# OPERATIONAL RISK

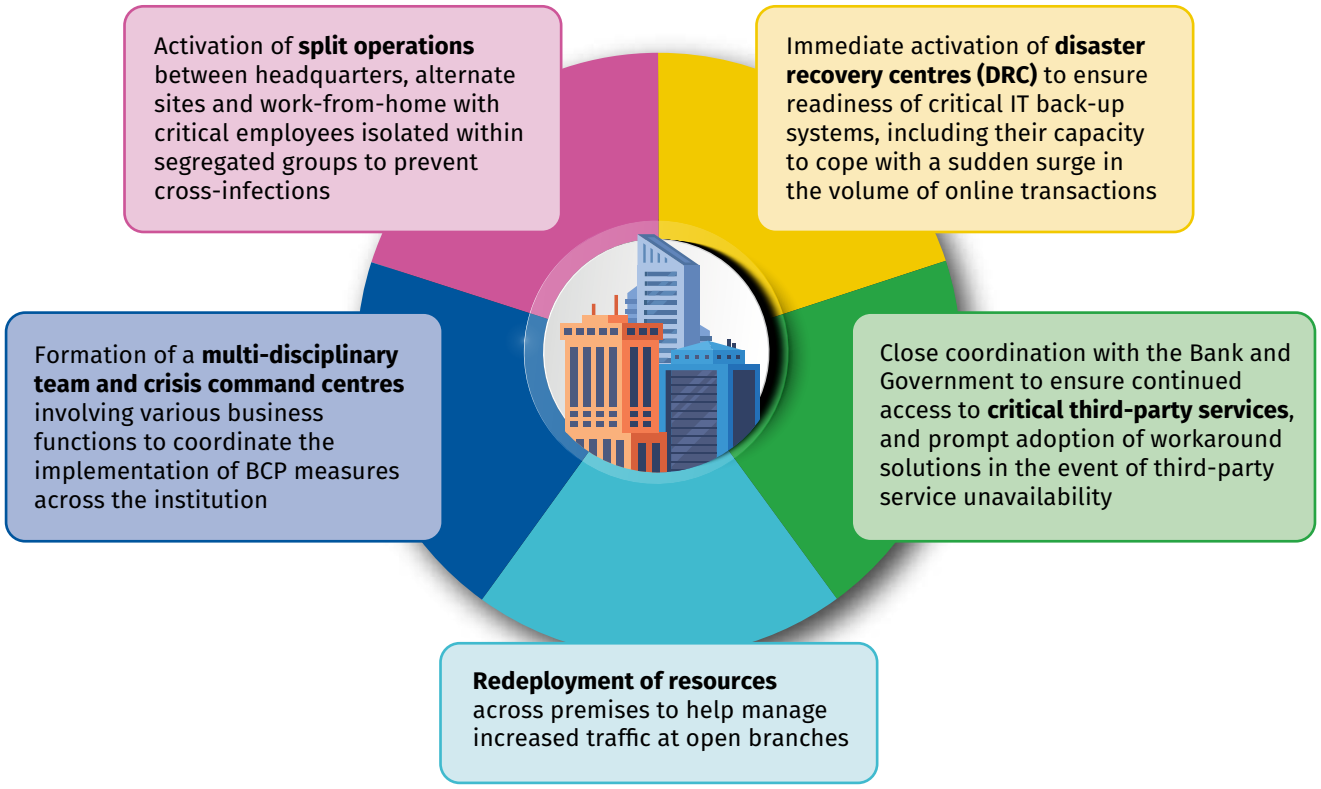
## There were no operational disruptions despite heightened operational risks during the pandemic, and financial institutions are taking further steps to strengthen business continuity plans

The pandemic presented new operational challenges which tested the agility of financial institutions' business continuity plans (BCPs). Notwithstanding heightened operational risks, financial institutions successfully activated BCPs which enabled the continued provision of essential financial services to the public, while protecting the health and wellbeing of staff and customers (Diagram 1.2).

The implementation of the MCO to contain the outbreak also introduced additional restrictions that required financial institutions to swiftly adapt their operations in ways that were not previously contemplated in most BCPs (further elaborated below).

The immediate establishment of a centralised communication channel between the Bank and the industry prior to the onset of the MCO was critical to effectively coordinate the implementation of health measures across the financial sector. It also supported the swift transmission of critical information on operational risk incidents throughout the MCO period which enabled financial institutions to take pre-emptive measures to protect their staff, customers and operations on a continuous basis. Financial institutions largely continued to operate within their recovery time objectives for critical operations, supported by increased resources and management attention directed towards ensuring system resilience throughout the MCO period.

**Diagram 1.2: BCP Responses by Financial Institutions during the Pandemic**




Source: Bank Negara Malaysia

While financial institutions remained operationally resilient, they are taking steps to further enhance existing BCPs to specifically incorporate measures to respond to a pandemic event:

i. **Preparation for prolonged or widespread disruptions to business**
BCPs typically have been designed to respond to disruptions that are either temporary in nature, or contained to a limited number of locations, facilities or systems, such as those caused by power or infrastructure failures, cyber-attacks and natural disasters. While some BCPs included pandemics as a potential scenario, few financial institutions envisioned disruptions to business operations that could arise from multiple waves of a pandemic affecting different parts of the country and the world over an extended period of time. For instance, financial institutions assumed that operations could continue to function by 'swinging' to disaster recovery centres (DRCs), and by ensuring staff are split between production and recovery centres. However, movement restrictions under a nationwide MCO forced financial institutions to rely heavily on remote working arrangements to support split operations or alternative sites. At the height of the pandemic, staff working from home accounted for up to 70% of the total industry workforce. The enforcement of remote working arrangements and higher staff absenteeism due to quarantine measures also necessitated swift adjustments to business processes with a corresponding increase in unplanned IT needs for remote working. Therefore, financial institutions will need to review their risk assessments under a pandemic scenario to identify the potential impact on their resources, IT capacity and capability to support large-scale remote working arrangements and the increased usage of online banking services over a prolonged period.

ii. **Readiness for a full shutdown of the headquarters**
While BCPs generally contemplated the inability of financial institutions to access their main premises, some financial institutions struggled to swiftly shift their entire operations to alternate sites and/or remote working arrangements after the location of their headquarters or main offices were subjected to enhanced MCO (EMCO). The experience highlighted the need to improve continuity planning particularly to maintain effective controls over critical functions that are generally reliant on the physical presence of staff such as treasury operations, call centres and IT support. For example, financial institutions are setting up alternative controls to ensure the secure handling of customers' and other confidential information by call centres and treasury staff working from home, and preparing multiple alternative sites to locate critical staff who are not able to conducively perform their functions from home. Financial institutions also need to ensure that they maintain and regularly review their list of critical activities and staff, including pre-identified replacement staff who should be provided with continuous practical training to ensure their readiness to perform such activities at all times.

iii. **Reliance on critical third-party service providers**
The pandemic revealed instances in which the industry's increasing reliance on third-party service providers to support critical business operations had not been adequately acknowledged and addressed in financial institutions' BCPs. For instance, in the general insurance business, loss adjusters that are critical in assessing damage claims could not perform site visits, thus causing interruptions in the claims process. Many external IT vendors and support staff could not provide timely technical support as a result of movement restrictions, raising the risk of systems failure. Some banks also had to ration the issuance of replacement credit and debit cards, as they could not replenish their stock of cards. Financial institutions will need to holistically review their existing arrangements for communicating and coordinating with third-party service providers to secure assurances on the state of BCP preparedness of these entities, and assess their own ability to move critical functions in-house or to alternative service providers when necessary.

**iv. Robustness of Security Operations Centre (SOC)**

In an environment of diverse and increasing connectivity to internal corporate networks, financial institutions require SOCs that are capable of monitoring their technology security postures. During the pandemic, connectivity notably increased due to greater reliance on remote working arrangements, higher number of end-point devices and external connections, and the rising volume of online financial transactions, thereby prompting financial institutions to review the capability and coverage of SOC surveillance. For SOCs managed by a third party, BCPs will also need to incorporate appropriate contingency plans to ensure continued surveillance over cyber and end-point security.

## No spike in operational risk losses and incidents, but emerging risks warrant continued vigilance

Despite the operational challenges arising from the pandemic and MCO, operational risk losses have remained broadly stable. Nonetheless, the Bank and financial institutions remain vigilant to risks associated with operational adjustments that financial institutions have made to conform to new norms of physical distancing. These include:

- Increased exposures to cyber-attack risks arising from the implementation of teleworking arrangements and greater reliance on digital platforms;
- Risks of information leakage and data theft from operations conducted in home-based environments;
- Human error amid an anticipated increase in exception handling and manual interventions to minimise operational disruptions. Ineffective communication during split operations and changes to standard operating procedures may also increase risks of errors and omissions; and
- Potential cross infections at work premises following the gradual return of staff to the workplace amid a continuing threat of subsequent waves of COVID-19 infections.

## Payment and settlement systems maintained operational continuity without major disruptions

Malaysia's payment systems continue to operate smoothly without major disruptions, with the large-value payment system, Real-time Electronic Transfer of Funds and Securities System (RENTAS),[23] and retail payment systems maintaining high system availability above 99.9%. Enhancements to the payment systems that were successfully completed prior to the implementation of MCO further reduced the risk of disruptions. As a result, the number of incidents that caused isolated disruptions to RENTAS and retail payment systems declined significantly in 1H 2020 by 24% and 43%, respectively, compared to the same period last year. Despite an increase in payment transactions due to, among others, the surge in e-commerce activity and implementation of Government measures such as *Bantuan Prihatin Nasional*, both RENTAS and retail payment systems were able to meet the increased demands on capacity.

BCPs that included activating recovery centres, implementing split operations between various sites and enhancing remote access capabilities were effectively implemented by the payment system operators and have enabled continued operations with no major disruptions. The close coordination and communication between payment system operators and participants through the activation of Crisis Management Teams (CMTs) further ensured the timely implementation of corrective measures to minimise risks of potential disruptions. Similar to financial institutions, payment system operators are also enhancing their BCPs to reflect insights and lessons from the pandemic as part of ongoing measures to preserve operational continuity.

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