OPERATIONAL RISK

Financial institutions remained operationally resilient despite challenges

The pandemic has continued to test the operational resilience and business continuity frameworks of financial institutions, with the resurgence of infection risks and an extended period of remote working arrangements now built into baseline scenarios for the foreseeable future. Adaptations made to business continuity plans (BCPs) since the first MCO in March 2020 have enabled financial institutions to remain operationally resilient without any major operational, information technology (IT) and cyber disruptions, thus ensuring the continued provision of essential financial services to the public.

Notwithstanding this, financial institutions are continuing to review and update their BCPs and disaster recovery plans (DRPs). This aims to provide greater assurance of their ability to maintain critical operations and increase the speed with which business operations are able to adapt to changing conditions in the event of a prolonged full-scale lockdown at critical premises, sudden unavailability of key third-party service providers, and major breakdowns in IT infrastructure supporting remote working arrangements (Diagram 1.3). These enhanced BCPs and DRPs will reinforce financial institutions' capacity to anticipate, prepare for, and adapt to future shocks.

Despite the pandemic coinciding with the technology refresh cycle of key operating platforms used in the banking industry, financial institutions have generally been able to keep to their committed plans for the implementation of critical IT projects. While temporary delays have been unavoidable in some cases due to prolonged movement restrictions, adjustments to implementation timelines have not been material. The industry remains committed to completing these technology refresh projects in a timely manner, given the importance of strictly observing IT lifecycle management policies for high-risk systems reaching end-of-life to reduce operational risks. With the increasing prevalence of mobile and internet banking since the MCO, banking institutions are also reviewing plans to expedite the migration to alternative authentication methods for internet banking transactions. This will serve to avoid potential disruptions to online transactions by putting in place back-up solutions to the one-time password (OTP) to allow for the safe use of alternative forms of multi-factor authentication.

Diagram 1.3: Enhancements to Business Continuity Plans and Disaster Recovery Plans Observed Among Financial Institutions

Readiness for a prolonged full-scale lockdown at critical premises

01 Establishment of policies and procedures to facilitate operational workflows during large-scale split operations

02 Establishment of additional strategic alternate sites in the event the head office becomes inaccessible and to support split operations

03 Improvements to crisis communications to support swift adaptations to directives from the Government, regulators and relevant authorities

Preparation for sudden unavailability of key third-party service providers

01 Contingency plans that identify alternate third-party service providers, or establish internal capability

02 Better coordination with third-party service providers to facilitate their operations during MCO (e.g.: travel authorisations)

Provisions for major breakdown in IT infrastructure

01 Strengthened preparedness to deploy manual processes

02 Expanded capacity and strengthened operational readiness of disaster recovery centres (DRCs)

03 Established additional alternate sites equipped with backup infrastructure to continue essential business operations

Source: Bank Negara Malaysia

Total operational risk losses among financial institutions in the second half of 2020 remained stable and insignificant, similar to previous years. Losses from the materialisation of operational risk events amounted to 0.5% and 0.04% of total profit before tax of banking institutions (including development financial institutions) and insurance and takaful operators, respectively. The Bank and financial institutions remain vigilant against heightened risks, particularly from extended remote working arrangements which have required financial institutions to enable staff to access critical information and systems remotely, either on a business-as-usual or exceptional basis to support business continuity.

Payment and settlement systems continued to operate with minimal disruptions

Malaysia's payment systems continued to operate smoothly without major disruptions, with the large-value payment system, Real-time Electronic Transfer of Funds and Securities System (RENTAS),[28] and retail payment systems (RPS) maintaining high system availability at above 99.9%. Online payment transactions continued to increase, driven by e-commerce activity as consumers adjusted to movement restrictions, with a total of 1.1 billion transactions amounting to RM 1.3 trillion conducted in RPS in the second half of 2020 (1H 2020: 0.8 billion transactions amounting to RM1 trillion). For RPS, a slightly higher number of incidents of isolated disruptions were reported in the second half of 2020 compared to the first half of the year. However, these were swiftly resolved and did not cause major disruptions, with contingency and recovery plans operating as expected. For RENTAS, the completion of technology refresh efforts since the first quarter of 2020 has further reduced potential risks of disruptions. As a result, the number of incidents that caused isolated disruptions to RENTAS declined by 32% in the second half of 2020, compared to the first half of 2020.

Both RENTAS and RPS operators have maintained split operations despite the lifting of movement restrictions following the first MCO in the first half of the year. These operators have also further enhanced their BCPs to incorporate remote access capabilities and security to enable more staff to work from home. Personnel were also identified and trained to increase the number of reserve staff available to readily take over critical operations if necessary. These payment system operators also continued to conduct planned business continuity exercises under the 'new normal' to test response and recovery measures in order to minimise service disruptions.

[28] RENTAS is a real-time gross settlement system for interbank fund transfers, debt securities settlement and depository services for scripless debt securities.