BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Business Continuity Management

Applicable to−

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers
5. Licensed takaful operators
6. Prescribed development financial institutions
7. Operators of designated payment systems
8. Approved issuers of electronic money

Issued on: 19 December 2022 BNM/RH/PD 028-126

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Operational resilience of financial institutions is critical to ensure continuity in the provision of financial services through periods of disruptions, maintain orderly market conditions and sustain public confidence in the financial system.

1.2 Business continuity is an integral pillar of operational resilience. Business continuity management (BCM) entails an enterprise-wide framework, policies and processes that enable financial institutions to respond, recover and resume operations of critical business functions from operational disruptions that arise from internal or external risk events. Effective BCM can minimise operational, financial and reputational risks that can materially impact financial institutions.

1.3 This policy document aims to–

(a) facilitate the development and implementation of a robust BCM framework, policies and processes by financial institutions which are integrated with their overall risk appetite and reinforce sound risk management practices;

(b) strengthen the capacity and preparedness of financial institutions to respond and recover from operational disruptions; and

(c) preserve the continuity of critical business functions and essential services within a specified timeframe in the event of an operational disruption.

2 Applicability

2.1 This policy document is applicable to financial institutions as defined in paragraph 5.2.

2.2 For a financial institution operating as a foreign branch in Malaysia, the requirements in this policy document shall apply to the Malaysian branch with the following modifications:

(a) any reference to the board in this policy document shall refer to the governing body/committee of the foreign branch; and

(b) any reference to senior management in this policy document shall refer to the officers performing a senior management function of the branch.

3 Legal provisions

3.1 The requirements in this policy document are issued pursuant to−

(a) sections 47(1) and 143 of the Financial Services Act 2013 (FSA);

(b) sections 57(1) and 155 of the Islamic Financial Services Act 2013 (IFSA); and

(c) sections 41(1) and 116(1) of the Development Financial Institutions Act 2002 (DFIA).

3.2 The guidance in this policy document is issued pursuant to –
(a) section 266 of the FSA;
(b) section 277 of the IFSA; and
(c) section 126 of the DFIA.

4 Effective date

4.1 This policy document comes into effect on 19 December 2023, with the exception of the requirement on the testing of disaster recovery plan as specified in paragraph 9.48 which comes into effect on 19 December 2025.

4.2 A financial institution is permitted to implement requirements in paragraph 9.48 earlier than 19 December 2025.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, the IFSA or the DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purposes of this policy document−

"S" denotes a standard, an obligation, requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement actions;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"alternate site" refers to a site ready for use during a disruption to maintain the business continuity of the financial institution. A financial institution may have more than one alternate site. In some cases, an alternate site may involve facilities that are used for normal day-to-day operations but are able to accommodate additional business functions when a primary location becomes inoperable;

"board" refers to the board of directors of a financial institution, including a committee of the board where responsibilities of the board as set out in this policy document have been delegated to such committee;

"business continuity" refers to the ability of a financial institution to maintain continuity of its operations and services to its customers during an event of disruption;

"business continuity management" or **"BCM"** refers to an enterprise-wide framework that encapsulates policies, processes and practices that ensure the continuous functioning of a financial institution during an event of disruption. It also prepares the financial institution to resume and restore its operations and services in a timely manner during an event of disruption, thus minimising any material impact to the financial institution;

"business continuity plan" or **"BCP"** refers to a comprehensive action plan that documents the processes, procedures, systems and resources necessary to resume and restore the operations and services of a financial institution in the event of a disruption;

"business impact analysis" or **"BIA"** refers to the process of measuring the quantitative and qualitative impact to the operations and services of a financial institution in the event of a disruption. It is used to identify recovery priorities and recovery strategies that are critical to develop a business continuity plan;

"call tree" refers to a layered hierarchical communication model that graphically depicts the calling responsibilities and calling order used to contact senior management, employees, customers, vendors and other key contacts in the event of a disruption;

"communication protocol" refers to established procedures of communication for a financial institution to implement internally and those that were agreed in advance between a financial institution and external parties. Such procedures typically include the methodology for transmitting, writing, and reading of data, for example:

(a) phone calls and text messages;
(b) e-mails and intranet for employees;
(c) teleconferences or meetings with identified internal or external parties; or
(d) press releases, website postings, or news conferences for the public and other external stakeholders;

"crisis management plan" refers to a comprehensive action plan that documents the procedures and processes to support decision making by the crisis management team (CMT) in the event of a crisis. It includes criteria for activating the BCP and disaster recovery plan (DRP);

"critical business functions" or "**CBF**" refers to business functions undertaken by a financial institution, where the failure or discontinuance of such business functions is likely to–

(a) critically impact the financial institution financially or non-financially; and
(b) disrupt the provision of essential services to its customers;

"**cyber incident**" refers to an event that-
(a) jeopardises the cyber security of an information system;
(b) jeopardises the information the system processes, stores or transmits; or
(c) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or otherwise;

"disaster recovery plan" or **"DRP"** refers to a comprehensive action plan that documents the procedures and processes that are necessary to recover and restore information technology systems, applications and data of a financial institution in the event of a disruption;

"disruption" refers to an incident, whether anticipated or unanticipated, that causes degradation to the normal performance of a business function that would affect a financial institution's ability to continue its operations and services to its customers;

"essential services" refers to financial services that are essential to support financial intermediation activities which must continue to be provided by a financial institution in the event of a disruption;

"financial institution" refers to–
(a) a licensed person under the FSA and IFSA;
(b) a prescribed institution under the DFIA;
(c) an approved issuer of electronic money which is an eligible issuer of e-money as defined in the policy document on *Interoperable Credit Transfer Framework*[1]; and
(d) an operator of a designated payment system;

"full-blown test", for the purpose of gauging load handling and capacity of a recovery site, refers to an extensive and thorough exercise that involves large or wide scope or scale of testing of all systems, including network infrastructure and connectivity using production data and resources at recovery sites. Where necessary, business operations are shifted to the recovery site in accordance with the DRP;

"integrated testing" refers to an exercise conducted on multiple inter-related components of a BCP, either under a simulated or live operating environment. Examples of inter-related components may include intra-group entities, inter-dependent business functions, departments or interfaced systems;

"key service provider" refers to an entity, including an affiliate, providing services to a financial institution under an outsourcing agreement that supports the critical business functions.

[1] For ease of reference, an "eligible issuer of e-money" is defined as an approved issuer of electronic money with substantial market presence based on the criteria set out in Appendix 1 of the policy document on *Interoperable Credit Transfer Framework* or such other criteria as may be specified by the Bank from time to time.

"live-run test" refers to a comprehensive exercise that involves the use of production data and resources for testing on recovery sites in a live environment;

"maximum tolerable downtime" or **"MTD"** refers to a timeframe allowable for a recovery to take place before a disruption compromises the critical business functions of a financial institution;

"recovery site" refers to a recovery or backup site for systems as an alternate to the primary data centre which may also be known as a disaster recovery (DR) site. Examples of arrangement at recovery sites include–

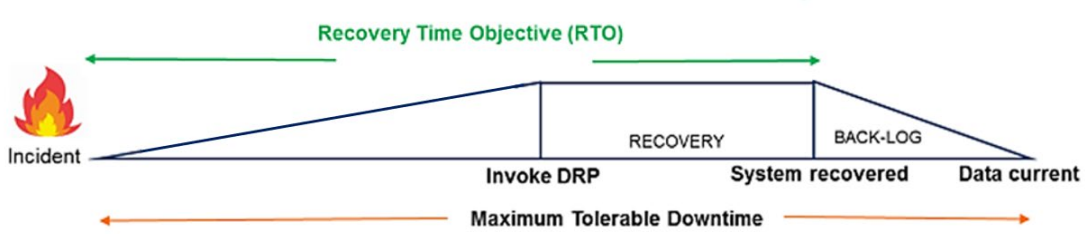
(a) replacement – do nothing but replace the system after a disaster;
(b) cold site – complete data centre infrastructure but without equipment;
(c) warm site – capable of providing backup operating support but would require the restoration of current data at minimum;
(d) hot site – fully equipped, operationally ready data centre;
(e) reciprocal arrangement – mutual back-up between entities;
(f) full redundancy – dual production systems configuration, where the production system is duplicated at recovery site; and
(g) commercial recovery facility – subscribe to a site provided by a service provider;

"recovery strategy" refers to a strategy that sets out the recovery objectives and priorities of a financial institution in the event of a disruption, and is developed based on the risk assessment, business impact analysis and critical business functions of the financial institution. It establishes, amongst others, targets on the level of service the financial institution would seek to deliver in the event of a disruption and the framework for ultimately resuming and restoring its business operations fully;

"recovery time objective" or **"RTO"** refers to the timeframe required for systems and applications of a financial institution to be recovered and operationally ready to support its critical business functions after a disruption. A recovery time objective has the following two components:

(a) the duration of time from the disruption to the activation of the BCP; and
(b) the duration of time from the activation of the BCP to the recovery of the business operations;

(See illustration below)



"risk assessment" or **"RA"** refers to the process of identifying risks that may disrupt the operations of a financial institution, assessing the critical business functions, defining the controls in place to reduce the exposure and evaluating the costs for such controls. Risk assessment and analysis often involve an evaluation of the likelihood or probabilities of a particular event of disruption.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant legal instruments and policy documents that have been issued by the Bank and as may be specified or amended by the Bank, in particular–

(a) *Corporate Governance* issued on 3 August 2016;
(b) *Corporate Governance for Development Financial Institution* issued on 13 December 2019;
(c) *Data Management and MIS Framework* issued on 29 August 2011;
(d) *Data Management and MIS Framework for Development Financial Institutions* issued on 5 November 2012;
(e) *Interoperable Credit Transfer Framework* issued 23 December 2019;
(f) *Operational Risk* issued on 10 May 2016;
(g) *Operational Risk Integrated Online Network (ORION)* issued on 25 February 2021;
(h) *Outsourcing* issued on 23 October 2019;
(i) *Recovery Planning* issued on 28 July 2021;
(j) *Risk Governance* issued on 1 March 2013;
(k) *Risk Management in Technology (RMiT)* issued on 19 June 2020; and
(l) Letter on the *Implementation of Financial Stability Board's Cyber Lexicon and Bank Negara Malaysia's Cyber Incident Scoring System for the Financial Institutions* issued on 28 September 2020.

7 Policy documents and circulars superseded

7.1 This policy document supersedes the following:

(a) *Guidelines on Business Continuity Management (Revised)* issued on 3 June 2011;
(b) *Disaster Recovery Readiness for Critical Systems and Services* issued on 14 February 2020;
(c) Letter on *Preparedness for Influenza Pandemic (H1N1)* issued on 8 July 2009;
(d) Letter on *Preparedness for Cyber Threat* issued on 16 June 2011;
(e) Letter on *Preparedness for Disruptions from Planned Rally* issued on 8 July 2011; and
(f) Circular on *Preparedness for Monsoon Floods* issued on 24 November 2011.

PART B POLICY REQUIREMENTS

8 Responsibilities of the board and senior management

S 8.1 The board and senior management's roles on the business continuity of a financial institution are vital. The board and senior management must be responsible for the effective oversight and implementation of the BCM framework that is integrated with the overall risk management framework of the financial institution[2].

S 8.2 In fulfilling its responsibilities under paragraph 8.1, the board must–

(a) establish a clear risk appetite and risk management strategy governing the BCM framework;

(b) approve the BCM framework of the financial institution and ensure subsequent reviews are conducted at least annually;

(c) establish a sound internal governance structure that provides effective oversight over the implementation of the BCM framework, consistent with the overall business strategy and risk appetite of the financial institution;

(d) ensure sufficient management capacity and resources, including budget and staff, are allocated to support an effective BCM framework; and

(e) instil a strong organisational culture that embeds the BCM framework in the strategy and business operations of the financial institution.

S 8.3 In fulfilling its responsibilities under paragraph 8.1, the senior management must–

(a) develop and ensure effective implementation of the BCM framework including relevant strategies and practices, commensurate with the operational environment, business activities and inherent risks of the financial institution;

(b) clearly define the roles and responsibilities of staff, functions and committee referred to in paragraphs 8.4 and 8.5 accountable for the BCM framework of the financial institution;

(c) ensure regular testing of the BCM framework;

(d) review the BCM framework at least annually, to ensure that it is up-to-date, effective and appropriate to the scope, nature and complexity of the operations of the financial institution;

(e) allocate sufficient resources to effectively implement and maintain the BCM framework;

(f) ensure the BCM framework is embedded in the strategy and business operations of the financial institution;

(g) ensure adequate organisational understanding of the BCM framework and that all levels of staff are well equipped to perform their roles;

[2] This includes putting in place appropriate governance requirements and allocating sufficient time to discuss cyber-related issues, as described in paragraph 8 of the policy document on *Risk Management in Technology (RMiT)*.

(h) maintain adequate documentation of the BCM framework (including its implementation) and make available such documentation to the Bank upon request;
(i) communicate with the board regularly to address strategic issues and concerns with regard to the BCM framework in a timely manner; and
(j) timely notify the Bank in writing on developments concerning the BCM framework that result, or could result, in a material adverse impact to the financial institution.

S 8.4 A financial institution must ensure that a committee is accountable for the development and implementation of the BCM framework. The committee must be led by a member of senior management and comprise members with relevant expertise. The committee must ensure robust deliberations on matters related to the BCM framework with timely escalation to the board.

G 8.5 For the purpose of paragraph 8.4, a financial institution may place the accountability on an existing committee or establish a dedicated BCM committee to facilitate the deliberations and decision-making on matters relating to the BCM framework.

G 8.6 A financial institution may also consider the establishment of a BCM function either as a standalone function or part of other functions, commensurate with its size, nature, complexity and risk profile. The BCM function may be supported by BCM coordinators, whose roles and responsibilities may include the following:
(a) coordinate and facilitate the implementation, testing and review of BCM framework with the relevant functions or departments;
(b) report to the committee referred to in paragraph 8.4 regularly on the progress of implementation and issues relating to BCM framework; and
(c) coordinate actions on BCM and recovery in the event of a disruption.

S 8.7 A financial institution must set up a Crisis Management Team (CMT) that comprises key representatives of the senior management to make key decisions during a crisis. The financial institution must ensure that the governance, processes and criteria/riggers to activate the CMT are set out clearly and are integrated with the BCM and risk management frameworks of the financial institution to preserve overall operational resilience. The CMT must undertake the following roles and responsibilities:
(a) assume the central role to assess and monitor the severity and impact of the disruption;
(b) make management decisions in response to the disruption;
(c) lead and oversee the implementation of business continuity and disaster recovery plans;
(d) communicate with internal and external stakeholders; and
(e) report to the board on the status of disruption and recovery efforts.

S 8.8 The internal audit of a financial institution is responsible for providing an independent assessment of the BCM framework. In fulfilling its responsibilities, the internal audit must–

(a) cover BCM as an audit area in its overall audit plan[3];
(b) ensure that the scope of audit on BCM is sufficiently comprehensive and cover all critical business functions;
(c) participate as independent observers during the development and testing of the CMP, BCP and DRP to provide an independent evaluation of the testing preparation and performance;
(d) undertake periodic review of the post-test analysis report of CMP, BCP and DRP as required in paragraph 9.53;
(e) establish follow-up, monitoring and escalation processes for audit issues related to BCM to the relevant oversight functions such as the board audit committee; and
(f) make available the audit reports on BCM to the Bank upon request.

G 8.9 A financial institution may engage an independent party[4] to audit the BCM framework.

S 8.10 In addition to this policy document, a financial institution must also comply with guidelines, requirements and standard operating procedures in relation to BCM issued by other relevant authorities.

S 8.11 For purposes of paragraph 8.10, where there are requirements on the same subject matter, a financial institution must comply with the more stringent requirements, as the case may be.

9 BCM framework and methodology

Risk assessment (RA), business impact analysis (BIA) and critical business functions (CBF)

S 9.1 A financial institution must undertake RA to identify potential risks that may cause business disruptions and result in the financial institution not being able to fulfil its business obligations, and assess the likelihood of the occurrence of these threats.

S 9.2 In performing the RA, a financial institution must consider the potential loss or diminished availability of the following resources during a disruption:

(a) key staff (including decision makers and recovery staff);
(b) office premises (including branches that are domiciled locally or abroad) and facilities within the same or adjacent geographical location or region;
(c) critical business information and records;

[3] Based on its internal audit methodology (which will inform the audit frequency).
[4] Refers to a separate department, unit, individual or external party that is free from any conflict of interest or potential conflict of interest that could impair the ability to provide an objective assurance and/or assessments on the financial institution's BCM framework.

(d) IT systems and infrastructure as well as other support facilities (including network devices and peripherals); and
(e) services of service providers.

S 9.3 A financial institution must also undertake BIA to assess the potential impact of various disruption scenarios to the financial institution.

G 9.4 For purposes of paragraph 9.3, examples of possible scenarios that may cause operational disruption are listed in Appendix 1.

S 9.5 In performing the BIA, a financial institution must assess the financial and non-financial impacts to the financial institution due to the unavailability of critical business functions, resources and infrastructure during a disruption for a specific period of time, including prolonged periods as a result of high absenteeism or movement restrictions.

S 9.6 In performing the RA and BIA, a financial institution must include the following consideration:
(a) the likelihood and impact of multiple operational risk events occurring at the same time, for example a cyber-attack that happens during a pandemic or natural disaster;
(b) the evolving nature of operational risks and how these risks transmit and impact the business operations; and
(c) interactions between different risk factors and scenarios.

S 9.7 Based on the outcome of the RA and BIA, a financial institution must identify its CBFs and establish priorities for recovery.

G 9.8 In determining CBFs, a financial institution may be guided by business functions which involve the following:
(a) large-value and time-sensitive payment instructions;
(b) clearing and settlement of material transactions;
(c) fulfilment of material end-of-day funding and collateral obligations;
(d) management of customers' risk positions;
(e) provision of essential banking services and payment services such as cash withdrawals, deposits and fund transfers through various delivery channels that are necessary to maintain public confidence;
(f) provision of essential insurance or takaful services; and
(g) provision of other services that may have systemic impact to other market participants or financial system.

S 9.9 A financial institution must review its RA and BIA at least annually and when there are material changes to its CBFs driven by internal or external developments.

Maximum tolerable downtime (MTD) and recovery time objective (RTO)

S 9.10 Based on the RA and BIA performed, a financial institution must determine the business continuity objectives for CBFs that correspond to varying levels of disruption as defined in paragraph 10.2. The business continuity objectives, which include the MTD and RTO, must -

(a) be consistent with the overall risk appetite and risk management framework of the financial institution;

(b) commensurate with the nature, scale and complexity of business functions and the inter-dependencies between functions;

(c) correspond with the importance and criticality of the business functions; and

(d) include procedures and the minimum level of resources required to recover the CBFs within the MTD and RTO.

S 9.11 A financial institution must set shorter MTD and RTO for business functions that have significant impact on customer services such as those listed in paragraph 9.14.

S 9.12 In determining the MTD and RTO, a financial institution must ensure that:

(a) RTO does not exceed MTD; and

(b) MTD and RTO facilitates the prompt recovery of essential services and CBFs that pose systemic impact to financial stability.

S 9.13 A financial institution must maintain proper documentation of business continuity objectives internally, which is to be made available to the Bank upon request.

Essential services

S 9.14 A financial institution must ensure continued availability of its essential services during a disruption. Depending on its core business, these essential services include–

(a) self-service terminals at accessible locations such as automated teller machines (ATMs) and cash deposit machines;

(b) online services such as electronic banking, mobile banking, trading platforms, payment card services, money changing, fund transfers and electronic money services;

(c) call centres or customer contact centres;

(d) issuance of guarantee letters for medical insurance or medical takaful coverage, claim processing and issuance and renewal of insurance policies and takaful certificates; and

(e) authorisation, clearing and/or settlement of payment transactions.

S 9.15 To ensure continued availability of the essential services, a financial institution must have in place contingency arrangements to provide these essential services during a disruption and incorporate these arrangements in the BCP. This includes services which are performed by service providers on behalf of the financial institutions under outsourcing arrangements.

G 9.16 For the purpose of paragraph 9.15, examples of measures that can be taken are listed in Appendix 2.

S 9.17 A financial institution must maintain proper documentation and records of all identified essential services, as well as the business functions, processes and systems that support these essential services, which are to be made available to the Bank upon request.

Recovery strategy

S 9.18 A financial institution must have in place a comprehensive recovery strategy that encompasses:

(a) recovery objectives that take into account its risk appetite and nature, scale and complexity of its business operations;
(b) recovery priorities that correspond to the recovery objectives and criticality of its business functions;
(c) maximum time for recovery for its essential services, including MTD and RTO;
(d) adequacy and capability of infrastructure to support recovery (including functional relocation, alternate site and recovery site, modes of processing, work area, data and facility); and
(e) adequacy and capability of staff to support recovery (including recovery staff and decision makers).

S 9.19 In developing a recovery strategy, a financial institution must ensure that its strategy and responses comply with the legal and regulatory requirements of relevant authorities and government ministries or agencies.

Crisis management plan (CMP), business continuity plan (BCP) and disaster recovery plan (DRP)

S 9.20 Based on the recovery strategy, a financial institution must formulate robust and consistent CMP, BCP and DRP to guide recovery actions for all CBFs, including those for domestic and overseas branches or subsidiaries, in the event of a disruption. These plans are interlinked and may be activated simultaneously depending on the nature and extent of the disruption.

S 9.21 For purposes of paragraph 9.20, the BCP and DRP must include–

(a) governance, processes and criteria to activate the BCP and DRP;
(b) roles and responsibilities of the BCM function and recovery staff, including their alternates;
(c) procedures to be followed in response to a disruption to business operations, in order to respond swiftly to a crisis situation, recover or resume CBFs, resources and infrastructure within the stipulated timeframe;
(d) escalation, declaration and notification procedures, including call trees and contact lists;
(e) a list of all resources required to recover CBFs in the event of a disruption. This would include, but is not limited to, key recovery staff, systems,

computer hardware and software, office equipment and relevant documentation;

(f) relevant information about the alternate site and recovery site; and

(g) procedures for restoring normal business operations. This would include, but is not limited to, orderly entry of all business transactions and records into relevant systems and completion of all verification and reconciliation procedures.

S 9.22 A financial institution must also develop a CMP[5] to guide and support the decision making by the CMT. The CMP must include the following:

(a) the governance, processes and triggers to activate the CMT;

(b) the roles and responsibilities of the CMT members;

(c) identification of key internal and external stakeholders and their expected roles and involvement in managing a crisis;

(d) methodology to be used by the CMT to assess impact of a crisis and guide actions to be taken (including ensuring staff safety, incident containment, evacuation and other crisis management procedures);

(e) clear criteria for activation of BCP, DRP and alternate site;

(f) clear process on–

(i) information gathering and status update to the CMT;

(ii) timely internal and external communications; and

(iii) supporting the CMT's oversight on the recovery and restoration efforts;

(g) proper records of decisions made during a crisis; and

(h) potential responses in the event that the duration of a crisis is prolonged[6].

S 9.23 A financial institution must take into account the factors in paragraph 9.6 when reviewing the effectiveness and feasibility of CMP, BCP and DRP.

S 9.24 A financial institution must ensure that its CMP, BCP and DRP provide for all outsourcing arrangements and comply with the relevant requirements in the policy document on *Outsourcing*.

S 9.25 To enhance the effectiveness of BCM, a financial institution must incorporate the following requirements and clauses in contractual and outsourcing arrangements with key service providers, suppliers and counterparties:

(a) require the key service provider, supplier and counterparty to have in place sound and effective BCP for the outsourced arrangement, including specific MTD and RTO requirements that align with the financial institution's MTD and RTO, and provisions for legal liability if MTD or RTO requirements are not met;

(b) require the key service providers to participate in the financial institution's integrated testing, as stipulated in paragraph 9.50(d);

(c) allow the internal audit of the financial institution or other independent party appointed by the financial institution to review the BCM of the key service provider, supplier and counterparty; and

[5] For cyber-related incidents, refer to paragraph 11.22 of policy document on *RMiT.*

[6] The financial institution must take into consideration new or unprecedented risks (e.g. prolonged split operations or remote working).

(d) allow the financial institution to have access to all relevant records and information maintained by the key service provider, supplier and counterparty with respect to the outsourced arrangement.

S 9.26 A financial institution must have in place processes to perform periodic reviews, validations and updates on the components of its BCM framework to ensure their continued relevance and effectiveness towards the evolving changes in the operating environment, business activities and risks, and to address gaps identified from testing exercises.

S 9.27 In the event of an operational disruption, a financial institution must conduct a post-event review on the effectiveness of its CMP, BCP and DRP. The report must be communicated to the board and senior management for actions to be taken to address any identified gaps.

G 9.28 A financial institution is strongly encouraged to adopt systematic version control[7] for BCP, DRP and CMP, to facilitate updating and maintenance of the plans.

Crisis communication

S 9.29 A financial institution must formulate a crisis communication strategy and a crisis communication plan, which is incorporated in its CMP.

S 9.30 In the crisis communication plan, a financial institution must include–

(a) a list of all relevant internal and external stakeholders that the financial institution plans to communicate with, in the event of a crisis, and the corresponding prioritisation and timeline of the communication;
(b) designated contact person(s) to lead the communication with internal and external stakeholders;
(c) broad messages that will be included in the communication statements to the different internal and external stakeholders based on the different disruption scenarios;
(d) the appropriate communication protocol that must be adhered to; and
(e) the communication channels, including the alternative channels that can be used when the primary communication channel is unavailable.

G 9.31 For purposes of paragraph 9.30, examples of stakeholders may include–

(a) staff, parent company, head office, branches and subsidiaries of a financial institution; and
(b) regulatory authorities, investors, customers, participants of designated payment systems, counterparties, business partners, service providers, media and the public.

S 9.32 A financial institution must ensure that its crisis communication provides clarity to its stakeholders on the business continuity and recovery actions that would be taken to restore the CBFs and essential services.

[7] Refers to records of all changes made over time.

S 9.33 A financial institution must establish a communication protocol which include–
(a) the nature and content of information to be shared with each stakeholder; and
(b) the classification of the sensitivity of information to be shared with each stakeholder, consistent with the information security classification of the financial institution.

Interdependencies

S 9.34 A financial institution must have in place processes[8] to identify and assess various internal and external interdependencies[9] (within and outside of the financial institution) that are necessary for the CBFs to operate, to minimise gaps and blind spots in BCM.

S 9.35 Where interdependencies exist, a financial institution must–
(a) understand and assess the impact of interdependencies in its RA, BIA and CBF assessments;
(b) incorporate consistent, specific and measurable MTDs and RTOs in the relevant contractual and outsourcing arrangements;
(c) take into account interdependencies when developing crisis response, recovery strategy, CMP, BCP and DRP and resource planning;
(d) set out explicit plans, frequencies and scope for integrated testing and BCM exercises with the relevant and interdependent stakeholders; and
(e) ensure consistent crisis communication among related stakeholders, where relevant.

S 9.36 For a financial institution that is a part of a financial group, the financial institution, when developing its BCM framework, must–
(a) take into account the reporting structure within the financial group and the interdependencies of the entities within the financial group, such as dependencies on shared functions;
(b) ensure consistency of its assessment, crisis response and BCM strategy for similar risks between the entities within the financial group; and
(c) develop a consistent crisis communication strategy for the entities within the financial group.

Alternate site and recovery site

S 9.37 A financial institution must set up its alternate site and recovery site that can be used if the business premise, infrastructure or systems supporting the CBFs become unavailable in the event of a disruption.

[8] This includes the mapping of people, processes and technologies (and their interdependencies), which are necessary to support the CBFs.
[9] External interdependencies include dependencies on intragroup companies, suppliers, counterparties and service providers (e.g. trading platforms, data/information storage, telecommunication network and power utilities).

G 9.38 For purposes of paragraph 9.37, examples of an alternate site and a recovery site include in-house arrangements, or available through agreement with service providers, or a combination of both options.

S 9.39 A financial institution must assess the suitability and capacity of the alternate site and recovery site to ensure that the sites are–

(a) sufficiently distanced from the primary site to minimise the risk of being affected by the same source of disruption;

(b) using separate or alternative telecommunication network and power grid from the primary site to minimise the risk of single point of failure;

(c) readily accessible and available for occupancy, taking into consideration the logistic requirements within the recovery timeframe stipulated in the BCP and DRP; and

(d) functional and able to meet technological and resource requirements, and are commensurate with the criticality of the business functions.

S 9.40 For technology requirements, a financial institution must ensure that the IT systems and telecommunications network at the recovery site are–

(a) compatible with the primary systems of the financial institution in terms of capacity and capability to adequately support the CBFs; and

(b) continuously updated with the latest version of systems and application software to align with the system configurations of the financial institution, including hardware and software upgrades or modifications.

S 9.41 Where the alternate site or recovery site is managed or owned by a third party, a financial institution must ensure its outsourcing arrangements are in accordance with the policy document on *Outsourcing*, particularly the following:

(a) execution of a service level agreement (SLA) between the financial institution and the third-party provider to ascertain the level and type of services to be provided to the financial institution in order to safeguard the interest of the financial institution;

(b) mitigation of concentration risks, where the alternate or recovery site provided, managed or owned by the third party will be utilised by several customers or to customers within the same locality or industry. In this regard, the SLA must specifically identify the conditions under which the alternate or recovery site may be used and specify how customers would be accommodated if simultaneous disruptions affect several customers of the service provider;

(c) assessment of the capacity and capability of the service provider for use for a reasonably prolonged period;

(d) adequacy of physical and logical access controls provided by the service provider to safeguard the alternate or recovery site; and

(e) periodic test, continuous review and monitoring on the level and type of service provided and the risk mitigation measures maintained by the financial institution.

Critical business information records

S 9.42 A financial institution must maintain and safeguard critical business information records that are crucial in providing essential services.

S 9.43 A financial institution must have in place proper processes and controls to safeguard critical business information and ensure that they are readily accessible to facilitate recovery of CBFs in the event of a disruption.

Testing and exercises

S 9.44 A financial institution must have in place a rigorous testing program to evaluate the functionality and effectiveness of its BCM, readiness of staff and adequacy of resources in an event of a disruption. The testing program must cover the CMP, BCP and DRP of a financial institution.

S 9.45 In the testing program, a financial institution must determine the type and frequency of testing for its CBFs.

G 9.46 The type of testing may cover functional tests such as simulated test, live-run test or full-blown test, and non-functional tests such as call tree or desktop exercise.

S 9.47 A financial institution must conduct periodic testing of the following, at least annually:
(a) BCP for all CBFs;
(b) DRP for all critical application systems; and
(c) CMP.

S 9.48 For the purpose of paragraph 9.47(b), a financial institution must ensure the following aspects of the DRP are tested:
(a) a live-run test must be conducted on a business day with latest peak load and volume;
(b) a scenario of prolonged disruption for at least three consecutive business days must be tested from the recovery site; and
(c) all failed live-run tests must be re-tested within a year from the date of the failed tests.

S 9.49 The scope of testing conducted by the financial institution must be sufficiently comprehensive to cover the key components of the BCP and DRP as well as coordination and interfaces among important stakeholders. The testing requirements must include–
(a) verifying completeness of the plan and adequacy of recovery procedures;
(b) assessing familiarity of staff with their business continuity responsibilities and the evacuation procedures of the financial institution;
(c) evaluating the connectivity, functionality, performance and load capacity of the alternate site and recovery site;
(d) assessing adequacy of security implementation and ensuring staff awareness on such security implementation;

(e) assessing effectiveness of communication plan and coordination with relevant stakeholders; and
(f) evaluating response time of business recovery processes.

S 9.50 A financial institution must periodically conduct an integrated testing on a reasonable wide-scale basis for all the CBFs, including those undertaken by the key service providers, commensurate with its size, nature, complexity and risk profile. In doing so, the financial institution must–
(a) use backup IT systems to gauge and assess its application system linkages and network connectivity;
(b) calibrate the load or capacity requirements that are required to support minimum service levels to be provided during a disruption;
(c) include such calibrations in subsequent rounds of testing; and
(d) ensure participation of key service providers to evaluate their adequacy and readiness to respond to the recovery measures, that the financial institution needs to deploy during a disruption.

S 9.51 In designing and carrying out the testing, a financial institution must–
(a) develop test plans with predetermined test goals, scope and test evaluation criteria, using realistic simulations[10] and activity volumes;
(b) develop metrics to measure effectiveness of the BCP and DRP and the extent to which various business continuity objectives are met;
(c) develop necessary contingency measures in the event of failed testing to avoid business disruptions; and
(d) maintain formal testing documentation, including test plan, objectives, scenarios, procedures and results, for future reference and audit.

S 9.52 A financial institution must ensure that its senior management and staff with BCM responsibilities, including the designated alternates, participate in all relevant tests.

S 9.53 A financial institution must prepare a post-test analysis report to evaluate the testing outcomes against the testing goals. This is to ensure adequacy and integrity of testing, to identify problems and to develop the necessary corrective action plans. The test results and post-test analysis report must be communicated to the board in a timely manner and made available to the Bank upon request.

G 9.54 A financial institution is encouraged to participate in testing or exercises organised by government agencies, regulatory bodies and industry associations, to better understand the inter-dependencies between one another and improve overall business continuity capability during a period of disruption.

[10] The financial institution must take into consideration new and unprecedented risks from recent crises (e.g. movement control restrictions and prolonged remote working arrangements).

PART C NOTIFICATION OF DISRUPTIONS TO THE BANK

10 Notification of disruptions to the Bank

G 10.1 As financial institutions operate in an ever-changing environment, it is imperative for financial institutions to have the capability and capacity to promptly detect any disruptions that affect their CBFs and the extent that such disruptions permeate. Timely notification to the Bank will allow the Bank to gain an understanding of the nature of the disruptions and how these may potentially manifest. With this information, the Bank can intervene as early as possible where necessary (including the activation of an industry-wide crisis response, if required) to ensure financial stability is preserved.

Non-cyber incident

S 10.2 For a disruption that is not a cyber incident, a financial institution must categorise the level of disruption (LoD) that affect the CBFs based on the locality, as described below:

LoD	Description
1	• Affect CBFs; and • Affect isolated areas of the business operations such as a branch or department.
2	• Affect CBFs; and • Affect a number of branches or departments.
3	• Affect CBFs; and • Affect head office business premises
4	• Affect CBFs; and • Affect region or entire state where the institution operates. • May cause systemic impact
5	• Affect CBFs; and • Affect nationwide or regional.

S 10.3 For avoidance of doubt, where the disruption referred to in paragraph 10.2 is assessed by a financial institution to meet the description of multiple LoDs, the financial institution must categorise the disruption as the highest LoD.

S 10.4 A financial institution must notify the Bank of a disruption that is not a cyber incident within the respective timelines for the corresponding LoD, as set out in the table below:

LoD	Notification Timeline
1	Within 48 hours from the detection of the disruption for all information specified in the reporting template (Attachment 1) that is applicable to the disruption concerned
2	Within 24 hours from the detection of the disruption for all information specified in the reporting template (Attachment 1) that is applicable to the disruption concerned
3, 4, 5	(a) Within 2 hours from the detection of the disruption for mandatory information specified in the reporting template (Attachment 1); and (b) Within 12 hours after the initial notification referred to in paragraph (a) for all remaining information specified in the reporting template (Attachment 1) that is applicable to the disruption concerned.

Cyber incident

S 10.5 For all cyber incidents, a financial institution must notify the Bank within 2 hours upon the confirmation[11] of the disruption.

Requirements for all forms of disruptions

S 10.6 A financial institution must notify the Bank of all non-cyber and cyber incidents via the centralised email mylod@bnm.gov.my.

G 10.7 Where a financial institution is unable to notify the Bank via the centralised email as required in paragraph 10.6, the Bank may accept notification from the financial institution via alternative channels such as text messages or calls to the respective relationship manager(s) or office-in-charge in the relevant departments of the Bank.

S 10.8 Notwithstanding paragraph 10.7, a financial institution must comply with paragraph 10.6, as soon as the financial institution is able to do so.

S 10.9 As the information on disruptions could change as more details on the disruption come to light, a financial institution must progressively update the Bank with the latest information as it becomes available to facilitate appropriate response and intervention by the Bank, where necessary.

[11] Following a preliminary investigation to determine if the incident is cyber centric or originated from a cyber related root cause (e.g. ransomware, DDoS, data leak).

S 10.10 All notifications to the Bank as required above must be submitted in accordance with the following templates:

(a) Non-cyber incidents - Attachment 1: LoD Reporting Form; and

(b) Cyber incidents - Attachment 2: Cyber Incident Scoring System (CISS) Form.

APPENDIX 1 LIST OF POSSIBLE SCENARIOS LEADING TO OPERATIONAL DISRUPTION

The list below is non-exhaustive.

Scenario	Impact						
	Essential services facing customers	Customer data breach	Loss/ unavailability of staff	Loss/ unavailability of premises	IT systems	Service provider	Reputational impact
Nationwide/ district-wide war or riot							
Natural disaster (e.g. flood, earthquake, tsunami, haze)							
Fire							
Sabotage/ terrorism (e.g. bomb attack, arson)							
Epidemic/ pandemic (e.g. SARS, H1N1, COVID-19)							
Strike by employees							
Cyber attacks							
IT outage (prolonged)							
Power outage (prolonged)							

APPENDIX 2 EXAMPLES OF PRECAUTIONARY AND CONTINGENCY MEASURES TO SUPPORT PROVISION OF ESSENTIAL SERVICES

Preparedness for pandemic

1. Consider forming a multi-disciplinary pandemic team to monitor and implement BCP measures, and where possible, improve the BCP to cater for pandemic scenarios. The team may include representatives from the following functions:
   (a) BCP function;
   (b) key business functions;
   (c) information technology;
   (d) human resources; and
   (e) office administration.

2. Ensure adequate measures to ensure protection of staff against the infectious disease during the pandemic such as–
   (a) increasing staff awareness of the pandemic/infectious disease;
   (b) maintaining high standards for hygiene policies and preventive measures against infection;
   (c) responding to possible infection or incident of staff or visitor showing symptoms of infection in the workplace;
   (d) contact tracing and tracking of suspected or confirmed exposures of infected staff;
   (e) distributing personal protective equipment and medical supplies; and
   (f) updating evacuation and medical assistance procedure.

3. Establish split operations or remote working arrangements

4. Assess capabilities to operate remotely such as–
   (a) reviewing capacity readiness of electronic channels to handle a potential or sudden upsurge in the volumes of electronic transactions;
   (b) preparing for increased human resource demands in call centres;
   (c) reviewing readiness of policies and mobile computing equipment (e.g. laptop computers, landlines);
   (d) reviewing the existing arrangements with internet service providers to increase network bandwidth at short notice;
   (e) raising awareness about cybersecurity and information technology threats from remote working or telecommuting arrangements; and
   (f) upgrading remote system access capabilities (e.g. tele- and video-conferencing facilities), if needed.

Preparedness for disruption from social unrest

Heighten security at the financial institution’s branches especially in affected areas in the event of social unrest such as planned rally and riot.

Preparedness for natural disasters

1. Ensure safety protocols for staff and security measures to safeguard physical assets are in place to prevent casualties and property damage in the event of a natural disaster such as flood.

2. Ensure effective customer support and public communication that may include pre-emptive alert on potential affected areas, alternate branches and availability of the customer services/call centres.