GUIDING PRINCIPLES ON BUSINESS CONTINUITY MANAGEMENT

1.0 Introduction

1.1 An effective business continuity management provides a holistic approach for financial institutions to manage and minimise the operational, financial, legal, reputational and other material consequences arising from operational disruption. It helps to ensure the restoration of the information technology infrastructure and timely recovery and resumption of critical business functions for the fulfilment of business obligations.

1.2 The recent pandemic and various widespread natural disasters have served to magnify the priority for financial institutions to manage their business effectively through a comprehensive, relevant and effective business continuity management.

1.3 The *Guiding Principles on Business Continuity Management* (the Guiding Principles) is consistent with the expectations on business continuity as required by the international standards set by the:

(i) Basel Committee on Banking Supervision;

(ii) International Association of Insurance Supervisors;

(iii) International Organisation of Securities Commissions; and

(iv) Group of International Financial Centre Supervisors[1].

2.0 Regulatory Expectation

2.1 The Guiding Principles outlines the regulatory expectation on the business continuity requirements to be observed by Labuan financial institutions (LFIs).

[1] Standard on the Regulation of Trust Company and Corporate Service Providers

2.2 The application of the principles is to be achieved by the LFIs through the minimum requirements of the Guiding Principles and be complemented by the recommended best practice standards:

(i) Minimum requirements must be complied with by all LFIs. For completeness, these applications may refer to relevant regulatory requirements of other existing guidelines that have been issued by Labuan FSA, but are included in the Guiding Principles to ensure cohesiveness in their collective application; and

(ii) The best practice applications are broad guidance on other advanced applications of the BCM commonly observed in international markets. This includes BCM recommendations of the International Organization for Standardization (ISO). Although these best practices are not made mandatory, LFIs are encouraged to adopt them as their business operations grow and mature over time.

2.3 While LFIs are expected to observe the principles prescribed by the Guiding Principles, the nature and extent of measures to be effected by individual LFIs should be proportionate to the nature of their business operations.

3.0 Applicability

3.1 The Guiding Principles is applicable to the following LFIs:

(i) Labuan banks and investment banks licensed under Part VI of the Labuan Financial Services and Securities Act 2010 (LFSSA);

(ii) Labuan Islamic banks and Islamic investment banks licensed under Part VI of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA);

(iii) Labuan insurers and reinsurers licensed under Part VII of the LFSSA;

(iv) Labuan takaful and retakaful operators licensed under Part VII of the LIFSSA;

(v) Labuan captive insurance business and Labuan captive takaful business licensed under Part VII of the LFSSA and Part VII of the LIFSSA, respectively;

(vi) Labuan insurance-related companies and Labuan takaful-related companies licensed under Part VII of the LFSSA and Part VII of the LIFSSA, respectively;

(vii) Labuan fund managers licensed under Part III of the LFSSA and Part IV of the LIFSSA;

(viii) Labuan securities licensees and Islamic securities licensees licensed under Part IV of the LFSSA and Part V of the LIFSSA, respectively;

(ix) Labuan trust companies including Labuan managed trust companies licensed under Part V of the LFSSA; and

(x) Labuan exchanges approved under Part IX of the LFSSA.

3.2 Notwithstanding paragraph 3.1, Labuan FSA reserves the right to direct other LFIs to observe the requirements of the Guiding Principles which may be specified from time to time.

3.3 The ability to harness potential group synergies and expertise has the benefits of cost-rationalisation and efficient deployment of intra-Group resources. In this regard, the LFI may leverage on and adopt its group or head office's business continuity management practices as long as the approach is no less stringent than the requirements of the Guiding Principles.

3.4 The Guiding Principles shall complement and to be read together with the requirements under the following Guidelines:

(i) Paragraph 5.2 (vii) of the *Guidelines on Corporate Governance for Labuan Banks and Labuan (Re)Insurers*;

(ii) Paragraph 9.11 to paragraph 9.16 of the *Guidelines on External Service Arrangements for Labuan Financial Institutions*;

(iii) Paragraph 45 of the *Prudential Framework of Corporate Governance for Labuan Insurance and Insurance-Related Companies*;

(iv) Paragraph 8.6 (iii) to paragraph 8.7 (ii) of the *Governance and Market Conduct Framework for Labuan Trust Companies*;

(v) Paragraph 8.6 of the *Guidelines on the Establishment of Labuan Fund Manager;* and

(vi) Paragraph 8.5 of the *Guidelines on the Establishment of Labuan Securities Licensee including Islamic Securities Licensee*.

4.0 Legal Provision

4.1 The Guiding Principles is issued pursuant to Section 4A of the Labuan Financial Services Authority Act 1996 (LFSAA) to specify the minimum regulatory expectations on the business continuity management for LFIs.

5.0 Effective Date

5.1 The Guiding Principles shall come into effect on **1 June 2021**, and would remain effective and applicable unless amended or revoked. Notwithstanding this, LFIs which wish to early adopt the requirements of the Guiding Principles are permitted to do so prior to the effective date.

6.0 Definitions

Business Continuity Management (BCM)	A whole-of-business approach that includes policies, standards and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption.
Business Continuity Plan (BCP)	As part of BCM, BCP is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of the LFI in the event of a disruption.
Business Impact Analysis	As part of BCM, business impact analysis is the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements, and essential staff and to help shape a BCP.
Recovery Objective	A pre-defined goal for recovering specified business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).
Call Tree	A layered hierarchical communication model used to notify specific individuals of an event; typically unplanned in nature as a means to co-ordinate recovery, if necessary. Also known as a phone tree, call list, phone chain, or text chain.

KEY PRINCIPLES

7.0 Responsibilities of the board and senior management

<u>Principle 1</u>: The board of directors and senior management are collectively responsible in ensuring that the LFI establishes and maintains a sound and effective BCM.

Minimum Requirements

7.1 The board of directors and senior management[2] are accountable to ensure that the BCM is appropriate taking into account the nature, scale and complexity of the LFI's operations.

7.2 The responsibility of the board and senior management also includes oversight on the effectiveness of the BCM and that sufficient resources are accorded to execute the BCM's activities including testing.

Best Practices

7.3 In order to promote an organisational culture that prioritises on business continuity, the Board and senior management may consider that the LFI:

(i) has a committee or a formal designation of business continuity responsibilities amongst the senior management officers to enable smooth planning and effective execution of the BCM; and

(ii) secures an independent external review of its BCM on periodic basis.

[2] For LFI operating as a branch, any reference made in the Guiding Principles in relation to the 'board' should refer to the LFI's regional/head office or an equivalent person, whichever is relevant while 'senior management' should refer to the Principal Officer (PO) of the branch or any officer performing a senior management function in respect of the branch operation.

8.0 Major operational disruptions and outsourcing risks

<u>Principle 2</u>: The risks emanating from major disruptions, concentration of critical business functions and outsourcing arrangements must be thoroughly identified, assessed and mitigated as part of the LFI's BCM.

Minimum Requirements

8.1 In undertaking the risk assessments as part of BCM, a systematic approach is needed to ensure smooth dealing of disruptions and swift response actions.

8.2 The LFI is required to identify and monitor any potential disruptions' risks to business operations which may include:

(i) financial and non-financial risks arising from internal and external factors;

(ii) risks that may arise from the interdependencies of critical business functions as well as the extent to which they depend on other parties;

(iii) concentration risks arising from centralisation of critical and support functions; and

(iv) outsourcing risks arising from the inability of the service provider to perform or serve the LFI's critical business functions.

8.3 The LFI is required to assess the level of severity of potential operational disruptions to its critical business functions. Any adverse impacts and implications of risks from the disruptions must be assessed adequately so that appropriate set of mitigating measures can be encapsulated in the BCM. By doing so, the BCM ensures the smooth and timely resumption of LFI's critical functions and operations in the event of a disruption.

8.4 The senior management must be regularly updated on business impact analysis as well as major changes (i.e. change in structure and organisation of people, process, technology and locations) that may affect the effectiveness of the LFI's BCM arrangements.

8.5 The LFI's business continuity and resumption plan for critical business functions must include measures to address the immediate consequences of a disruption, minimise the interruption period as well as maintain the level of services to relevant stakeholders.

Best Practices

8.6 The assessment and evaluation of potential operational disruptions severity may include:

(i) business impact analysis and identification of critical business functions or operations to be prioritised in LFI's recovery strategies. For this purpose, the LFI may keep the Board informed of the business impact analysis on ongoing basis. This is especially pertinent if there are significant changes that might affect the BCM procedures or protocols; and

(ii) probability assessment of a disruption taking into consideration the geographical locations of all facilities, their susceptibility to threats and the proximity to key infrastructure.

8.7 The LFI may enhance its policy response measures documentation by describing in detail the means of ensuring the continuity of its critical business functions and operations, at a minimum level of service and within an acceptable period.

9.0 Risk-based recovery strategy

<u>Principle 3</u>: The recovery objectives and strategies shall reflect the magnitude of the potential disruption risks to the LFI's critical business operation.

Minimum Requirements

9.1 The recovery objectives and strategies take into consideration the identification of recovery levels and recovery time for specific business lines to give assurance on the level of resilience and recovery timeframe during an operational disruption.

9.2 The LFI is expected to recover and resume its critical business functions within the recovery timeframe as specified in its BCP.

9.3 As part of the recovery strategies, any remote working arrangements such as the usage of the head office and group's facilities, co-located office[3] or work from home (WFH) can be considered as an alternative recovery arrangement. In this regard, the following parameters may be considered in effecting remote working arrangements:

(i) the core systems can be operated and accessed remotely in a safe and secure manner;

(ii) the critical functions and services can be recovered and carried out seamlessly within maximum tolerable downtime;

(iii) IT security controls and data confidentiality measures for remote working arrangement are in place and adhered by staff; and

(iv) the staff are equipped with the required skills and know-how to operate the systems remotely and recover the critical operations and services.

Best Practices

9.4 The LFI may have more than one recovery site as part of the expanded and additional BCM measures in the event where the primary site is inaccessible.

9.5 The LFI might reasonably be held to a within-the-day-of-disruption recovery time objective in the case of major operational disruptions resulting from discrete events, and generally be expected to recover critical operations and services in those affected areas.

[3] Only applicable to banks and (re)insurers that have been approved to have co-located offices.

10.0 IT Disaster Recovery Plan (DRP)

Principle 4: As part of BCM, an IT DRP for critical business functions and related technology infrastructure is needed to provide assurance to relevant internal and external stakeholders on LFI's preparedness in the event of a major disruption.

Minimum Requirements

10.1 The IT DRP must specify the LFI's recovery and restoration plan for technology services and infrastructure components such as data, systems, network, services and applications in the event of a major disruption.

10.2 In regard to the outsourced critical business functions, the LFI is required to seek the external service provider's annual assurance on its DRP preparedness. In this regard, the assurance from the external service provider may include key information on its DRP preparedness such as the:

(i) back-up arrangements are available and ready to be operated when necessary; and

(ii) external party service provider periodically tests its DRP and provides any test reports, including any identified deficiencies and measures to address such deficiencies as soon as practicable.

10.3 An alternative data centre including the cloud-based/ virtual data centre that is to be established by the LFI must commensurate with the capacities (including cyber security controls) maintained in the main data centre.

Best Practices

10.4 The LFI may have a dedicated personnel such as an IT manager to be responsible for maintaining and keeping the IT DRP and arrangements up-to-date.

11.0 BCM awareness and testing

<u>Principle 5</u>: A continuous organisation wide awareness and testing for business continuity and resumption plans is required to provide assurance on the LFI's BCM relevancy and effectiveness.

Minimum Requirements

11.1 A periodical awareness programme and testing shall be undertaken to inculcate awareness, familiarity and understanding among key personnel (including business continuity coordinators) of their roles and responsibilities in the event of a major operational disruption.

11.2 The testing for critical business functions shall be conducted in a timely, periodic basis to ensure that the BCM continues to be effective and relevant in tandem with the current internal and external developments.

11.3 The scope of the BCM's testing should be properly planned. The scope of BCM testing may include but not limited to:

(i) Desktop walk-through exercise to full system test;

(ii) Staff call-tree activation (with and without mobilisation);

(iii) Back-up site to back-up site exercise (including with external service providers);

(iv) Alternative arrangements of shared services;

(v) Back-up storage medium restoration; and

(vi) Retrieval of vital records.

11.4 The LFI should retain a formal documentation of the testing results as well as the post-mortem reviews of the testing programme. The effectiveness of the testing is required to be communicated to the Board, as far as practicable.

Best Practices

11.5 The documentation relating to the BCM testing programme and results may be verified and sign-off by the senior management.

11.6 To ensure the BCM is frequently reviewed on its effectiveness, the LFI may:

(i) undertake a comprehensive BCM testing on an annual basis;

(ii) conduct a thematic testing such as periodic testing of call tree to enhance the escalation and communication process within the LFI; and

(iii) participate on joint testing with the external party service provider as part of a comprehensive testing to enable an end-to-end BCP or IT DRP test, where it is reasonably practicable to do so.

12.0 Communications

Principle 6: An effective communication plan for internal and external stakeholders in the event of a major operational disruption is incorporated into the BCM to address the reputational risks.

Minimum Requirements

12.1 The LFI's communication plan includes comprehensive escalation and communication procedures as well as contact information of all relevant stakeholders in the event of major disruption. This includes identifying those responsible for communicating with staff and external stakeholders as well as addressing related issues during a major operational disruption.

12.2 It would be appropriate for LFI to have alternative methods of communication to avoid over-relying on one primary mode.

12.3 The LFI is required to notify Labuan FSA's Supervision and Monitoring Department through expeditious means (e.g. email, phone call, WhatsApp or Telegram text messages etc.) on the occurrence of any event that leads to the activation or

execution of the business continuity arrangements as soon as practicable or within 48 hours. The notification should provide the trigger and extent of the BCM incident.

12.4 The LFI is required to maintain the *Incident Reporting Template* as part of its BCM record keeping. As a reference, the LFI may consider at the minimum the content of the Template as outlined in the **Appendix**. This document may be requested by Labuan FSA as part of its supervisory monitoring.

Best Practices

12.5 As part of the communication plan, the LFI may include a systematic communication method and procedures by incorporating key information, amongst others:

(i) digital and analogue means such as land line phones, automated phone tree platforms, mobile phones, text messaging, emails, etc. for both primary and alternative mode of communication;

(ii) key contact information to address issues relating to failures in primary communication systems; and

(iii) the manner to actively monitor and respond to potential misinformation and misrepresentation of facts in all communication and media platforms that may adversely affect the LFI's reputation.

13.0 Maintenance and review

<u>Principle 7</u>: A periodic review and maintenance of approaches and strategies for business continuity is needed to reflect the LFI's operating environment and business circumstances.

Minimum Requirements

13.1 The LFI is required to plan for the maintenance and review of its BCM on on-going basis.

13.2 All relevant material changes in terms of technological, procedural updates as well as changes in the roles and responsibilities of employees need to be reflected in the BCM.

13.3 Any significant amendments or updates to the BCM would be subject to the senior management's concurrence.

13.4 In view that BCM covers critical function and business operation of the LFI, the review of the BCM would be part of the auditable scope of the LFI's internal audit function. For the LFI that leverages on its group's BCM, such audit can be undertaken by the group's internal audit.

Best Practices

13.5 The LFI may incorporate the maintenance and review of its approaches to business continuity as part of day-to-day business operations. For this purpose, the LFI may consider having a designated team or officer responsible for maintaining the relevant documentations.

13.6 To ensure the ongoing relevancy and effectiveness of the BCM, maintenance and reviews may not only be activated by post-testing findings or limited to a scheduled basis.

Labuan Financial Services Authority
23 February 2021

APPENDIX INCIDENT REPORTING TEMPLATE

Name of LFI (may include the LFI's logo) Incident Reporting Template		
Part A: Contact Information		
(i)	Name & designation of the Reporting Officer	
(ii)	Date of report	
Part B: Details of Incident		
(i)	Nature of incident	
(ii)	Immediate actions or responses taken	
Part C: Impact Assessment		
(i)	Impact to business/ operations	
(ii)	Impact to stakeholders	
Part D: Root Cause Analysis		
(i)	Factors/gaps that have contributed to the incident	
(ii)	Actions taken/ enhancement or rectification identified to prevent future incidents	