their fraud detection capabilities. Enhancements of fraud prevention measures by banks as part of broader efforts to strengthen the overall multi-layered defence of online banking security (Diagram 1) have resulted in a downward trend of cases of unauthorised online banking transactions (2022 vs 2023: 28% reduction) reported to the National Scam Response Center (NSRC). In 2023, fraudulent financial transactions amounting to RM383 million were successfully blocked by financial institutions. The fraud countermeasures have also been extended to all eligible EMIs to secure more effective sector-wide protection.

[30] As stipulated in S10.32 in the Risk Management in Technology (RMiT) policy document.

Diagram 1: Industry-wide Efforts to Strengthen Security of Online Banking



Source: Bank Negara Malaysia

Continuous efforts are in place to ensure resiliency of payment and settlement systems

The Real-time Electronic Transfer of Funds and Securities System (RENTAS) and major retail payment systems (RPS) continued to maintain high system availability throughout the first half of 2024. While no major incidents or service disruptions were observed for RENTAS, the DuitNow services under the Real-time Retail Payment Platform (RPP) and cheque services under the National Electronic Cheque Information Clearing System (eSPICK) experienced a service disruption in May due to hardware failure. Both services were promptly recovered following the successful activation of contingency and recovery plans which operated as expected. No recurrent incidents have been observed.

Since 1 July 2024, all RENTAS participants have successfully migrated their RENTAS payment transactions to ISO 20022, marking the conclusion of a project that began in 2019 to support the futureproofing of a key domestic payment infrastructure. Adopting the ISO 20022 messaging standard provides financial institutions access to richer and more structured data, including payment references, invoice details and regulatory information. With this information, RENTAS participants can enhance compliance screening, increase process automation and provide better customer service. Participants are now shifting their focus to the migration for cross-border payments which is expected to be completed by June 2025 for key payment messages, and November 2026 for non-key messages to meet the timeline prescribed by SWIFT.[31] As of July 2024, around 32% of participants have completed the migration for cross-border payments, with the remaining participants on-track to meet the prescribed timelines.

Malaysia's regional cross-border instant payments connectivity with Indonesia, Thailand and Singapore has contributed to the increasing usage of the cross-border Quick Response (QR) payments. The total QR payment transactions in the first six months of 2024 alone already doubled the transaction volume recorded for the whole of 2023. With volumes poised to grow further, ensuring that payment system operators continue to fulfil prescribed technical specifications on an ongoing basis will be critical to minimise service disruptions and improve security. This is being further reinforced by BNM's continuing efforts to enhance cross-border cooperative oversight arrangements with regulatory bodies in the respective jurisdictions.

[31] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global network operator facilitating secure financial transactions and communication between banks and other financial institutions.