Response to feedback received
Business Continuity Management

Introduction

The Bank today finalised for issuance the policy document on *Business Continuity Management*. This policy document incorporates the proposals from the exposure draft issued in December 2021, and has taken into consideration feedback received during the consultation period.

The Bank received written responses from 108 respondents during the three-month consultation period.

Bank Negara Malaysia
19 December 2022

1. Interdependencies with service providers

Feedback received

Some respondents sought clarification on the rationale for requiring their Maximum Tolerable Downtimes (MTD) or Recovery Time Objectives (RTO) for their critical business functions (CBFs) and essential services to be incorporated into contractual arrangements with service providers (as per paragraph 9.35(b) of the PD on BCM). They cited that it may not be feasible to meet this requirement for all service providers.

The Bank's view:

1.1 The requirement in paragraph 9.35(b) of the PD on BCM enables a financial institution (FI) to proactively seek assurance from their key service providers on their continued ability to support the FI's CBFs and provision of essential services, as well as to meet the FI's business continuity objectives (i.e. the MTD and RTO). This will in turn facilitate prompt recovery of essential services and CBFs in events of disruption.

1.2 Where there are practical limitations to comply with this requirement, the Bank expects the FI to take reasonable measures to mitigate or reduce to the extent possible the impact of potential disruptions emanating from key service providers. These measures may include implementing redundancy, back-up arrangements or action plans for alternative service provider(s), taking into account the degree of difficulty, cost and time required to appoint the alternative service provider(s).

2. Business continuity plan (BCP), Disaster recovery plan (DRP) and Crisis management plan (CMP) testing

Feedback Received

The respondents agreed that annual testing of BCP, DRP and CMP is integral in evaluating the viability, robustness and effectiveness of an FI's BCM practices in the event of a disruption. However, some respondents requested for further guidance on the type and scope of testing exercises proposed in the exposure draft as detailed requirements were not prescribed.

Some respondents also sought clarification on arrangements for testing exercises during a prolonged crisis scenario where BCPs/DRPs/CMPs are activated for a long period (e.g. beyond a year).

The Bank's view:

2.1 The policy document outlines the requirements for annual testing of BCPs, DRPs and CMPs to evaluate the preparedness of a FI in responding to a disruption. In determining the type and scope of testing exercises, the FI should firstly be clear about the testing objectives of these exercises, and consider amongst others, their CBFs and essential services undertaken, the interlinkages between the CBFs, systems and infrastructure, and risk events that could disrupt the smooth functioning of their business operations. We generally expect the testing exercises to commensurate with the scale, nature and complexity of their respective business operations. In terms of frequency of testing, a FI may coordinate and streamline multiple testing exercises to be conducted concurrently. However, each exercise must be tested comprehensively to achieve the expected outcomes of these exercises.

2.2 During a prolonged crisis, a FI is expected to adapt their testing scenarios to enable them to respond effectively to new and evolving risks, taking into account ongoing lessons learnt and adjustments made to their operations during the crisis (e.g. prolonged split operations). This is to ensure that the FI adequately identifies, assesses and manages risks, and is in a state of readiness to respond to new disruptions. As the FI transitions back to business-as-usual conditions, the FI must consider these risks when reviewing and enhancing their BCP, DRP and CMP on a periodic basis.

3. Notification of Level of Disruption (LoD) and Cyber Incident Scoring System (CISS) to the Bank

Feedback Received

Some respondents sought clarification on the differences (particularly in terms of timeliness as well as extensiveness of information required) between

(a) the proposed LoD and CISS notification requirements, and

(b) the reporting requirements under the *Operational Risk Integrated Online Network* (more commonly known as ORION).

The Bank's view:

3.1 The objective of LoD and CISS notification requirements is to inform the Bank about the incident of disruption and its potential impact on financial stability and the smooth functioning of the financial sector. This also helps the Bank to consider whether a response at the industry level is required. Therefore, the LoD and CISS notification requirements are generally more timely, depending on the type of disruption, the potential impact of the disruption on the financial institution and the broader financial industry as a whole. The information required is also deemed sufficient to enable timely reporting and to facilitate informed assessments by the Bank.

3.2 As for the ORION, a FI is required to provide further information on the incident of disruption with more extensive indicators such as loss event data, key risk indicators and scenario analysis. This is to enable the Bank to use more extensive data points to facilitate its on-going supervisory review and assessments of the FI's operational risk management. Therefore, a FI is given more time to report these information to the ORION. The Bank is currently reviewing the requirements under the ORION which is expected to be superseded by the requirements under the Operational Risk Reporting (ORR) at a later date.

4. Delays to notification of Level of Disruption (LoD) and Cyber Incident Scoring System (CISS) to the Bank

Feedback Received

Some respondents raised concerns on the repercussions of delays in notifying the Bank within the proposed LoD and CISS notification timeline, as FIs may direct their focus on more pressing response during a disruption such as evacuation or rescue of life.

In addition, given the dynamic nature of a disruption, some respondents were concerned with the potential inaccurate notification to the Bank, as new or different information may come to light at a later stage.

The Bank's view:

4.1 The Bank recognises that a FI will need to promptly deploy their resources to attend to the disruption in order to ensure continued functioning of their CBFs and availability of essential services to the public. However, it remains the responsibility of the FI to promptly notify the Bank on the nature of the disruption for the reasons highlighted in 3.1 above.

4.2 The Bank does not intend to pursue punitive actions as first resort against financial institutions for inaccurate or delayed notifications to the Bank. Nevertheless, the Bank will conduct ongoing supervisory engagements and reviews on the FI's BCM practices, and may consider a broader use of its supervisory tools as appropriate.