OPERATIONAL RISK

The financial sector remained operationally resilient amid an evolving risk landscape

Financial losses arising from operational risks reported by financial institutions remained low, accounting for just 0.04% of total banking system capital (2H 2024: 0.03%; 1H 2024: 0.05%). At the same time, financial institutions continued to demonstrate operational resilience and were able to provide reliable and efficient essential financial services to customers. Notably, incidents involving technological failures and severe prolonged disruptions of online services to the public declined by 38% during the period. This improvement reflects the additional efforts taken and investments made by financial institutions to strengthen their operational resilience to meet service availability standards expected by financial consumers. Nevertheless, continued efforts are important not only to maintain the availability and resilience of financial institutions' critical systems, but also to improve customer experience, including when certain financial services are unavailable or temporarily interrupted. Priorities include enhancing online service reliability and fostering a more customer-focused approach of managing service interruptions, with effective and timely communication to affected customers to minimise inconvenience.

While the number of reported cyber incidents increased in the first half of 2025, most were of minimal to low severity. The increase in reported cases partly reflects improvements in the comprehensiveness of cyber incident reporting by financial institutions, supported by ongoing awareness and knowledge-sharing efforts by BNM. Notably, no ransomware incidents were reported during the period. Amid persistent cyber threats, financial institutions continue to progressively enhance their cyber vigilance and response capabilities. This is reflected in financial institutions' enhanced capabilities in threat surveillance, detection, response and recovery functions, which have enabled more effective containment and management of cyber threats with minimal operational disruptions.

In response to the rising trend of reported cyber incidents and to further strengthen financial institutions' capabilities in managing emerging cyber risks across the sector, BNM conducted a focused review of financial institutions' Application Programming Interface (API) security management practices. The review revealed a high level of readiness across the financial sector, with widespread adoption of best practices in managing API-related security risks, particularly in areas such as development standards, security testing and assessment, and API authentication and access controls. However, governance in API management and the implementation of automated security controls were identified as key areas requiring further improvement by financial institutions.

While the industry's refined fraud countermeasures have curbed unauthorised scam cases,[18] the first half of 2025 saw a rise in authorised fraud schemes, driven by social engineering and manipulation tactics. These schemes often exploit customer trust and circumvent security controls. To strengthen defences against such threats, BNM and the financial industry stepped up customer education and awareness programmes. BNM also introduced enhanced fraud countermeasures to strengthen the fraud defence systems of financial institutions. Key expectations from these standards include:

- establishment of detailed risk profiles for each customer through behavioural analysis to enhance fraud detection;
- real-time detection and blocking of suspicious or fraudulent transactions;
- swift investigation and verification upon blocking;
- prompt detection and termination of hijacked sessions;[19] and
- continuous update and enhancement of fraud detection rules.

Safeguarding customer trust and the integrity of the banking system remains a priority for BNM. The National Fraud Portal (NFP), a key platform used by the National Scam Response Centre (NSRC) to trace stolen funds, will be enhanced with advanced analytical capabilities to enable early detection of mule accounts and suspicious transactions. This marks a significant step forward in the industry's shift towards proactive fraud prevention and, equally important, in minimising monetary losses to victims.

[18] An unauthorised transaction refers to a payment transaction that is not consented, initiated or authorised by the customer. This excludes transactions where the victim has willingly performed and approved the payment at the point of the transaction (e.g. love scam, investment scam and parcel scam).

[19] A hijacked session occurs when a fraudster takes control of a user's active online session.

Complementing these efforts are ongoing scam awareness and educational campaigns, jointly organised by public and private sector partners, aimed at empowering consumers to become more discerning and vigilant, particularly as authorised fraud schemes become increasingly prevalent. BNM continues to uphold the policy on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions, introduced in 2024. This policy reinforces consistent and fair outcomes for scam victims by requiring financial institutions to conduct timely, transparent investigations and offer fair compensation, including independent reviews where appropriate.

Following the conclusion of the public consultation on the Exposure Draft for Risk Management in Technology (RMiT) in February 2025, BNM will be issuing the finalised RMiT policy document in the final quarter of 2025. In response to the growing pervasiveness of digital services, the updated policy outlines new expectations for financial institutions to build service resilience. These include step-up service availability goals – particularly for banks with high volumes of retail transactions – to meet higher customer expectations, proactive management of intermittent performance issues, enhanced coordination with third-party service providers for effective incident response, and establishment of communication protocols to keep customers informed and supported during disruptions.

The updated policy also augments cyber defence requirements in line with global best practices, including the adoption of continuous control monitoring to mitigate third-party risks. The unified information technology (IT) risk management policy requirements will also be extended to large merchant acquirers and intermediary remittance institutions, based on specified thresholds, aimed at fortifying the security of the payment services ecosystem as a whole. In tandem, the regulatory review process will be simplified and streamlined to accelerate the deployment of mature technologies and facilitate the assessment of emerging technologies such as cloud computing.

Payment and settlement systems remained reliable and secure

The Real-time Electronic Transfer of Funds and Securities System (RENTAS) and major retail payment systems (RPS)[20] remained resilient, maintaining a high level of system availability throughout the first half of 2025. No major operational or cyber incidents were observed during this period. However, an isolated incident due to a third-party service's global outage temporarily disrupted connection to RENTAS. The issue was promptly addressed following the successful and timely activation of the third-party service's alternate site.

As part of ongoing supervisory efforts to strengthen the stability and resiliency of key payment infrastructure, BNM conducted a supervisory examination of the Real-time Retail Payments Platform (RPP) operated by PayNet. Efforts are ongoing to further improve the overall resiliency and security of the RPP, particularly in business continuity management as well as management of critical service providers, participants and cross-border services. As regional cross-border Quick Response (QR) payment connectivity broadens and grows, BNM will continue to enhance the oversight of cross-border payment arrangements through collaborative efforts with relevant regulatory authorities.

[20] Real-time Retail Payments Platform (RPP), Interbank GIRO (IBG), National Electronic Cheque Information Clearing System (eSPICK), Financial Process Exchange (FPX), Shared ATM Network (SAN), Direct Debit (DD), MyDebit, National Electronic Bill Payment (JomPAY) and Instant Transfer (IBFT).