GUIDING PRINCIPLES ON BUSINESS CONTINUITY

SC-GP/1-2019

1st Issued: 14 May 2019

Suruhanjaya Sekuriti
Securities Commission
Malaysia

GUIDING PRINCIPLES ON BUSINESS CONTINUITY

Effective Date upon 1st Issuance:	14 May 2019

CONTENTS

Page

PART I: INTRODUCTION AND OVERVIEW 1

PART II: DEFINITIONS 3

PART III: GUIDING PRINCIPLES ON BUSINESS CONTINUITY 5

Principle 1: Responsibility of the Board and senior management 5
Principle 2: Major operational disruptions 7
Principle 3: Recovery objectives and strategies 10
Principle 4: Communications 11
Principle 5: Testing and Training 13
Principle 6: Maintenance and Review 15

APPENDIX I: INCIDENT REPORTING TEMPLATE 16

PART I

INTRODUCTION AND OVERVIEW

Introduction

1.1 This document is applicable to all capital market entities[1].

1.2 It serves as a guidance on the Securities Commission Malaysia (SC)'s expectations on business continuity as well as a platform to increase awareness on the importance of having an effective business continuity arrangement.

1.3 Capital market entities may adopt the principles to varying degrees that is proportionate to their respective business activities and risk profile.

1.4 The SC, with its supervisory responsibility over capital market entities, requires each capital market entity to have business continuity management arrangements as part of ensuring systemic resiliency of the Malaysian capital market.

Overview

1.5 Business Continuity Management (BCM) is a whole-of-business approach that includes framework, strategies, systems, policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption[2]. BCM is complemented by a Business Continuity Plan (BCP), which is a comprehensive written plan of action that sets out the procedures and systems dependency necessary to restore the operations of an entity during any event of disruption.

1.6 The objective of this document is to guide the capital market entities on minimum standards where entities are encouraged to adopt based on the nature, size and complexity of their business operations. The overall intended outcomes of the principles are to ensure timely continuation of critical services and the fulfilment of

[1] Entities that are regulated by the SC either via licensing, authorisation, approval or registration as required under securities laws.
[2] High-level principles for business continuity, *The Joint Forum*.

business obligations in the event of disruptions and ultimately with the objectives to mitigate or manage any possible wider systemic risk[3] implications to the Malaysian capital market.

1.7 The Guiding Principles also seeks to enhance awareness and understanding on the importance of business continuity among capital market entities. It is important to note that these principles should not be considered as the only solution to achieving systemic stability in the capital market. In addition, the SC acknowledges that there is no one-size-fits-all approach towards how business continuity should be adopted within the scope of the Malaysian capital market.

1.8 The principles outlined are not intended to be prescriptive; rather, they constitute a broad framework of best practices relevant to all capital market entities.

[3] As defined in the *Securities Commission Malaysia Act 1993* (SCMA).

PART II

DEFINITIONS

2.1 Unless otherwise defined, all words or terms used in these Guiding Principles have the following meanings:

Capital market entities (the entity)	Entities that are regulated by the SC via either licensing, authorisation, approval or registration as required under securities laws. Among others, these will include approved stock exchange i.e. Bursa Malaysia, Capital Markets Services Licence (CMSL) holders, registered persons and self-regulatory organisations under securities laws. Exceptions include financial institutions who are registered persons as set out in Part 1, Schedule 4 of the CMSA as well as entities registered under the *Guidelines on the Registration of Venture Capital and Private Equity Corporations and Management Corporations,* and Pengurusan Danaharta Nasional Bhd and its subsidiaries.
Business continuity management	A whole-of-business approach that includes framework, strategies, systems, policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption.
Business continuity plan	A comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operations of an entity during any event of disruption.
Systemic risk	As defined in the *Securities Commission Malaysia Act 1993* (SCMA), "systemic risk in the capital market"

	means a situation when one or more of the following events occurs or is likely to occur: (a) financial distress in a significant market participant or in a number of market participants; (b) an impairment in the orderly functioning of the capital market; or (c) an erosion of public confidence in the integrity of the capital market.
Recovery objectives and strategies	Course of action and minimum required level of business operations following any disruptions. The recovery objective is defined, approved by senior management and has been tested on a periodic basis.
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.

PART III

GUIDING PRINCIPLES ON BUSINESS CONTINUITY

Principle 1: Responsibility of the Board and senior management

Intended Outcome

Board of directors and senior management[4] collectively hold the ultimate responsibility in ensuring sound and effective business continuity that is tailored to the nature, scale and complexity of the entity's business.

3.1 Board of directors and senior management are accountable for the entity's business continuity preparedness.

3.2 Formal designation of business continuity responsibilities is encouraged to enable smooth and efficient planning as well as seamless execution of the framework. Board of directors should appoint a member of senior management to be in charge of business continuity.

3.3 In addition, certain business continuity responsibilities and decision making may be delegated to individual business line managers for the purposes of capacity building and succession planning.

3.4 The roles and responsibilities of board of directors and senior management, at a minimum, include the following:

(a) Approve the business continuity framework, strategies and policies;

(b) Ensure effective implementation of the business continuity framework or approach;

(c) Allocate adequate manpower resources and training to increase organisational awareness on business continuity and preparedness;

[4] The terms "board of directors" and "senior management" are used in this document not to identify legal constructs but rather to label two decision-making functions within a capital market entity.

(d) Ensure clear articulation of roles, responsibilities, authorities and succession plans;

(e) Ensure that business continuity related matters are reported to the board of directors at least annually;

(f) Ensure at least an annual testing is conducted and regular updates of business continuity documents and processes by internal or relevant external party; and

(g) Ensure the business continuity framework complies with relevant regulatory and legal requirements as well as any directives that may be issued by regulatory authorities.

Principle 2: Major operational disruptions

Intended Outcome

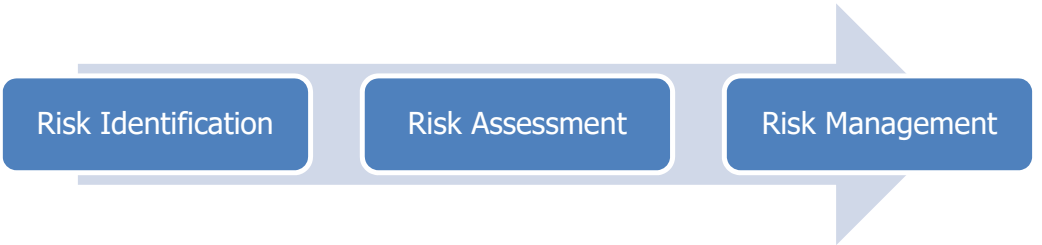
Major operational disruptions and risks arising from interdependency and concentration of critical business functions as well as outsourcing arrangements should be identified. Any adverse impacts and implications of risks from such disruptions are thoroughly assessed and analysed. Mitigation and management of such risks are captured within the business continuity approach adopted.

3.5 Major operational disruptions pose significant risk to the business continuity of an entity's operations. The entity may be affected by wide-area disruptions, due to natural disasters, terrorist attacks or pandemics as well as operational disruptions that occur in isolation such that it only affects a single entity's operations. In addition, the entity may be affected by new events related to growing automation, increased reliance on outsourcing and the interdependencies and interconnectedness within the capital market.

3.6 Given the time constraint and limited resources during major operational disruptions, capital market entities are encouraged to adopt a systematic approach to business continuity to ensure smooth dealing of disruptions and swift response actions. The approach is illustrated in Diagram 1.

Diagram 1

Approach to business continuity in dealing with major operational disruptions



Risk Identification

3.7 A capital market entity could be exposed to financial risks and non-financial risks. On an ongoing basis, the entity should identify and monitor such risks arising from within the entity and external factors that may eventually lead to disruptions to the entity's business operations.

3.8 The SC recommends that capital market entities should consider and monitor the following:

(a) Financial and non-financial risks potentially arising from internal and external factors;

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

(c) Concentration risks arising from centralisation of critical and support functions; and

(d) Risks of outsourcing its critical business functions to third-party service providers.

Risk Assessment

3.9 Risk assessment aims to evaluate potential operational disruptions based on their severity, which is determined by the probability of occurrence and their impacts on critical business functions and business operations as a whole.

3.10 The entity may choose to assess the impacts of operational disruptions on its critical business functions via business impact analysis and identify the critical business functions or operations that are necessary to be prioritised in its recovery strategies.

3.11 When assessing the probability of a disruption, the entity is encouraged to take into consideration the geographical locations of all facilities, their susceptibility to threats, and the proximity to key infrastructure. This is followed by gauging and determining the severity of the disruption. The entity can then take appropriate mitigating

measures to manage the disruptions and ensure continuity and resumption of its critical business functions and business operations as a whole.

Risk Management

3.12 Based on the risk assessment, the entity should establish its risk management objectives, including–

(a) managing the immediate consequences of a disruption;

(b) ensuring the continuity of critical business activities;

(c) maintaining an appropriate level of service; and

(d) reducing the duration of the interruption to a level acceptable to the entity and its relevant stakeholders.

3.13 With clear risk management objectives, the entity may align both its priorities and resources. As resources are generally scarce, the entity should effectively allocate necessary resources in order to plan for the continuity and resumption of its business activities and operations.

3.14 Response measures are encouraged to be put in place by the entity in order to describe in detail the manner of ensuring the continuity of its critical business functions and operations, at a minimum level of service and within an acceptable period.

Principle 3: Recovery objectives and strategies

Intended Outcome

Recovery objectives and strategies are developed according to risk-based principles where prioritisation of recovery are based on the degree or level of risk the entity's business units poses to the entire business operation.

3.15 Capital market entities are encouraged to develop recovery objectives and strategies that reflect the risk they represent to the operation. Recovery objectives and strategies may also be developed for specific business functions, which should be established in consultation with, or by, the respective business unit. Ultimately, the board of directors and senior management are responsible for the recovery objectives and strategies.

3.16 Recovery objectives and strategies should include identification of recovery levels and recovery time objectives for specific business lines. This aims to give assurance on the level of resilience and recovery timeframe during an operational disruption. This information may serve as a benchmark when testing adequacy of business recovery approaches.

3.17 The SC encourages capital market entities to have access to at least one or more recovery sites in the event where the primary site is inaccessible. Some of the factors that may be considered for recovery arrangements include–

(a) geographical location of the recovery site and its proximity to the primary site;

(b) adequacy of current data, equipment and system; and

(c) availability of sufficient staff, in terms of numbers and expertise, to recover critical operations and services.

Principle 4: Communications

Intended Outcome

Comprehensive escalation procedures and communication plans during major operational disruptions for internal and external stakeholders are established and embedded in the business continuity framework. Such procedures should enable timely, transparent and coordinated dissemination of information that are adequate to address any reputational risks arising from major operational disruptions.

3.18 Successful deployment and execution of a business continuity framework is highly dependent on co-ordinated, coherent, timely and effective communications within the entity and with its relevant external stakeholders in order to ensure consistent messaging and minimise reputational risks during major operational disruptions.

3.19 The SC recommends that capital market entities' business continuity framework to include comprehensive escalation and communication procedures as well as contact information of all stakeholders, including employees, counterparties, clients, service providers, building management, regulatory authorities,[5] government agencies, emergency services and media. In addition, entities are encouraged to take into account alternative methods of communication in the case of interruptions of primary method of communication.

3.20 The entity may also conduct call tree exercises and periodic testing of call tree to enhance the escalation and communication process within the entity.

3.21 Entities are encouraged to identify ways to actively monitor and respond to potential misinformation and misrepresentation of facts in all communication and media platforms that may adversely affect the entity's reputation.

3.22 With regard to communications with the SC, entities should immediately notify their respective regulatory supervisors in the SC of the occurrence of any event that would trigger the activation or execution of the business continuity arrangements or

[5] Including foreign regulatory authority for capital market entities with parent company/subsidiaries in foreign jurisdictions.

protocols, in such form and manner as may be specified by the SC. Following an incident, a report is to be submitted within three (3) business days based on the reporting template as provided in **Appendix I**.

Principle 5: Testing and Training

Intended Outcome

Testing and training are done at least annually by the entities to ensure ongoing reliability and relevancy, incorporating evolving market practices, changes in key personnel and technology utilised in day-to-day business operations as well as regulatory policy updates.

3.23 The SC takes note that testing of approaches or framework to business continuity is important to provide assurance that its plan is reliable and relevant. In addition, it is highly recommended that regular testing is done to assess effectiveness and relevance.

3.24 Testing for critical business functions should be carried out at least annually. Senior management and employees who are involved are encouraged to participate in these exercises to promote awareness, familiarity and understanding of their roles and responsibilities within the scope of the approach towards business continuity.

3.25 Testing objectives may include the integration of core components of the approach adopted for business continuity as well as incorporating various interdependencies within and outside of the entity's business operations. In conducting a testing exercise, the SC recommends considering different levels of complexity, degree of employee or service provider participation, types of critical functions as well as different physical locations.

3.26 At the end of each testing exercise, the entity is encouraged to prepare a formal documentation of the post mortem reviews of the testing programme. Testing results should be assessed to incorporate the necessary changes or remedial actions into the existing approach for business continuity, while the overall programme is evaluated for its effectiveness in achieving the testing objective and incorporating appropriate testing coverage.

3.27 Documentation relating to the testing programme and results should be prepared for senior management to sign-off and to be reported to Board of Directors for endorsement. These documentations should be made available upon the SC's request.

3.28 Capital market entities are encouraged to provide training to key business continuity coordinators to ensure adequate skillsets and competencies in managing or organising business continuity testing as well as to encourage awareness.

Principle 6: Maintenance and Review

Intended Outcome

The approach or framework for business continuity are regularly maintained and reviewed by capital market entities. Any material updates or changes are acknowledged, approved and endorsed by the Board and senior management. Employees are encouraged to be made aware of such updates or changes.

3.29 Maintenance and reviews may not be limited to only after testing or restricted to a scheduled basis. Any significant changes in terms of technological, procedural updates as well as changes in the roles and responsibilities of employees should be reflected as and when it occurs.

3.30 A capital market entity may incorporate maintenance and review as part of their day-to-day business operations. A designated team and/or officer should be in charge of maintaining relevant documentations. A copy of the entity's framework for business continuity should be made available to the SC upon request or during the SC's supervisory activities.

3.31 Amendments or updates should be acknowledged and signed-off by the Board and senior management. Independent review of the business continuity framework may be performed by the internal or external audit functions of the entity.

APPENDIX I

INCIDENT REPORTING TEMPLATE

Instructions:

1. All capital market entities should report any event that would trigger the activation or execution of their business continuity arrangements or protocols, in such form and manner as may be specified by the SC.

2. The **Incident Reporting Template is to be submitted within three (3) business days to each of the respective officer in the SC who is charge in terms of their day-to-day supervision**.

3. The SC may require the affected capital market entities to submit further detailed report on the incident, following the initial report.

4. In the event of an incident involving any cyber security or breaches, Paragraph 4.16[6] of the *Guidelines on Management of Cyber Risk* applies. A report submitted to the SC must be made in accordance with the reporting template as provided in the *Guidelines on Management of Cyber Risk*.

Incident Reporting Template	
Contact Information:	
• Date and Time of Notification to SC	
• Full Name of Entity	
• Name of Reporting Staff	
• Designation/Department	
• Contact details (e.g. email, mobile)	
Details of Incident:	
• Nature of incident	

[6] The capital market entity must report to the SC on any detection of a cyber incident which may or have had an impact on the information assets or systems of the entity, on the day of the occurrence of the incident.

• Actions or responses taken	
Impact Assessment (*examples given are none exhaustive and for illustration purposes)*):	
• Impact to business/operations – *E.g. clearing and settlement activities, online trading/transactions etc.*	
• Impact to stakeholders – *E.g. affected retail/institutional clients, affected counter parties, settlement institution and service providers etc.*	
Root Cause Analysis:	
• Factors contributed to the incident	
• Step identified/taken to address the incident in the longer term	

Note:

The SC will maintain the confidentiality of data received.