OPERATIONAL RISK

Operational Risk Losses among Financial Institutions Remained Small but Emerging Risks Warrant Close Vigilance

Occurrences of operational risk incidents in the financial system have risen amid increasing digitalisation and greater reliance on third party service providers. Nevertheless, the number of and total losses from these incidents have remained insignificant for banks, insurers and takaful operators relative to the volume of intermediation activities.

For banks and development financial institutions, total losses in 2019 from the materialisation of operational risk events accounted for 0.7% of total profit before tax, compared to 3.1% for credit risk losses. Almost all of the operational risk losses were attributable to trade finance related fraud, involving the recycling of used bills of lading and invoice reference numbers for fictitious trades. Such fraud continues to account for a small portion of the total trade finance exposures.

In the insurance and takaful sector, operational risk losses were largely driven by fraudulent claims, typically in relation to exaggerated vehicle accident damage or injuries, and staged accidents or thefts. As these types of fraud often involve multiple parties, many cases are difficult to prove and often remain unreported as fraud. Consequently, total reported losses from the materialisation of operational risk events in this sector accounted for a much smaller proportion of total profit before tax (less than 0.5%).[47]

Financial institutions' internal safeguards to detect and address fraudulent activities thus far have kept losses low. However, financial institutions should

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events (Table 1.4). It is inherent in all activities, products and services of a financial institution. Often, operational risks materialise in the form of fraud, physical damage, transaction failures and business disruption. This may result in direct as well as indirect financial losses, for example, loss of business and market share due to reputational damage.

Table 1.4

Characteristics of Operational Risk

Idiosyncratic	The operational risk profile of a financial institution is unique to its internal processes, people and systems. For example, an institution that is reliant on manual processes is more at risk of human error, while an institution that is reliant on IT systems is more at risk of IT system failures.
Multifarious	Operational risk can traverse multiple business lines and external parties associated with the institution. For example, disruptions to an institution's critical system can be caused by the failure of a third-party service provider to follow terms of a Service-Level Agreement. Conversely, operational failures in a financial institution can affect other institutions through connections to a shared infrastructure.
Fat-tailed distribution	Most of the time, operational risk events incur small-scale losses, such as fraudulent insurance claims. However, some operational risk events, such as a cyber-attack on a major payment system infrastructure, could lead to severe disruptions in the provision of financial services and erode public confidence.
Difficult to model	The fat-tailed nature of operational risk losses, the absence of a clear link with macroeconomic factors, the lack of historical data and difficulty in mapping past operational loss events[48] are among the factors that make operational risks particularly challenging to model. Risk modelling is also constrained by the evolving nature of a financial institution's operational risk profile with on-going changes in its business model, internal processes and the operating environment.

[48]This is because the realisation of losses from an operational risk event may only happen some time after the occurrence date, for instance, losses incurred from a fraud event may only materialise well after the fraud event has occurred

Source: Bank Negara Malaysia

[47] This is an estimation as the Bank continues to refine the operational risk data reporting by insurers and takaful operators to improve the industry's quality and consistency in reporting.

remain vigilant of the evolving modus operandi of such activities in response to the heightened controls by financial institutions.

While several financial institutions reported disruptions that affected the provision of financial services to some customers during the year, these were mostly isolated incidents involving temporary branch closures or disruptions to online transaction and customer services. For most incidents, services were resumed within one to two hours. In a few cases of more prolonged disruptions, customers were still able to access alternative channels to conduct financial transactions, including online and at neighbouring branches. During the Movement Control Order in March 2020 following the escalation of the COVID-19 pandemic, consumers continued to have access to essential financial services with financial markets also remaining open.

In an annual operational risk survey of financial institutions, a number of emerging risks were noted among the top risks that financial institutions face:

i. Cyber threats
Cyber threats are expected to become more sophisticated and frequent as financial institutions embrace digitalisation. Operations that are heavily dependent on interconnected systems are particularly at risk. Additionally, unauthorised access or unintended disclosure of customer information to external parties, arising from hacking or cyber-attacks could expose financial institutions to legal action and reputational risk, as well as affect public confidence.

ii. Outsourcing including cloud computing
Increasing reliance on cloud services and third-party vendors exposes financial institutions to higher risk of operational lapses as these vendors and services are not within the financial institution's direct control. Over-reliance on these service providers could also hamper the ability of financial institutions to maintain continuity of critical functions in recovery and resolution scenarios.

iii. IT system failure impacting more interconnected systems
System downtime and IT failures typically arise from power outages, obsolete hardware or applications, and poor legacy systems migration. In increasingly interconnected systems, a failure in one IT system is more likely to affect other customer-centric applications such as internet banking, online insurance services, and trade and settlement systems.

iv. Human error
Financial institutions expect human error[49] to continue to persist despite the adoption of technology. This risk is heightened by obsolete legacy systems that are not replaced in time and are unable to support new products and increasing business volumes, thus requiring more manual exception handling.

v. Regulatory complexity
The increasing complexity of global regulatory requirements have led to higher compliance risk for financial institutions. Compliance risk is higher for financial institutions with overseas operations, as they have to manage variations in the implementation of global reforms in other jurisdictions. Gaps in regulatory adherence may expose these institutions to enforcement actions including penalties.

The Bank has intensified its engagements with financial institutions on improving approaches to the measurement of operational risk as well as scenario analysis and stress testing. Financial institutions have also been required to regularly update and test their operational incident response plans in order to identify and address gaps in prevention, response and recovery capabilities.

In addition, the Financial Sector Cyber Threat Intelligence Platform (FinTIP) that is being established by the Bank in collaboration with the industry to collate, aggregate, analyse and share cyber threat information from multiple trusted sources is expected to be operational by the end of 3Q 2020. In the insurance industry, the Fraud Intelligence System (FIS) facilitates more efficient identification and investigation of potential fraudulent motor claims using data analytics and scoring. Efforts are ongoing to enhance the fraud alert accuracy and quantify cost savings from its utilisation. These developments complement

[49] Human error can arise from a combination of factors, including intentional and unintentional breaches of policies, careless execution of tasks, lack of knowledge and training, and unclear operating procedures.

the Bank's Operational Risk Integrated Online Network (ORION)[50] which facilitates system-wide monitoring and early detection of operational risk trends. An industry crisis simulation exercise planned for 2021 will provide an important opportunity to test current arrangements for responding to a crisis event both at the institution and system-wide levels. This in turn will provide further insights for ongoing improvements to the financial system's crisis preparedness and response capabilities.

Payment and Settlement Systems Remained Stable without Major Disruptions

In 2019, a total of 5.1 million transactions amounting to RM56.8 trillion were settled via the Real-time Electronic Transfer of Funds and Securities System (RENTAS),[51] equivalent to 37.8 times of Malaysia's gross domestic product (GDP). This represents an annual growth of 3.2% in total volume and 2.9% in total value. RENTAS continued to remain resilient and maintained high system availability above 99.9% throughout the year. While there were a few incidents of minor disruptions caused by network and infrastructure issues, these issues were promptly resolved with no recurring incidents.

Malaysia's retail payment systems also achieved high system availability above the target level of 99.9% throughout 2019. Credit transfers, such as Interbank GIRO (IBG) and Instant Transfer, which accounted for the bulk (62.4%) of retail electronic payments both achieved 100.0% system availability. Incidents involving other types of retail payment systems such as DuitNow, JomPAY and FPX which were caused by processing and system configuration issues resulted in some isolated settlement delays but did not affect the execution of payment transactions by customers. Similar to RENTAS, the issues have been resolved.

[50] Launched in 2014, the ORION is a risk surveillance system that consolidates information on operational risk incidents, including cyber-attacks.

[51] RENTAS is a real-time gross settlement system for interbank fund transfers, debt securities settlement and depository services for scripless debt securities. Besides Malaysian Ringgit, RENTAS also facilitates Renminbi and US Dollar transactions via appointed on-shore settlement institutions.