OPERATIONAL RISK

Financial institutions remained operationally resilient with sustained vigilance over emerging risks

Financial institutions remained operationally resilient throughout the second half of 2025. Associated financial losses increased but remained small at only 0.11% of total banking system capital (1H 2025: 0.04%; 2H 2024: 0.03%). The losses were primarily attributable to a few isolated external fraud cases and system disruptions, which were addressed through timely corrective and recovery actions. In parallel, financial institutions continued to strengthen their operational risk systems and processes with targeted investments aimed at addressing root causes and enhancing internal controls.

As digitalisation and technology adoption accelerate within the financial sector, strengthening cyber resilience remains a key priority. Financial institutions continue to uphold strong cyber hygiene standards and remain vigilant against evolving technological risks and cyber threats. While incidents involving third-party service providers (TPSPs) rose slightly amid global data leaks and supply-chain compromises, no major incidents or direct breaches impacting local financial institutions were reported.[23] Systemic risks from third-party failures remain low, given financial institutions' increasingly stringent risk management controls over third-party services and ongoing enhancements to response, recovery and contingency plans for TPSP-related risks.

Financial institutions also strengthened their vigilance against evolving fraud tactics. As a result, there was a notable increase in the volume of fraudulent transactions successfully blocked in 2025.[24] However, reported fraud cases continued to rise, driven mainly by sophisticated malware capable of compromising customer devices and enabling unauthorised fund transfers. In response, BNM and the industry enhanced mobile shielding capabilities to better protect mobile banking platforms and customer devices from malware and unauthorised access.[25] Complementing these efforts, BNM and the financial industry also initiated a structured migration plan to ensure that online banking services operate only on supported web browsers and mobile operating systems. This reduces vulnerabilities associated with devices that no longer receive critical security updates while preserving financial inclusion through compensating safeguards.[26]

Following the issuance of the revised Risk Management in Technology (RMiT) policy document in November 2025, financial institutions have been implementing the updated requirements to further strengthen service resilience and cybersecurity.[27] During this transition period, industry efforts focused on minimising and responding to service disruptions, as well as strengthening customer communication during service outages.

In the second half of 2025, BNM conducted targeted reviews of financial institutions' business continuity plans (BCPs) for critical customer-facing services. The reviews assessed the adequacy of workaround solutions in managing the impact of operational disruptions and ensuring service continuity to customers. While overall arrangements were assessed to be adequate, several areas for improvement were identified, including:

- developing and strengthening recovery capabilities, particularly by modernising core banking systems to meet heightened public expectations on service availability;
- enhancing internal governance and instituting consequence management to reinforce accountability and cultivate a strong operational resilience culture;
- accelerating efforts to identify single points of failure, particularly in online banking, Automated Teller Machines (ATMs) and call centres, given rising dependency complexities and potential systemic implications; and
- conducting more robust joint BCP testing with critical TPSPs to ensure continued delivery of essential financial services during disruptions.

---

23 Major global incidents involving TPSPs in 2025 included a data breach affecting legacy cloud environments of Oracle, a global database management software provider, resulting in the leakage of millions of authentication-related records. Another TPSP, Salesloft, similarly experienced a data breach that resulted in a supply-chain compromise. In this incident, attackers exploited the TPSP's integration with a widely used sales chatbot application to gain unauthorised access to multiple cloud environments, affecting several other TPSPs and, in turn, the financial institutions that relied on their services.

24 In 2025, banks successfully blocked approximately RM1.2 billion in fraudulent transactions compared to RM399 million in 2024.

25 These measures include advanced malware detection, blocking of risky applications, enforcing the use of supported devices and operating systems, regular security updates and device integrity checks.

26 In circumstances where customers' devices cannot support the required operating systems, financial institutions shall heighten monitoring of users on such devices, strengthen anti-malware measures and apply appropriate function restrictions to limit security risks.

27 These requirements include step-up service availability goals to meet higher customer expectations, proactive management of intermittent performance issues, enhanced coordination with TPSPs for effective incident response and establishment of communication protocols to keep customers informed and supported during disruptions.

Several large domestic banks have taken proactive steps to bolster crisis readiness by developing scenario-specific BCPs for events such as cyber breaches, power outages and critical information technology (IT) infrastructure failures. These efforts are supported by structured escalation processes with clearly defined timeframes to minimise delays in incident resolution.

Looking ahead to 2026, cyber risk remains the foremost concern for financial institutions amid increasingly sophisticated cyber threats, and the operational, financial and reputational implications.[28] The industry also cites strategic and organisational risks as key areas of operational risk, reflecting changes in business models to meet shifting customer needs, heightened competition for critical talent and faster technological advancements. Additionally, regulatory compliance remains a key focus to support institutional resilience. Other notable operational risks identified for the year include IT disruptions, potential execution failures stemming from human error and risks related to increasing reliance on external service providers (Diagram 1.1).

Given the importance for financial institutions to withstand potential disruptions and maintain continued delivery of financial services, BNM issued a Discussion Paper on Operational Resilience in December 2025 to surface key regulatory considerations governing financial institutions' operational resilience posture and practices. The paper underscores the need for institutions to maintain robust operational risk management capabilities, supported by resilient technology and cyber defences to mitigate and manage disruptions effectively. It also highlights the importance of sound governance and accountability mechanisms, with financial institutions' boards driving tangible and sustained outcomes for operational resilience.

Diagram 1.1: Key Operational Risks and Mitigating Actions

Information security & cyber risk

- Deployment of key cybersecurity controls such as Multi-Factor Authentication (MFA), Privileged Access Management (PAM), Endpoint Detection & Response (EDR) and integrated threat intelligence platforms to enhance cyber defence.
- Regular cyber awareness programmes including phishing simulations to strengthen staff readiness.
- Improved incident response procedures, including escalation, communication and resolution protocols.

Regulatory compliance & transparency risk

- Regular regulatory gap analysis and impact assessments to identify control and policy gaps.
- Targeted compliance training for staff aligned to regulatory requirements.
- Strengthened governance through compliance taskforces, formal attestations and continuous regulatory engagement.

Strategic/organisational risk

- Workforce and leadership capabilities aligned to evolving strategic priorities through benchmarking, continuous learning and leadership development.
- Technology and operating model modernisation to support business transformation and evolving customer needs.
- Strong governance and cross-functional oversight of enterprise-wide change and risk management.

IT disruption risk

- Infrastructure enhancements including implementation of multiple live data centres to improve system availability and resilience.
- Regular business continuity plan/disaster recovery plan (BCP/DRP) testing to validate recovery readiness.
- Adoption of latest cloud-based architecture enabling automatic scaling, controlled system updates and embedded security to enhance system stability.

Execution & process failures risk

- Regular review of standard operating procedures (SOPs) and targeted staff training to reduce human error and mitigate process failures in day-to-day operations.
- Enhanced quality assurance and use of analytics tools to detect systemic issues.

Third-party & outsourcing risk

- Enhanced vendor monitoring through Key Performance Indicators (KPI) and issue tracking.
- Stronger contractual safeguards covering service levels, termination and exit strategies.
- BCPs and contingency plans to mitigate disruption from vendor failures, with strengthened crisis communication during service outages.
- Joint BCP testing with critical third-party service providers (TPSPs).

Source: Bank Negara Malaysia

[28] Based on the 2025/2026 Emerging Operational Risk Survey conducted by BNM.

Key initiatives are in place to ensure continued resilience of payment and settlement systems.

The Real-time Electronic Transfer of Funds and Securities System (RENTAS) and major retail payment systems (RPS) remained resilient and sustained a high level of system availability in the second half of 2025, with isolated incidents promptly rectified. In addition to ongoing monitoring of key payment infrastructures, BNM conducted targeted supervisory reviews of selected payment service regulatees to assess the adequacy and robustness of fraud controls,[29] effectiveness of IT and cyber risk management, and soundness of conduct practices. The reviews observed that payment service regulatees are taking proactive steps to strengthen fraud mitigation measures and meet compliance requirements. While measures for IT and cyber risk management as well as conduct practices were generally assessed to be adequate, the effectiveness of governance and oversight functions on these areas can be further strengthened. Remediation actions taken following the supervisory reviews have enhanced the level of compliance, reduced operational risks and reinforced the efficiency and reliability of payment services.

As e-payment transactions gain momentum, managing credit and settlement risks associated with real-time retail payments has become increasingly important. To address the interbank settlement risks inherent in deferred net settlement models, BNM has introduced near real-time settlement for Real-time Retail Payments Platform (RPP) transactions through the launch of RENTAS+ in late September 2025. Under this, RPP transactions are settled on a near real-time gross basis, significantly mitigating interbank credit and settlement risks while further strengthening confidence in the payment systems. Further details on RENTAS+ can be found in the chapter on 'Promoting Safe and Efficient Payments and Remittance Services' in BNM's Annual Report 2025.

[29] These controls include the implementation of five key fraud countermeasures mandated by BNM for eligible electronic money issuers effective January 2025. The measures comprise robust multi-factor authentication, cooling-off periods, single secure device authentication, a kill switch and the establishment of a 24-hour complaints channel.